IRIS plus

How Private is Personal Data?

2013-6

LEAD ARTICLE

Copyright and the Protection of Personal Data
Intermediaries Caught Between Two Areas of the Law
- Legal bases at European level
- Actual areas of conflict

RELATED REPORTING

Recent Case Law
- Germany
- Finland
- France
- United Kingdom
- Netherlands
- Russian Federation

ZOOM

The Patriot Act & the Fourth Amendment
How the US Government is Secretly Expanding its Authority to Collect the Private Data of its Citizens

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS *plus* 2013-6
How Private is Personal Data?

ISBN (Print Edition): 978-92-871-7791-9
Price: EUR 25,50
ISBN (PDF-Electronic Edition): 978-92-871-7794-0
Price: EUR 34,50
European Audiovisual Observatory, Strasbourg 2013

IRIS *plus* Publication Series 2013
ISSN (Print Edition): 2078-9440
Price: EUR 100
ISSN (PDF-Electronic Edition): 2079-1062
Price: EUR 130

Director of the Publication:
Susanne Nikoltchev, Executive Director of the European Audiovisual Observatory
E-mail: susanne.nikoltchev@coe.int

Editor and Coordinator:
Dr Susanne Nikoltchev, LL.M. (Florence/Italy, Ann Arbor/MI)

Editorial Assistant:
Michelle Ganter
E-mail: michelle.ganter@coe.int

Marketing:
Markus Booms
E-mail: markus.booms@coe.int

Typesetting:
Pointillés, Hoenheim (France)

Print:
Pointillés, Hoenheim (France)
Conseil de l'Europe, Strasbourg (France)

Cover Layout:
Acom Europe, Paris (France)

Publisher:
European Audiovisual Observatory
76 Allée de la Robertsau
F-67000 Strasbourg
Tel.: +33 (0)3 90 21 60 00
Fax: +33 (0)3 90 21 60 19
E-mail: obs@obs.coe.int
www.obs.coe.int

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Contributing Partner Institutions:

Institute of European Media Law (EMR)
Franz-Mai-Straße 6
D-66121 Saarbrücken
Tel.: +49 (0) 681 99 275 11
Fax: +49 (0) 681 99 275 12
E-mail: emr@emr-sb.de
www.emr-sb.de

Institute for Information Law (IViR)
Kloveniersburgwal 48
NL-1012 CX Amsterdam
Tel.: +31 (0) 20 525 34 06
Fax: +31 (0) 20 525 30 33
E-mail: website@ivir.nl
www.ivir.nl

Moscow Media Law and Policy Center
Moscow State University
ul. Mokhovaya, 9 - Room 338
125009 Moscow
Russian Federation
Tel.: +7 495 629 3804
Fax: +7 495 629 3804
www.medialaw.ru

Please quote this publication as:
IRIS *plus* 2013-6, How Private is Personal Data?, Susanne Nikoltchev (Ed.), European Audiovisual Observatory, Strasbourg 2013

How Private is Personal Data?

Foreword

In 2010, Facebook's co-founder and CEO Mark Zuckerberg declared that "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time". Indeed, many things seem to have changed since the emergence of the Internet, notably the way we make information available to the public. New expectations about what should be freely available to all of us have also developed. And some argue that these changes should be reflected in legislation.

Of course, legislation tends to follow societal developments at a slower pace, so that it often seems to fall behind widespread attitudes and behaviours. But does that mean that legislation should always conform to social norms? Whereas the latter tend to reflect the majority view, the law is the result of a balancing act in which different rights and interests have to be pondered and weighed against each other, including those of minority groups. And besides, who decides on what is a social norm? Obviously, not Mark Zuckerberg alone...

In general terms, it could be said that privacy is a person's right not to make public certain personal information. Whether or not this right is enforceable in an online environment is a matter of concern for many people, and not only Facebook users. Every user's Internet activity leaves a trail of digital breadcrumbs behind that serve as clues to this user's life. This information can be gathered and used by third parties in many profitable ways. In some cases, this information has been provided by the user either willingly or in others inadvertently. But sometimes third parties require insight into a user's life that goes beyond what a user is prepared to accept. Two examples of this have raised a lot of attention recently. The first concerns rightsholders seeking to find out about the identity and whereabouts of Internet users in order to sue them for copyright infringement. The second concerns the eavesdropping activities of national intelligence agencies for the purpose of protecting their citizens from terrorist and other criminal activities. In both cases, the fact that they need this data does not mean that they are legally allowed to have it.

This IRIS *plus* analyses the boundaries of privacy and its relation to other fundamental rights. The lead article discusses the somewhat strained relationship between copyright and the protection of personal data. The related reporting section presents recent case law relevant to the questions raised by the lead article. Finally, the Zoom section deals with the recent scandal provoked by the publication in the press of leaked documents concerning secret surveillance programmes carried out by US agencies.

Strasbourg, November 2013

Susanne Nikoltchev
Executive Director
European Audiovisual Observatory

TABLE OF CONTENTS

LEAD ARTICLE

RELATED REPORTING

ZOOM

Copyright and the Protection of Personal Data

Intermediaries Caught Between Two Areas of the Law

Dr Martin Rupp and Mag. Peter Matzneller,
Institute for European Media Law (EMR), Saarbrücken/Brussels

I. Introduction

There is an uneasy relationship between copyright and data protection, the main reason being that the legal rules governing both these areas are based on a potentially conflicting idea. There is a clash of objectives between copyright law and data protection law, but this does not immediately become apparent when the intention of the legislators in each case is compared.

Copyright law protects the author's/creator's intellectual property both from the non-material and, in particular, the material point of view. The purpose of the provisions on content, scope and transferability as well as on the consequences of a violation and on the ability to enforce copyright claims is to enable the author/creator to exploit their work economically.

The aim of *data protection law*, on the other hand, is to enable individuals to decide themselves whether to disclose personal information about them and how it is to be used.

The extent to which the "peaceful coexistence" of the two areas of legislation could be problematic is not immediately obvious. However, a clash of objectives comes about as soon as rightsholders want to investigate a breach of copyright, in which case they will have an interest in asserting their claims against the infringer. These claims may involve an application for an injunction, damages, the destruction of material, etc. In order to assert these claims, the rightholders must first of all identify the infringer, for which purpose copyright law provides them with special rights regarding the disclosure of information – including vis-à-vis third parties.

It is precisely here that a conflict ensues between data protection law and copyright law. Data protection law imposes limits on "unlimited information". Copyright infringers – or even potential infringers – are also entitled to assert the rights granted to them by data protection law to continue to determine the use of their personal information, and the legal order is therefore required to regulate this sensitive area. On the one hand, rightsholders need certain information in order to assert their rights effectively; on the other hand, data protection law requires that steps be taken to prevent the proliferation of that information. This article discusses this uneasy relationship.

In order to examine this conflict, we shall first of all discuss the legal sources of the European Union and the Council of Europe, the bases of which are the so-called Founding Treaties[1] of the European Union and the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms[2] (ECHR), which set out the citizens' basic rights and freedoms. However, the main focus will be on the shaping of copyright law and data protection law by secondary legislation. The European Union has given shape to both areas of the law Europe-wide by issuing various directives.

Actual areas of conflict will then be described. Current examples, taken especially from the case law of the Court of Justice of the European Union (CJEU), will make clear the nature of the problem and illustrate the conflicting interests from the practical point of view. A brief look at individual national legal orders will indicate alternative models for asserting copyrights without the disclosure of too many personal data.

II. Legal bases at European level

The legal bases at European level are primarily established in the law of the European Union, but important provisions are also to be found in the legal instruments of the Council of Europe.

1. Aspects in terms of fundamental rights

1.1. Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (CFREU) is of particular importance for the uneasy relationship between the interests of copyright law and data protection.[3]

In this connection, support for copyright and rights owners is always provided by Article 17 CFREU, paragraph 2 of which expressly protects intellectual property, whereas Article 8 CFREU enshrines the protection of personal data as a fundamental right. Moreover, in some situations freedom to choose an occupation or freedom to conduct a business applies pursuant to Articles 15 and 16 CFREU. Freedom of information pursuant to Article 11 CFREU also becomes relevant as soon as filtering systems to prevent copyright infringements are employed.[4] In the event of a conflict, the CJEU often tries to balance the competing interests in order to reconcile them.

1.2. Convention for the Protection of Human Rights and Fundamental Freedoms

Furthermore, data protection on the one hand and the protection of authors'/creators' rights on the other are also enshrined in the canon of rights of the Council of Europe. Article 8 ECHR guarantees the right to respect for private and family life, while Article 1 of Protocol No. 1 to the ECHR provides for the protection of property. When the dissemination of copyright-protected works is also considered from the point of view of the dissemination of information and opinions, the rights to freedom of expression and to freedom of information pursuant to Article 10 ECHR also come into play.[5] The European Court of Human Rights (the Strasbourg Court) also stresses the need to weigh up the positions of both sides in cases that involve a conflict of the objectives of copyright law with other interests.

1) The Treaty on European Union in the version of the Treaty of Lisbon (TEU Lisbon) of 13 December 2007 (OJ C 306 p. 1, OJ 2008/C 111 p. 56, OJ 2009/C 290 p. 1, OJ 2011/C 378 p. 3) and the Treaty on the Functioning of the European Union (TFEU) in the version of the announcement of 9 May 2008 (OJ C 115 p. 47).
2) http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.
3) Charter of Fundamental Rights of the European Union of 12 December 2007, OJ C 303 p. 1.
4) See on this C. Angelopoulos, *Filtering the Internet for Copyrighted Content in Europe*, IRIS *plus* 2009-4.
5) Corresponding to Article 11 CFREU.

In its case law to date, the Strasbourg Court has not very often had to deal with the specific conflict between copyright law and data protection. The "classic" Strasbourg Court judgments on media issues involve the clash between Article 8 and Article 10 ECHR. These are mostly cases in which media reporting interferes with the private life of the person concerned. Up to now, copyright law has proved relatively "unaffected" by the Court's case law. Two of its most recent judgments should be emphasised. First of all, in *Ashby Donald and Others v. France*[6] French copyright law clashed with Article 10 ECHR. In that case, fashion photographers published copyright-protected pictures of fashion shows without the fashion companies' consent and the domestic French courts ordered the photographers to pay fines and damages for a breach of copyright. The Strasbourg Court confirmed the precedence of copyright law in such a situation, stating that the fines and damages were not disproportionate and that the decisions of the domestic courts could be regarded as a fair balance of the conflicting interests.

Of particular interest for the roles of intermediaries is the Strasbourg Court's decision of 19 February 2013 in *Neij and Sunde Kolmisoppi v. Sweden*.[7] The applicants were the developer and the press officer of The Pirate Bay, the world's largest so-called BitTorrent tracker.[8] Although the file-sharing did not take place via the service provider's server, they were sentenced in the domestic proceedings before the Swedish courts for complicity to commit breaches of copyright to ten and eight months' imprisonment respectively and ordered to pay damages amounting to EUR 5 million.

The Strasbourg Court held that the service provided by The Pirate Bay was protected by Article 10 ECHR and that the judgment of the Swedish courts accordingly constituted interference with the right to freedom of expression. The crucial factor was therefore whether that interference was "necessary in a democratic society", in the words of Article 10(2) ECHR. The Court ruled that that was the case and that there had been no violation of Article 10 of the Convention. Owing to the overriding interests of the Swedish state in protecting the copyrighted property, no fault could be found in the assessment of The Pirate Bay's services as complicit acts involving criminal liability. In this connection, the Court also took account of the fact that the operators had refused to remove the torrent files despite being asked to do so on several occasions.

Apart from the Strasbourg Court's case law, the European Convention on Human Rights also plays an important role at national level since it applies in all Council of Europe member states in the form of directly applicable domestic law, ranking either above ordinary laws[9] or having the status of constitutional law.[10] Furthermore, the basic rights enshrined in the ECHR are, pursuant to Article 6(2) and (3) TEU, also part of EU law.

2. Primary law

The importance of copyright law and data protection for the enactment of legislation by the organs of the European Union already becomes clear from the primary law that forms the basis for EU action.

2.1. Copyright law

Copyright law has a strong economic connection, which means it is particularly important for the free movement of goods and services and free competition. The creation and exploitation of

6) Judgment of 10 January 2013, Application No. 36769/08, available in French at http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-115845; see also D. Voorhoof, IRIS 2013-3/1.
7) Application No. 40397/12, available in English at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-117513. See also D. Voorhoof, IRIS 2013-5/2.
8) A BitTorrent tracker does not carry out the exchange of files itself but helps providers and seekers of certain files to find one another. They then exchange files direct without using the tracker.
9) As in the case of most states, such as Belgium, France, Greece, Portugal, Spain and Switzerland.
10) For example in Austria. In Germany, Italy and the United Kingdom, the ECHR has the status of an ordinary law, although in these states too particular consideration must be given to the ECHR when interpreting other laws so that it ranks higher de facto than any other ordinary law.

copyright-protected works and the assertion of the copyrights in them do not only take place at national level but easily cross national borders[11] – not least given the many technical means available. This applies in particular to the distribution of such works by audiovisual media services.[12]

According to Article 26 TFEU, the European Union endeavours to create an internal market without internal frontiers in which the free movement of goods (Articles 28 ff. TFEU) and services (Articles 56 ff. TFEU) as well as free and fair competition (Articles 101 ff. TFEU) are guaranteed. This is accompanied by efforts to harmonise the legal order(s) within the EU, so Article 114 TFEU calls for the approximation of laws. With the Treaty of Lisbon, an explicit legal basis for harmonisation in the field of copyright was established in Article 118 TFEU, according to which the EU should work towards providing "uniform protection of intellectual property rights throughout the Union". Also as a result of the Treaty of Lisbon, intellectual property was recognised in Article 207(1), 1st sentence, TFEU as an element of the common commercial policy.

On this basis, the European Union has enacted a number of directives for copyright law that have had a clear impact on member states' legal orders (see below).

2.2. Data protection law

Like copyright-protected works, personal data often also possess economic value. The information is used to conduct business deals and – as in the present case – is of particular relevance for the – if necessary forced – assertion of copyrights. For the same reasons to do with the internal market in the case of copyright law, the European Union accordingly believes it must take regulatory action. The TFEU also contains a special provision for data protection: Article 16(1) TFEU first of all postulates the right to the protection of one's own personal data, while Article 16(2) TFEU in conjunction with Article 39 TEU also instructs the European Union and its member states to enact rules on data protection. However, this is not only directed at data protection itself but also the provision of a guarantee of the free movement of data.[13]

3. Secondary law

Both copyright law and data protection law are set out in detail in the relevant EU directives and regulations in particular.

3.1. Copyright law

The copyright law of the European Union is made up of a large number of directives and other legal instruments. Of particular importance for the uneasy relationship between data protection and copyright law is, first of all, the Directive on the harmonisation of certain aspects of copyright and related rights in the information society (2001/29/EC),[14] the aim of which is to bring about the EU-wide adaptation of copyright law to the digital world and electronic commerce. To this end, the rights of authors/creators – such as reproduction rights and the right to communicate and make available to the public – are adapted for the online sector in particular, thus placing authors/creators in a stronger position. Article 8(3) of the Directive provides for court injunctions against mediators

11) See on this the Communication from the Commission on "Enhancing the enforcement of intellectual property rights in the internal market" of 11 September 2009, COM(2009) 467 final, and the Communication from the Commission on "Content in the Digital Single Market" of 18 December 2012, COM(2012) 789 final.
12) A. Yliniva-Hoffmann/P. Matzneller, *The Legal Protection of Broadcasters – Challenges Posed by New Services?*, IRIS *plus* 2010-5. All IRIS *plus* lead articles cited here are available at www.obs.coe.int/oea_publ/iris/iris_plus/index.html.
13) However, the data protection to be guaranteed in accordance with Article 16(2) TFEU is primarily binding on the organs, institutions and authorities of the European Union and member states insofar as they are engaged in activities that fall within the scope of EU law.
14) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society ("Copyright Directive" or "Information Society Directive"), OJ L 167 of 22 June 2001, pp. 10-19.

when their services are used by a third party for the purpose of copyright infringements.[15] Directive 2001/29/EC is closely connected to Directive 2000/31/EC (E-Commerce Directive[16]), Articles 12, 13 and 14 of which contain significant limitations of liability with regard to intermediaries, who as service providers are not responsible for any information and content that is:

- only transmitted by them (Article 12: Mere conduit);
- automatically stored on a temporary basis (Article 13: Caching);
- provided by the user and stored by the intermediary at the user's request (Article 14: Hosting).

However, these limitations of liability do not affect a service provider's duty to terminate or prevent breaches of the law and they expressly permit member states to enable their courts and administrative authorities to issue the relevant orders.

Furthermore, Article 15(1) of the E-Commerce Directive establishes that intermediaries are not in any way obliged to monitor the information that they transmit or to take action to investigate circumstances indicating illegal activity. Paragraph 2, on the other hand, provides for the possibility of compelling intermediaries in individual member states to inform the competent authorities about any alleged illegal activities. In addition, national legislation can give the relevant supervisory authorities the right to require intermediaries to provide information on the users of their service. It is possible to conceive of situations where the criminal law of copyright applies and the national investigating authorities, such as public prosecutors, contact intermediaries with requests for information.

However, only the "competent authorities" have the above-mentioned right contained in Article 15 of the E-Commerce Directive to request information. In particular, this excludes the rightsholders, who generally have a considerable interest in asserting their claims in the case of copyright violations, of which a large number take place in the online sector.[17] The liability of intermediaries as third parties can be ruled out on the basis of the aforementioned Articles 12 to 14 of the E-Commerce Directive, so rightsholders must turn to the actual infringer. In order to establish the latter's identity, however, they need to have the same rights to request information as those provided for by Article 15 of the E-Commerce Directive in the case of public authorities.

Such a right for rightsholders to request information – which did not yet exist in some member states – was granted by Enforcement Directive 2004/48/EC.[18] This right was created with the intention of limiting any discrepancies regarding the provisions on interim measures for securing evidence or for putting an end to breaches of the law[19] and is enshrined in Article 8 of the Enforcement Directive.[20]

15) See also Recital 59: "In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work [...] in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.".

16) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("E-Commerce Directive"), OJ L 178 of 17 July 2000, pp. 1-16.

17) It is often necessary to take the "roundabout route" via the public prosecutor in order to establish the infringer's identity in countries where the domestic legal order does not give the rightsholder a direct right to request information from the access provider.

18) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights in the amended version of 30 April 2004, OJ L 157 of 30 April 2004, pp. 45-86.

19) See Recital 7 of the Enforcement Directive (2004/48/EC).

20) Article 8 of Enforcement Directive 2004/48/EC accordingly puts in more concrete terms the generally worded legal remedy in Article 8(3) of the Copyright Directive 2001/29/EC.

According to Article 8, member states must ensure that, in proceedings concerning copyright infringements, courts can also request information from third parties (and therefore intermediaries) at the claimant's request if the case involves specific circumstances such as the commercial scale of the infringement. This request for information relates to the origin and distribution channels of the copyright-infringing activities, but it may be appropriate to extend it to include the names and addresses of those involved in the infringement. In comparison to earlier plans of the European Commission, Article 8 of the Enforcement Directive contains a "more limited" right of information: Article 9 of the Commission's original proposal for a directive on measures and procedures to ensure the enforcement of intellectual property rights[21] contained a more extensive right to request information from "any person", and a mere suspicion of a breach of the law was to be a sufficient ground for doing so. This was severely criticised by data protection experts as this version would not have limited the right of information to the context of pending proceedings and that right could have been enforced in civil proceedings "against person or persons unknown".[22] In the light of the proposal, it was feared that access providers would be investigated in cases of mere suspicion. In the proposal for a directive, the right of information was also extended to any private individual and not only to those who infringe copyright on a commercial scale. Furthermore, under Article 9(4) of the proposal customs and police authorities were to forward automatically to the rightsholders concerned any data that became known to them in connection with copyright infringements. This provision was not included in the final version of the Enforcement Directive either.

3.2. Data protection law

Secondary copyright legislation is subject almost entirely to the data protection provisions of EU law. According to Article 2(3)(a) of the Enforcement Directive 2004/48/EC, the provisions of this directive do not affect the Data Protection Directive 95/46/EC.[23] Data protection law was thus given priority over copyright law because the other relevant directives mentioned in Article 2(3)(a) apply subject to other rules in the Data Protection Directive or at least to compliance with the data protection provisions when applying copyright law.[24] For the field of electronic commerce, too, the E-Commerce Directive refers in Recital 14 to the Data Protection Directive in its entirety. Especially with regard to rights to request information under the E-Commerce Directive, the latter always takes priority.[25]

The Data Protection Directive contains the basic provisions and principles concerning data protection that form part of the secondary law of the European Union and have been transposed into the data protection laws of all member states. These principles include a ban on action being taken unless permission is granted: according to Article 7 of the Data Protection Directive, personal

21) COM/2003/0046 final – COD 2003/0024; the Enforcement Directive (2004/48/EC) is based on this proposal.
22) This was stated for example by Germany's Federal Commissioner for Data Protection and Freedom of Information in a press release of 10 March 2004, "Schaar begrüßt Stärkung des Datenschutzes bei der IPR-Enforcement-Richtlinie" available at http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/Archiv/06-04StaerkungDesDatenschutzesBeiDerIPR-Enforcement-Richtlinie.html?nn=409394
23) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23 November 1995, pp. 31-50
24) See Recitals 57 and 60 of the Copyright Directive (2001/29/EC) and Article 1(5)(b) and Recital 14 of the E-Commerce Directive (2000/31/EC). On the conflict between data protection law with media freedoms, see Alexander Scheuer/Sebastian Schweda, "The Protection of Personal Data and the Media" in: *Limits to the Use of Personal Data*, IRIS *plus* 2011-6, pp. 7-29.
25) Recital 14 of the E-Commerce Directive (2000/31/EC): "The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC [... This] already establish[es] a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive [...]; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards [...] the liability of intermediaries.".

data may only be processed if the person concerned expressly gives their consent.[26] However, this article provides for exceptions in various cases, including where:

(c) "processing is necessary for compliance with a legal obligation to which the controller is subject."[27]
(f) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."

3.3. Legal instruments of the Council of Europe

In the area of data protection, the Council of Europe plays a leading role in the creation of a Europe-wide data protection standard with its Data Protection Convention of 28 January 1981.[28] In legal practice, the EU's data protection law is now more important than the Convention.

The Council of Europe has also turned its attention to the subject of copyright in the online sector and recognised the conflict with the interests of users.

On 12 March 2010, the Council of Europe Parliamentary Assembly (PACE) adopted Recommendation 1906 (2010), which deals with intellectual property rights in a digital society.[29] The aim was to initiate a discussion on a model that finds a balance between the copyrights of authors of intellectual works, investors and the general public. PACE believes that the balance between these interest groups has been significantly affected in the light of the development of the digital society and says that the international instruments available are no longer capable of guaranteeing creators fair remuneration for their works while at the same time ensuring the protection of personal data. According to the recommendation, on the one hand the survival of the creative professions is at stake and on the other hand there is a danger of Internet surveillance.

Although the Council of Europe primarily sees its member states as having an obligation to create a balance, it regards itself as duty-bound to become involved in this process. Paragraph 8.4 of the recommendation refers to the particular role played by mediators ("access providers, content-sharing platforms, search engines").

The Council of Europe was already active in this area a decade earlier, although its focus at that time was clearly more on the protection of copyrights and less on achieving a balance between them and the protection of personal data. In Recommendation Rec(2001)7 on measures to protect copyright and neighbouring rights and combat piracy, especially in the digital environment,[30] the Committee of Ministers deals with the emergence of new forms of piracy.[31] With regard to instruments of civil law, the recommendation calls for the judicial authorities to be empowered to order provisional measures for the prevention and pursuit of infringements, where appropriate

26) This requirement is also contained in Article 6 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), of 25 January 2012.
27) This is the case for example when an intermediary is obliged to disclose a client's personal data owing to a third party's right of information.
28) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) of 28 January 1981.
29) Recommendation 1906 (2010), Rethinking creative rights for the Internet age, available at http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta10/EREC1906.htm. See also V. Breemen, IRIS 2010-10/4.
30) Recommendation Rec(2001)7 of the Committee of Ministers to member states on measures to protect copyright and neighbouring rights and combat piracy, especially in the digital environment, available at https://wcd.coe.int/ViewDoc.jsp?Ref=Rec%282001%297&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383. See also P. Thórhallsson, IRIS 2001-9/7.
31) The recommendation is based on older recommendations dating from 1988 to 1995.

without hearing the other party. It also calls for provision to be made for infringers to be ordered to produce evidence and to disclose the identities of third parties involved in the illicit activity. However, it does not provide for the exercise of rights against intermediaries.

The Convention on Cybercrime also dates from 2001.[32] The approach adopted is clearly based on the criminal law and it does not deal with rightsholders' entitlement to request information from intermediaries. However, "[m]indful ... of the right to the protection of personal data" and of the 1981 Data Protection Convention[33] it does provide for intermediaries to be obliged to disclose information to the competent authorities,[34] which can order service providers to submit subscriber information. For the purposes of this convention, that information comprises, *inter alia*, the type of service used and the period of use and the user's identity (e.g., home address, telephone number). Although the possibility of government bodies obtaining such information is an explosive issue in the context of data protection, the focus of the present discussion is on the relationship between rightsholders, intermediaries and end-users. "Roundabout routes" provided by criminal procedure laws may enable rightsholders to identify copyright infringers but usually do not prove very effective.

The Convention on Cybercrime, which is based on the criminal law, consequently recognises other instruments established in the civil law: according to Article 10(3) it is even possible not to impose criminal liability "provided that other effective remedies are available". Accordingly, if rightsholders are given effective ways to pursue their rights under the civil law this may be considered another effective remedy.

III. Actual areas of conflict

In order to assert their copyrights or related rights, rightsholders, whether they be collecting societies, exclusive licensees or the rightsholders themselves, need a minimum of personal information about the person against whom the claim is directed. In order to be able to contact that person and, as the case may be, enforce their claims through the courts, they at least need the name and address of the person concerned. In addition, it is often of particular interest for the rightsholder to know how and to what extent copyright infringements have taken place. This information also constitutes personal data within the meaning of data protection legislation,[35] which is based on the idea of preventing an uncontrolled flow of personal information. The rightsholder's interest in exploiting a work thus always has to be balanced against the right to privacy of the person concerned.

1. Right to request information from the infringer

The most obvious situation in which copyright and data protection come into conflict arises first of all when rightsholders contact copyright infringers direct in the exercise of their right of information enshrined in Article 8(1) of the Enforcement Directive 2004/48/EC. This right of information does not result in establishing the infringer's identity (which must logically already be known). Rather, the information serves to establish the origin of illicit services, the distribution channels employed and the identity of those involved in the copyright infringement. According to Recital 21 of the Enforcement Directive 2004/48/EC, this so-called third party information serves to ensure a high level of protection for copyrights as it enables other infringements in the same context to be pursued.

32) Of 23 November 2001, ETS 185, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. See also L. Asscher / T. McGonagle, IRIS 2001-5/2 and I. Gentile, IRIS 2001-7/1.
33) See the preamble to the Convention on Cybercrime.
34) Article 18 of the Convention on Cybercrime.
35) Personal data are all information about an identified or identifiable natural person – see Article 2(a) of the Data Protection Directive 95/46/EC.

However, the right is always likely to prove a blunt instrument when the rightsholder simply does not know the infringer's identity. In these cases, rightsholders turn the focus of their attention to intermediaries.

2. Right to request information from intermediaries

The conflict between copyright and data protection becomes more concrete when rightsholders pursuing copyright violations on the Internet would like to use subscriber data held by an Internet access provider or service provider in connection with the provision of its services.

2.1. Identifying the infringer

Copyright infringers, who are initially able to move about the Internet anonymously, can usually only be identified through an IP address allocated at a specific point in time – information that in most cases is only available to the access provider, which can link the subscriber data to the IP addresses allocated.[36] The same applies to Internet service providers (e.g., so-called social networks or hosting websites) insofar as they require their subscribers to register with personal data.

If the rightsholder discovers on the Internet an infringement of the copyright in a work, they initially only have the IP address available to them, so it will probably be more attractive for them to contact the intermediary direct to obtain compensation. However, the intermediary itself is protected by the limitations of liability enshrined in Articles 12 to 15 of the E-Commerce Directive 2000/31/EC and does not incur liability for infringements committed by using its services.[37] Exceptionally, liability is only conceivable when the intermediary is in some way involved in, tolerates or encourages the infringement.[38] In such a case, the details required by Article 5(1) of the E-Commerce Directive make it easier for the rightsholder to take action against the intermediary, which has to make its personal data "easily, directly and permanently accessible" on its website. The Internet service provider is therefore – unlike the end user – not granted the right to move about anonymously online. The rightsholder can not only demand damages from the service provider for infringements that have already occurred[39] but also take preventive action against it for likely future infringements.[40]

However, the rightsholder will primarily be interested in calling the infringer to account under the civil law, for which they will need the personal data behind the IP address (essentially the name and home address). Assistance is provided here by the right to request information from the intermediary enshrined in Article 8(3) of the Copyright Directive 2001/29/EC and Article 8 of the Enforcement Directive 2004/48/EC. Without this right of information, the rightsholder has no option but to initiate criminal proceedings "against person or persons unknown". As a result of its right to the provision of information in criminal proceedings, the investigating authority can then obtain the details of the infringer's identity from the intermediary.[41] Finally, the rightsholder could discover that identity as a result of the right to consult the investigating authority's case files. The right to obtain information directly from the intermediary shortens this uncertain and laborious procedure.

---

36) This presupposes that the user does not employ any identity-concealing measures such as so-called Tor software or proxy servers.
37) See II.3.1 above.
38) In order to clarify the conditions for establishing that involvement, toleration or encouragement, the EU plans to revise Article 14 of the E-Commerce Directive. The consultation on this ended on 11 September 2012, www.ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm
39) See Article 13 of the Enforcement Directive 2004/48/EC.
40) See Articles 9 to 11 of the Enforcement Directive 2004/48/EC; e.g., in the form of a block on access to the website concerned. Cf. H. Karl, IRIS 2011-7/8.
41) See Article 15 of the E-Commerce Directive 2000/31/EC.

2.2. Limits to the right of information

However, data protection aspects need to be considered when asserting the right of information. In spite of the (presumed) commission of a copyright infringement, the infringer's identity is protected under data protection law. In this situation, it would be unrealistic to assume that consent would be given to disclosing the identity, so that a special exception that justifies the processing without consent must apply pursuant to Article 7(b) to (d) of the Data Protection Directive 95/46/EC. Article 13(1)(g) states that limits to data protection may be imposed if they are necessary to protect "the rights and freedoms of others". This imprecise wording opens the door to the contradictory provisions of copyright law, so it is always necessary in cases of conflict to balance the interests involved.

Here, an important role is played by the interests of the intermediaries, which first of all see themselves incurring considerable effort and uneconomic costs as a result of the rights to information. This is compounded by the concern that it might jeopardise their subscribers' confidence in being able to use the service anonymously as far as possible, which could then lead to subscriber defections and economic losses. This is why the emphasis in the political discussion about intermediaries' obligations is always on the limitations of liability provided for in the E-Commerce Directive. The greater the risk of intermediaries being held liable, the more difficult it becomes for them to offer low-priced, attractive services. The intermediaries thus form a "third bloc" in the conflict between data protection and copyright.[42]

2.3. The right of information in the case law of the CJEU

Several CJEU judgments illustrate how the Court defines and weights the opposing interests and what criteria it employs to assess the legality of measures taken. Observations indicate that the CJEU increasingly includes the EU's Charter of Fundamental Rights in its examination of a case and strikes a balance between the fundamental rights concerned.

Judgment of 29 January 2008 (Promusicae)

A first CJEU decision involving the family of copyright-motivated directives (Copyright Directive 2001/29/EC, Enforcement Directive 2004/48/EC) and the Privacy and Electronic Communications Directive 2002/58/EC[43] was handed down in the *Promusicae* case.[44] *Promusicae*, a Spanish association of producers of music and audiovisual recordings, demanded from *Telefónica*, a Spanish access provider, the disclosure of the names and addresses of various subscribers who had infringed copyrights via a so-called shared folder using the KaZaA file exchange program. In the light of this request for information, the domestic court asked the CJEU for an interpretation of the above-mentioned directives. The question was whether EU law required member states to provide for an obligation to disclose personal data in civil proceedings aimed at securing effective copyright protection. While EU law expressly provides for a right of information in criminal proceedings, the legal situation in the case of civil proceedings seemed unclear. Based on an overall assessment of

42) Data protection requirements can occasionally also have a negative impact on consumers themselves, who may resist a warning issued by the rightsholder and want to find out in what context their access provider has provided information about them. The German Federal Commissioner for Data Protection and Freedom of Information, for example, has said that an access provider is not obliged to inform its subscribers about the provision of information. In particular, however, in the Commissioner's opinion a provider may not store the information content, so it is not possible to give the subscriber those details when requested to do so. See the Commissioner's 23rd Activity Report 2009–2010, p. 52, available at www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf?__blob=publicationFile

43) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive), OJ L 201 of 31 July 2002, pp. 37-47, last amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on co-operation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337 of 18 December 2009, pp. 11-36.

44) CJEU, Case C-275/06, *Promusicae*, judgment of 29 January 2008, Reports of Cases 2008 I-00271.

these directives, the CJEU ruled that no such requirement existed. Although the member states, pursuant to Article 8(1) of the Enforcement Directive 2004/48/EC, had to ensure that the civil courts *could*, in response to a reasoned and proportionate request by the complainant, order the intermediary to disclose information in proceedings concerning an infringement of copyright, Article 8 contained no general obligation to establish such a right of information. This is because Article 8 is expressly limited in its scope of application by the provisions on data protection.[45] The CJEU made it clear at the same time, however, that the member states are not prohibited from providing for such obligations to disclose information when an appropriate balance is to be found between the various fundamental rights protected by EU law[46] – in this case in particular the right to property and the right to the protection of personal data. However, when it comes to implementing such measures it is clear that the principle of proportionality must be observed.

Decision of 19 February 2009 (LSG)

The CJEU expressed the same opinion about a year later in its decision in the *LSG* case.[47] Those proceedings also concerned the disclosure of usage data by an Internet access provider. In the original proceedings, the Austrian collecting society *Wahrnehmung von Leistungsschutzrechten GmbH* (LSG) requested information from the intermediary *Tele 2 Telecommunication GmbH* on the names and addresses of persons behind dynamic IP addresses by means of which illegal file sharing was carried out. The thrust of the question asked by the Austrian Supreme Court was not the same in this particular case since the court explicitly enquired whether EU law prohibited ordering the disclosure of data in order to bring civil proceedings for copyright infringements. However, as the CJEU had already stated in the aforementioned judgment that EU law did not actually preclude this it was able to deal with this question fairly quickly and simply issued a decision instead of a judgment. Nonetheless, it once again called on member states to observe fundamental rights and other general principles of EU law, especially the principle of proportionality, when establishing a right of information under the civil law.

The principle of proportionality, which is always emphasised but is extremely abstract, does not, however, create a high degree of legal certainty. It is at most permissible to conclude that a right under the civil law to require the access provider to disclose information on a user who systematically commits large-scale breaches of copyright is unlikely to infringe EU law. On the other hand, it is more difficult to argue that the principle of proportionality has been observed when a member state's right of information were to enable the disclosure of the personal data of the user concerned as a result of a single presumed breach of copyright.[48]

Judgment of 19 April 2012 (Bonnier Audio)

The last CJEU judgment on this subject for the time being was in the *Bonnier Audio* case,[49] in which the group of directives to be considered was joined for the first time by the Data Retention Directive (2006/24/EC[50]). The starting-point was the same as in the two previous proceedings: Swedish holders of rights in audio books sent a request for information to an access provider via whose server audio books had allegedly been distributed in breach of copyright. Here, too, the CJEU referred in detail to, and did not deviate from, its previous rulings in the *Promusicae* and *LSG* cases. However, it made it clear that the Data Retention Directive could not be consulted for satisfying rights to information under the civil law.

45) See Article 8(3)(e) of the Enforcement Directive 2004/48/EC.
46) See II.1 above.
47) CJEU, Case C-557/07, LSG, Decision of 19 February 2009, Reports of Cases 2009 I-01227; see also A. Yliniva-Hoffmann, IRIS 2009-9/7.
48) However, the German Federal Court of Justice has affirmed that the principle of proportionality is observed in such a case, Decision of 19 April 2012, Case I ZB 80/11, available at http://lexetius.com/2012,3310
49) CJEU, Case C-461/10, *Bonnier Audio*, judgment of 19 April 2012; see F. Dohmen, IRIS 2012-6/4.
50) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 of 13 April 2006, pp. 54-63.

In order to understand this judgment, it is necessary to be aware of the relationship between the Data Retention Directive 2006/24/EC and the Privacy and Electronic Communications Directive 2002/58/EC. Both deal with the retention of traffic data:[51] on the one hand, the obligation to store data without particular cause for the purpose of investigating, establishing and prosecuting serious criminal offences or of combating terrorism; on the other hand – and in a way as an exception to data protection considerations – the possibility granted to providers of storing data for a limited period, for example for billing purposes. The essence of the *Bonnier Audio* case can therefore be described as follows: data stored in order to comply with an obligation in implementation of the Data Retention Directive must *not* be used to satisfy rights to information under copyright law. This is expressly stated in Article 4, first sentence, of the Data Retention Directive, according to which member states must ensure that data retained in accordance with the Directive are provided only to the competent national *authorities* in specific cases. However, traffic data still legally stored with the provider in implementation of the Directive 2002/58/EC on privacy and electronic communications may be used, but it goes without saying that this must always be in accordance with the principle of proportionality and after striking a balance between the fundamental rights involved.

The key factor, therefore, is whether the national legislature has established an obligation or authorisation to retain data independently of the data retention provisions of Directive 2006/24/EC. Permission to retain data for billing purposes is, for example, granted by Article 6(2) of the Privacy and Electronic Communications Directive 2002/58/EC. This raises the question of what effect is had by the modern form of charging, the so-called flat rate, since it does not require any precise connection data in order for charges to be billed. And even where this is necessary Article 6(2) of the Privacy and Electronic Communications Directive calls for data to be deleted as soon as the demand for payment can be made. Both initially lead to a further reduction in the data available to meet a request for information and therefore to the question of what happens if the access provider nevertheless stores the connection data in breach of the law. Such data cannot be the subject of a right of information either. Accordingly, the Austrian Supreme Court ruled in its decision of 14 July 2009 that data lawfully retained for a legitimate purpose could only be used for that purpose and then had to be deleted.[52] It was, the court said, accordingly unlawful for the access provider to disclose information unless a law expressly provided for an obligation in that connection.

Data can therefore only be used in accordance with the exception provided for by Article 15 of the Privacy and Electronic Communications Directive 2002/58/EC, according to which the confidentiality of data may only be limited if this is proportionate and serves to safeguard national security, defence, public security and the prevention, investigation, and prosecution of criminal offences. This list does not include possible civil claims for damages by the rightsholder. However, the member states are free to create rights to information under the civil law. This is made clear by Article 13(1)(g) of the Data Protection Directive 95/46/EC, which enables the level of data protection to be lowered if that is necessary to protect the rights of others. Article 15 of the Privacy and Electronic Communications Directive 2002/58/EC must therefore be read in conjunction with Article 13(1)(g) of the Data Protection Directive 95/46/EC . The two sets of rules thus permit the scope of the data protection provisions to be limited in favour of the protection of copyrights. The decisive factor is therefore always the national legal order of the member state concerned.

Notwithstanding Article 4, first sentence, of the Data Retention Directive 2006/24/EC, the Austrian Ministry of Justice is, according to media reports, endeavouring to give rightsholders a right

51) Traffic data are, according to Article 2(b) of the Privacy and Electronic Communications Directive 2002/58/EC, any data processed for the purpose of the conveyance of a communication on an electronic communications network. In the situation under discussion, it includes for example the information that a certain file was uploaded at a specific time using a specific IP address. However, of interest to rightsholders is always the personal information about the user (also called master data or user data). Only this information enables action to be taken against the user for a copyright infringement.

52) Supreme Court, decision of 14 July 2009. See A. Yliniva-Hoffmann, IRIS 2009-9/7.

of information concerning data stored pursuant to the data retention obligation.[53] This would mean that the retention of traffic data without particular cause, which is a controversial data protection issue, would be extended for the benefit of taking action against copyright infringements. However, that would conflict with Article 4, first sentence, of the Data Retention Directive 2006/24/EC, which provides for stored data to be passed to the competent authorities and, therefore, not to private third parties. The progress of the legislative procedure, which has come to a standstill (probably in the light of the proceedings pending with the CJEU to examine the legality of the Data Retention Directive[54]) remains to be seen.

3. Proportionality of national rights to information

With its judgments in the conflicting areas of data protection and copyright law, the CJEU has always stressed that a proper balance between the opposing fundamental rights must be created. In order to ensure the proportionality of a right of information, member states employ various criteria. Certain preconditions are usually required in order to enforce a right of information from intermediaries contrary to data protection interests.

A frequent precondition for the assertion of a right of information is to be found in the Enforcement Directive 2004/48/EC, Article 8 of which states that the copyright infringement must be on a "commercial scale". Only when the infringer's act is motivated by direct or indirect economic or commercial advantage should it be possible for a right of information to apply, which means that, in particular, acts carried out by the end-consumer in good faith can be ruled out.[55]

This way of thinking is also to be found in national legislation. In Germany the right of information requires that the copyright infringement be on a commercial scale,[56] that the question of proportionality be examined in each individual case and that an application for a court order be made to obtain the information.[57] A similar situation applies in Austria, where, according to the Supreme Court's judgment of 14 July 2009, the right of information[58] does not extend to data that has to be deleted. It also requires a written and sufficiently substantiated entitlement claim, the reason for this being to prevent large numbers of requests being made. This is not unlike the situation in Sweden,[59] where a court order must also be obtained and the applicant must not only provide sufficient justification but also show that the information wanted will make it much easier to bring civil proceedings against the copyright infringement. All the rights to information referred to above have in common the requirement mentioned in respect of Germany that the question of proportionality be examined in each individual case.[60]

4. Intermediaries' obligation to establish filter systems

Friction not only exists between copyright and the protection of personal data in the case of rights to information. National legal orders have created alternative models for the enforcement of copyright law in the online sector. In two proceedings, both brought by the Belgian collecting

53) http://akvorrat.at/Ausweitung_der_Vorratsdatenspeicherung_BMJ_lehnt_Dialog_mit_BuergerInnen_ab.
54) Request for a preliminary ruling from the High Court of Ireland, submitted on 11 June 2012, Case C-293/12, joined for a joint decision with the request for a preliminary ruling from the Austrian Constitutional Court, submitted on 19 December 2012, Case C-594/12.
55) Recital 14 of the Enforcement Directive 2004/48/EC.
56) However, according to the judgment of the Federal Court of Justice of 19 April 2012 (Case I ZB 80/11), it is sufficient when the service used for the activity in breach of copyright is provided by the intermediary on a commercial scale.
57) Section 101 of the German Copyright Act.
58) Section 87b of the Austrian Copyright Act.
59) Section 53c of the *Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk* (Act on Copyright in Literary and Artistic Works).
60) For a detailed discussion on these rules and other corresponding rules in other EU member states, see C. Kuner/C. Burton/J. Hladjk/O. Proust, Study on Online Copyright Enforcement and Data Protection in Selected Member States, November 2009, available at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf

society *Société d'Auteurs Belge – Belgische Auteurs Maatschappij* (SABAM), the CJEU had to rule on the compatibility with EU law of orders to filter content.[61]

The *Scarlet Extended*[62] case was about a court decision to order the general and precautionary obligation of an Internet access provider to install filter systems to prevent copyright infringements committed via peer-to-peer programs with the help of its services. The *Netlog NV*[63] case concerned the obligation of an operator of a social network to prevent its users from sharing musical and audiovisual works on their profile pages.

In both judgments, the CJEU ruled that such obligations would force the companies concerned to install a filter system, which would mean the active monitoring of all the data of each individual user. The Court then cited several fundamental rights that had to be taken into account when enforcing another fundamental right, namely the right to intellectual property (Article 17 of the Charter of Fundamental Rights): for the various service providers, there is some conflict with the protection of freedom to conduct a business (Article 16 of the Charter), while in the case of the users of those services there is interference with their freedom of information (Article 11) and – as already mentioned several times – interference with the right to the protection of personal data (Article 8).

In both cases, the CJEU ruled, after careful consideration, against the collecting society, stating that a general obligation to monitor information transmitted with no reference to specific content was no longer compatible with Article 15 of the E-Commerce Directive 2000/31/EC. It was, it said, not proportionate to force service providers to install a complicated, expensive and permanent filtering system entirely at their own expense. For data protection reasons, users' fundamental rights had to be considered more important, especially in view of the possibility of identifying copyright infringers by establishing and processing IP addresses or gathering information on the user profiles concerned. When filtering systems are installed as a precautionary measure, this systematic analysis of every user's personal data takes place without any concrete evidence of a copyright infringement. Moreover, in the CJEU's view freedom of information is undermined because such a filtering system might not be able to distinguish between lawful and unlawful content and this could lead to the blocking of lawful content – here, one only need think of legal exceptions to copyright such as lawful private copies or public domain or orphan works.

5. Internet access blocks – national provisions

The European Union member states have created further alternatives to the rightsholders' direct right to obtain information from the access provider concerning the infringer's personal data. From the data protection point of view, these models are less intrusive provided that the rightsholder cannot readily access the presumed copyright infringer's personal data. Instead, a system of intermediate steps, which is often referred to by the catchy term "three strikes procedure" and usually provides as a last resort for a temporary Internet access suspension, is employed. Although the processing of personal data may be less extensive, interference with freedom of information and opinion is much more intensive.[64]

5.1. France: HADOPI

Since 2010, France has gone its own separate way with regard to dealing with copyright infringements and accordingly exhibits a number of special features. With the establishment of the *Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet* (High Authority

61) See on this the detailed discussion by C. Angelopoulos, *Filtering the Internet for Copyrighted Content in Europe*, IRIS *plus* 2009-4.
62) CJEU, Case C-70/10, *Scarlet Extended*, judgment of 24 November 2011; see C. Angelopoulos, IRIS 2011-6/2; IRIS 2012-1/2.
63) CJEU, Case C-360/10, *Netlog NV*, judgment of 16 February 2012; see K. Breemen, IRIS 2012-3/3.
64) A critical position is held for example by the Organisation for Security and Co-operation in Europe (OSCE). See M. Stone, IRIS 2012-2/1.

for the Distribution of Works and the Protection of Rights on the Internet – HADOPI) it has set up a separate body with around 60 staff who are responsible for pursuing breaches of copyright on the Internet.[65] It becomes involved either when contacted by a rightsholder (usually organisations that represent professional interests, collecting societies such as the *Société des Auteurs, Compositeurs et* Éditeurs *de Musique* [SACEM] or the *Centre national de la cinématographie*) or when asked to do so by the Public Prosecutor's Office. The rightsholder informs HADOPI about the time of the copyright infringement, the IP address used, the copyright-protected works and the name of the Internet access provider. HADOPI can then ask the access provider to let it have the personal data of the user linked to the IP address (name, telephone number, e-mail and postal address).

Initially, the presumed copyright infringer receives an e-mail asking them to comment on the allegation. The second step is to send a registered letter. If HADOPI comes across the same infringer a third time, it can institute simplified legal proceedings that provide for penalties such as fines. In the first three years of its existence, there was also provision for a sanction in the form of a – much criticised – temporary Internet access suspension. Having previously been the subject of legal disputes, that possibility was rescinded on 9 July 2013, not least as a result of the change of government that had taken place in the meantime in France.[66] The *Conseil constitutionnel* (Constitutional Council) declared HADOPI's original power to impose Internet access suspensions itself unconstitutional and revoked it.[67] The legislature subsequently amended the law, which now requires HADOPI to apply to a court in order to impose an access suspension.[68] However, in the entire period in which it was legally possible to impose an Internet suspension this was only done once.[69] In addition, some access providers initially expressed reservations about sending out HADOPI's warning e-mails and refused to forward them to the users concerned. The French legislature responded accordingly and created a statutory obligation to forward the e-mails. If the access provider fails to comply, it faces a fine of EUR 1 500.[70]

With regard to data protection requirements, French law provides that personal data may only be communicated to the *Commission de protection des droits* (Rights Protection Committee), the HADOPI body that examines the applications made by rightsholders. The HADOPI procedure thus proves, at least from the data protection point of view, to be more moderate than a general right to obtain information from intermediaries since the personal information is initially only available to part of a state authority. In the case of the model involving a direct right to obtain information from the access provider, every private rightsholder potentially has access to the end-user's personal information. If the rightsholder is able to do so, it is uncertain what further use they will make of it. The HADOPI method initially leaves the personal data in the hands of a state authority, which processes them in an institutionalised procedure. That method, which has been severely criticised from many points of view, is therefore more data protection friendly than the establishment of a direct right to obtain information, especially as HADOPI is legally obliged to delete the data within specific time-limits.[71]

65) A. Blocman, IRIS 2010-9/24.
66) Décret nº 2013-596 du 8 juillet 2013 supprimant la peine contraventionelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du code de la propriété intellectuelle; available at http://de.scribd.com/doc/152648389/joe-20130709-0157-0060.
67) Judgment 2009-580 DC of 10 June 2009; see A. Blocman, IRIS 2009-7/20; see also IRIS 2010-9/24.
68) The *Conseil d'Etat* (Council of State) infers the necessity of a court order from Article 6 ECHR (right to a fair trial), which requires that judicial proceedings be held whenever any type of sanction may be imposed. When HADOPI contacts the judicial authorities to report a copyright infringement, this cannot yet be regarded as a sanction or as an accusation but the latter is definitely the case when it comes to the imposition of an access suspension. The decision of 19 October 2011 is available in French at www.conseil-etat.fr/fr/communiques-de-presse/decrets_hadopi.html. See also A. Blocman, IRIS 2011-10/15.
69) According to media reports on the subject.
See www.pcinpact.com/news/80487-hadopi-600-d-amende-et-quinze-jours-suspension-pour-abonne.htm
70) A. Blocman, IRIS 2010-10/30.
71) Two months after the report by a rightsholder, etc., when no warning is issued. In the case of a first warning: after 14 months when no second warning is issued. In the case of a second warning: 20 months provided that no new copyright infringements are committed.

Although HADOPI is due to be wound up following criticism of its inefficient working methods, the procedure is to be retained and transferred with slight changes to the media regulator *Conseil supérieur de l'audiovisuel* (CSA).[72]

At the level of EU law, similar ideas are to be found in the European Parliament's so-called Gallo Report,[73] in which stiff penalties are demanded for copyright infringements in the online sector since civil claims for damages are considered not to be effective.[74] The report nonetheless emphasises the particular importance of data protection, which, it says, must be taken into account in the establishment of sanctions.

5.2. United Kingdom: Digital Economy Act

A similar model as in France is also employed in the United Kingdom. For example, sections 124A-124N of the Communications Act 2003 (inserted by the Digital Economy Act 2010) provide for an extensive procedure that enables rightsholders to inform Internet access providers that have signed an "Initial Obligations Code" to be drawn up by the British regulator Office of Communications (Ofcom)[75] about copyright infringements and to instruct them to notify their subscribers. Once the reports on a specific user reach a minimum figure to be laid down in the Initial Obligations Code, Internet access providers will be obliged to put them on an anonymised copyright infringement list.[76] On request, the list or parts of it must be given to the rightsholders in an anonymous form that ensures compliance with data protection legislation.

On the basis of this list, rightsholders can, by applying for a court order, demand the disclosure of the personal information concerned in order subsequently to bring an action for damages against the copyright infringer. According to sections 33 to 35 of the Explanatory Notes, the Secretary of State can provide for access providers to be obliged to implement additional technical measures if the list procedure (alone) proves insufficient.[77] Here, Internet blocks in the form of bandwidth capping or a temporary suspension are expressly considered.

The two British access providers British Telecommunications Plc and TalkTalk Telecom Group Plc took legal action against these provisions and claimed extensive breaches of EU law.[78] *Inter alia*, they maintained that the Digital Economy Act was incompatible with the Privacy and Electronic Communications Directive 2002/58/EC. The England and Wales High Court (Administrative Court) ruled in its judgment of 20 April 2011 that there was no such breach of data protection law as any processing of personal data would be done for the establishment of legal claims and for promoting the right to property and served to pursue a legitimate interest (in this case the rightsholder's economic interests). The processing of the data was thus covered by Article 7(c), (e) and (f) and Articles 8 and 15 of the Data Protection Directive 95/46/EC.

The court also rejected the claim that Article 12 of the E-Commerce Directive 2000/31/EC had been breached, stating that the access providers would not be liable on the basis of the contested provisions but would only document breaches of the law and provide rightsholders with information. Nor was there a breach of the ban contained in Article 15 of the E-Commerce Directive on obliging

72) A. Blocman, IRIS 2013-6/19.
73) Resolution of the European Parliament of 22 September 2010 on the enforcement of intellectual property rights in the internal market (2009/2178(INI)); available at www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2010-0340+0+DOC+PDF+V0//EN
74) The failed proposal of 12 July 2005 for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights, COM(2005)276 final, was along similar lines. The proposal is available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0276%2801%29:EN:HTML
75) Ofcom published a draft of this code in June 2012 and at the same time launched a one-month consultation (available at http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf). The code has not yet been finally adopted.
76) Sections 124A-124N of the Communications Act 2003.
77) The Explanatory Notes on the Digital Economy Act 2010 are available at www.legislation.gov.uk/ukpga/2010/24/notes/contents?view=plain
78) See on this T. Prosser, IRIS 2011-6/20.

providers to monitor information transmitted since the activity was not monitored by the access providers themselves, which only documented the rightsholders' applications. The claimants were also unsuccessful in the appeal proceedings before the England and Wales Court of Appeal (Civil Division), which in its decision of 6 March 2012 essentially agreed with the arguments of the court below.[79]

The High Court also conducted a detailed examination of the question of fundamental rights but ruled that the Digital Economy Act did not impose an excessive limitation on the right to the protection of personal data since the conflicting right to property also had to be protected. Nor was it possible to discern an equally effective measure for the protection of intellectual property in the online sector that would be less intrusive. The design of the Digital Economy Act was therefore proportionate.

Like the HADOPI model, this system also has the advantage from the data protection point of view that the (presumed) copyright infringer's personal data initially do not find their way into the hands of private third parties. The British system even goes so far as to ensure that the data are not even disclosed to an authority. The access provider merely produces documentation in an anonymised form, and the rightsholder can only access the personal information behind the IP addresses in the course of legal proceedings. In addition, the procedure for users is transparent because they are informed about it as soon as the access provider issues the first report.

5.3. Ireland: Self-regulation

Ireland employs a model for involving intermediaries in dealing with copyright infringements that is comparatively independent of the government. The biggest Irish telecommunications company Eircom and Irish representatives of the four major record labels EMI, Sony, Universal and Warner have agreed a "three-strikes protocol" as a result of a legal dispute on the disclosure of customer data.[80] This is not based on legal provisions but only on an agreement between the parties.[81]

According to the agreement, Eircom adopts a three-stage approach towards its subscribers. After the first copyright infringement, the subscriber receives a notice from Eircom. On a second infringement they receive a warning threatening disconnection from the Internet, and on a third infringement the threat is carried out.[82] The Irish Data Protection Commissioner became involved and expressed misgivings with regard to Articles 8 and 6 ECHR. His first objection was that the handling of personal information associated with the three-strikes model breached the subscribers' privacy. Furthermore, the possibility of a fair trial was circumvented when the commission of the criminal offence of a copyright infringement was established without the involvement of a court and a punishment then imposed. However, the courts rejected these objections.[83] Copyright is protected by the Irish Constitution and deserves that protection. The main emphasis in the proceedings was on procedural matters, so the courts were called upon to a comparatively limited extent to consider the relationship between copyright and data protection law. On the other hand, in the Irish situation the legal issues involved should be seen more in the context of the restriction of freedom of information: the suspensions of Internet access are imposed without a legal basis or the involvement of a government authority.

79) T. Prosser, IRIS 2012-5/22.
80) M. McGonagle, IRIS 2006-4/26.
81) The Irish model thus proves to be innovative within the meaning of the Communication from the Commission "Enhancing the enforcement of intellectual property rights in the internal market", of 11 September 2009, COM(2009) 467 final, with which the Commission calls on the opposing interest groups to find practical solutions by making voluntary arrangements in order to bring about a balance between copyright and the protection of personal data, despite the fact that the subscribers themselves could not be involved in drawing up the agreement.
82) M. McGonagle, IRIS 2010-6/34.
83) M. McGonagle, IRIS 2012-8/29; recently confirmed by the Irish Supreme Court in a decision of 3 July 2013, available at www.supremecourt.ie/Judgments.nsf/1b0757edc371032e802572ea0061450e/c9861b9cda79509b80257b9d004e9a7a?OpenDocument

5.4. Spain: Ley Sinde

An entirely different model has been introduced in Spain, where suspensions of Internet access are directed less against the final user than the platform with the help of which the copyright infringements are committed.[84]

The so-called *Ley Sinde* (Sinde Act)[85] has created a procedure whereby rightsholders can report Internet platforms with the help of which copyrights are infringed, especially so-called peer-to-peer networks. A government commission then examines possible action that may be taken against the platform operators. If the commission considers the complaint justified, it will refer the proceedings to a court, which can order the suspension of the website concerned.

In comparison to the national measures described, the Spanish variant is, from the end-user's point of view, no doubt the least intrusive form of intervention under data protection law when it comes to safeguarding copyrights. The sanctions provided for here are initially only directed against the Internet service provider. Preventive measures such as blocking a website naturally involve less interference for the end-user as no personal data are collected in the light of an actual infringement. Nonetheless – as is always the case with such preventive measures – the users' freedom of information and opinion and the interests of the intermediaries are affected.

6. Problems involved when a service is used against payment

The cases described so far have always involved the use of a service in breach of copyright and the subsequent assertion of any claims for damages. However, a conflict between data protection and copyright may also occur when a service is used legally. For example, data protection law requires that a video-on-demand provider shall only gather and use data in connection with its service if this is *necessary* for the performance of a contract.[86] Not required are details of the individual's gender, academic degree, telephone number, etc. The provision of further details is possible, but only with the user's consent.[87] However, data protection law prohibits making access to a service dependent on consenting to the collection and processing of certain data. So-called online profiling, which involves cookies being used to record the behaviour of users in order to present them with offers tailored to their personal needs, must be seen as another critical area from the data protection point of view. The Copyright Directive 2001/29/EC sees such information systems as an opportunity for the modern management of copyrights[88] but calls for respect for the end-user's privacy, within the meaning of the Data Protection Directive 95/46/EC, when such systems are employed.

A high level of data protection is extremely important for the consumer, and therefore for the legal exploitation of copyrights in the online sector. A study carried out by IBM revealed that 41% of Internet users in the United Kingdom and 56% in Germany decide not to acquire a product when they are uncertain about the use of their personal data.[89] A data protection friendly offering may in this respect prove to be a driving force for online exploitation.

84) P. Letai, IRIS 2012-7/18; 2012-4/22; 2012-2/18.
85) *Real Decreto 1889/2011, de 30 de diciembre, por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual* (Royal Decree 1889/2011 of 30 December 2011 regulating the Intellectual Property Commission).
86) See Article 7(b) of the Data Protection Directive 95/46/EC and Article 6(1)(b) of the General Data Protection Regulation.
87) This is why a distinction is often made between mandatory fields and voluntary additional information when registering with Internet service providers.
88) Recital 57 of the Copyright Directive 2001/29/EC.
89) IBM Multi-National Consumer Privacy Survey, 1999, p. 27, available at ftp://www6.software.ibm.com/software/security/privacy_survey_oct991.pdf

IV. Conclusion

With its three key judgments on the relationship between copyright law and data protection law (*Promusicae*, *LSG* and *Bonnier Audio*), the CJEU has devoted its attention to the copyright interests of rightsholders and the data protection interests of users. As far as rights to information are concerned, the sweeping reference to the significance of the principle of proportionality does not permit very much to be gathered from the judgments in terms of tangible criteria. It can only be said at this moment in time that the application of data protection law enjoys precedence over the copyright directives and the disclosure of data and the creation of a right of information permissible under EU law are ultimately always based on striking a balance between the opposing fundamental rights, that is to say the right to property on the one hand and the right to the protection of personal data on the other. The CJEU has not created any concrete guidelines for this balancing exercise with any of its judgments in this particular area. Furthermore, it remains an open question as to how the abstractly worded right of information in EU law (Article 8 of the Enforcement Directive 2004/48/EC and Article 8 of the Copyright Directive 2001/29/EC) is actually to be enforced without disregarding the provisions of the Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC and the limitations on liability in the E-Commerce Directive 2000/31/EC.

The Belgian law firm Hunton & Williams established in the study it produced on behalf of the European Commission's Internal Market and Services Directorate General that in many respects no answers have been provided to these questions either at European or national level, with the result that there is very little harmonisation of the right to obtain information from intermediaries in the case of copyright infringements.[90] There is currently no evidence that the EU is seeking further harmonisation in this area. Although extensive efforts at reform are to be expected with the drafts of a General Data Protection Regulation and the proposal for a directive on collecting societies,[91] these reforms seem so far to be disregarding the conflict between copyright law and data protection law and, in particular, do not clarify any details regarding the question of rightsholders' rights to request information from intermediaries.[92]

The alternative to rights to information, namely the possibility of filtering systems and, in particular, Internet suspensions, sometimes seem less intrusive from the data protection point of view but they do cause significant interference with other rights of both users and intermediaries. The member states are already planning different approaches and it remains to be seen whether one system – and, if so, which– will ultimately be adopted for the assertion of copyrights in the online sector.

90) C. Kuner/C. Burton/J. Hladjk/O. Proust, Study on Online Copyright Enforcement and Data Protection in Selected Member States, November 2009, available at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf

91) Proposal for a Directive of the European Parliament and of the Council on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online uses in the internal market, of 11 July 2012, COM(2012) 372 final.

92) Instead, new areas of conflict are emerging. By way of example, reference may be made to the automated monitoring of licensed copyright protected works (see Recital 27 and Articles 22 ff. of the proposal for a directive on collecting societies).

IRIS plus
2013-6 p.27

Recent case law

As we have observed, the relationship between copyright, freedom of expression and privacy is of such a conflicting nature that it is often difficult to know when one right should prevail against the other. In such cases, courts have to take up the scalpel in order to finely dissect complex legal and technological issues before deciding who is right. This section gives you an overview of recent cases decided by national courts concerning, among others, such famous Internet services as the Pirate Bay, VKontakte, YouTube or Rapidshare. These decisions show not only how complex the matter at stake is, but also how these cases are not only decided on a case by case but also on a country by country basis.

Germany

Federal Supreme Court Clarifies Monitoring Obligations of *Rapidshare* File-Hosting Service

Christian Lewke
Institute of European Media Law (EMR), Saarbrücken/Brussels

In a decision of 15 August 2013, the *Bundesgerichtshof* (Federal Supreme Court - BGH) further clarified the extent of the duty of care of a file-hosting service provider and, in addition to the liability privileges enshrined in Articles 7(2) and 10 of the *Telemediengesetz* (Telemedia Act - TMG) and Articles 14(1) and 15(1) of the E-Commerce Directive (2000/31/EC), demanded that hosting service providers be subject to a partly-proactive monitoring obligation.

The ruling follows an action brought by the *Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte* (Society for musical performing and mechanical reproduction rights - GEMA) against the *Rapidshare* file-hosting service. Although the GEMA had issued a caution about a large number of music titles stored by *Rapidshare*, the provider had not completely removed them.

In its ruling, the BGH firstly confirmed its previous case law: in accordance with Article 7(2) TMG, the service provider did not have a general obligation to monitor data that it merely stored. However, depending on the circumstances of the individual case, a monitoring obligation might apply.

Service providers who stored information provided by users had a duty of care to take reasonable measures to identify certain types of illegal activities.

In this case, *Rapidshare's* business model had not been designed from the outset to facilitate infringements of the law, since the service could also be used for lawful purposes. It could not therefore be expected to monitor everything without specific cause.

However, for a number of reasons, the service provider was obliged to monitor stored data once it had been cautioned about an infringement of the law, since *Rapidshare*, through its own activities, was increasing the risk of its service being used illegally. For example, the claim that certain files had been downloaded 100,000 times, which *Rapidshare* used to advertise its hosting service, was only possible if the content concerned was highly attractive and illegal. The fact that the service could be used anonymously made it even more appealing for illegal use. The additional awarding of points to users, depending on the number of downloads, could also be seen as further evidence that mass infringements were being promoted.

It was therefore necessary to consider the extent to which the file-hosting provider was required to monitor content when asked to do so. In previous case law, the BGH had noted that, in principle, the service provider should be expected to monitor a reasonable number of relevant collections of links to certain designated content. In the instant case the BGH also explained that, with a large number of over 4,800 musical works, the hosting provider should be expected to regularly monitor collections of links. In this respect, a hosting provider could be required to use a word filter, at least.

Rapidshare was also obliged to find out about other illegal links via general search engines. The reference to general preventive measures that had been taken (17-person "abuse team", MD5 filter, deletion interfaces for rightsholders) could not, on its own, exonerate the defendant.

- *Urteil des BGH vom 15. August 2013 (Az. I ZR 79/12)* (BGH ruling of 15 August 2013 (case no. I ZR 79/12))
  http://merlin.obs.coe.int/redirect.php?id=16700

IRIS 2013-9/9

OLG Prohibits Rapidshare from Making Available Certain Content

Tobias Raab
Institute of European Media Law (EMR), Saarbrücken/Brussels

In two rulings of 14 March 2012, the *Hanseatisches Oberlandesgericht* (Hanseatic Appeals Court - OLG) prohibited the file-hosting site Rapidshare from making certain copyrighted content available to its users.

The judges therefore upheld the decision of the *Landgericht Hamburg* (Hamburg District Court - LG), which, in lower-instance judgments, had granted the request of the publishers Campus and De Gruyter and agreed with the legal opinion of the GEMA collecting society concerning Rapidshare's liability and obligations. Therefore Rapidshare is prohibited from making available the aforementioned publishers' literary works and music from the GEMA repertoire.

In order to establish disturbance liability, it was necessary in this case to consider the extent to which Rapidshare was liable for misuse of its service and whether it therefore played an "active role" or merely the role of a "neutral go-between". In this regard, the court ruled firstly that Rapidshare had, through its basic business model, tended to influence its users in such a way that they had committed offences and was therefore liable for the provision of storage space and the allocation of links. Without this, subsequent breaches of copyright would have been impossible. In addition, the measures previously taken to combat illegal use were inadequate. It was not sufficient just to take action against breaches of copyright and delete links after being notified by the copyright holders. If an illegal link was reported, it was also necessary to look for and monitor the link's "surroundings", including all related websites and similar links. Rapidshare should also keep an eye on current developments in order to fulfil its obligation to observe the market, and should not limit itself to known lists of links. This was the only way of effectively preventing the repetition of copyright infringements. Since Rapidshare had failed to meet these obligations, the OLG upheld the lower-instance rulings and prohibited the file-hosting site from making the relevant content available.

Nevertheless, the judges deviated from their previous case law in two respects. For example, they altered their view that a breach of copyright occurred at the point of uploading, since in the era of cloud computing such services were increasingly being used to store authorised copies. Since, in the period between the complaints being filed and the OLG's decision, Rapidshare had increasingly been describing itself as a "largely neutral provider" of serious cloud computing services, the previous accusations that it had tended to influence its customers in such a way that they acted illegally no longer applied. Even so, Rapidshare could still have disturbance liability despite these changes, although no longer on the basis of a tendency to influence users. Rather, such liability could now be based on the fact that Rapidshare enabled customers to use its services anonymously and, in this way, "actively" helped them to infringe copyright. Rapidshare could not justify its actions with reference to Article 13(6) of the *Telemediengesetz* (Telemedia Act - TMG), under which users must be able to use a provider's services anonymously or under a pseudonym. The TMG only allowed this "where this is technically possible and reasonable", which "in view of the dangers posed by the defendant's business model is clearly not the case here". Disturbance liability might therefore still apply in the future.

- *Pressemitteilung des Hanseatichen Oberlandesgerichts zum Urteil (Az. 5 U 87/09), 15. März 2012* (Press release of the Hanseatiches Oberlandesgericht on the ruling (case no. 5 U 87/09), 15 March 2012)
  http://merlin.obs.coe.int/redirect.php?id=15787

IRIS 2012-5/12

OLG Rejects Claim against YouTube for Disclosure of User Data

Anne Yliniva-Hoffmann
Institute of European Media Law (EMR), Saarbrücken/Brussels

According to media reports, the *Oberlandesgericht München* (Munich Appeal Court - OLG) decided in an urgent procedure on 17 November 2011 that YouTube was not obliged to disclose data identifying a user who had uploaded copyrighted material to the copyright holder.

In the case at hand, a YouTube user had published film material, which he had obviously created by filming a cinema screen, on the video portal. The film distributor concerned claimed that this breached its rights and demanded that YouTube remove the material and provide it with information about the user's identity. YouTube immediately complied with the first request, but refused to disclose the user data.

The *OLG München* has now also rejected the data request, confirming the decision of the lower-instance court. Although it was true that copyright had been breached, the commercial nature of the unlawful action required under Article 101 of the *Urheberrechtsgesetz* (Copyright Act) to justify the disclosure of information was not apparent in this case. The relevant information provided by the claimant was insufficient and there was, in particular, no evidence that the user had intended to profit financially from his actions.

According to reports, the film distributor is considering pursuing its claim in the main proceedings.

• *Beschluss des Oberlandesgericht München vom 17. November 2011 (Az. 29 U 3496/11)* (Decision of the Munich Appeal Court of 17 November 2011 (case no. 29 U 3496/11))

IRIS 2012-1/21

Finland

ISP not Granted Leave to Appeal in The Pirate Bay Case

Anette Alén-Savikko
Institute of International Economic Law/University of Helsinki, Facing the Coordination Challenge/Communication Research Centre, University of Helsinki

On 29 October 2012, the Supreme Court of Finland did not grant the telecommunications and ICT service provider Elisa Corporation leave to appeal in the case concerning The Pirate Bay (TPB). In the aftermath of the Swedish TPB case, an interim injunction was sought against Elisa in May 2011. The Copyright Information and Anti-Piracy Center (CIAPC) filed the application on behalf of the Finnish National Group of International Federation of the Phonographic Industry (IFPI). The aim was to prevent the continuance of copyright infringements.

The application was based on Section 60c of the Finnish Copyright Act (404/1961): According to paragraph 1, a court may, in trying a case and upon request of a rightsholder, order an intermediary to discontinue the making available of allegedly copyright-infringing material to the public (injunction to discontinue). It is to be regarded reasonable in view of the rights of the alleged infringer, the intermediary, and the author. Paragraph 2 provides for the situation where legal action against the alleged infringer (ref. in §60b) is not yet taken. Then, a court may issue an interim injunction. It may be issued without hearing the alleged infringer if deemed necessary for

the urgency of the case. The injunction remains in force until further notice. The alleged infringer shall be reserved an opportunity to be heard without delay and the court shall decide whether the injunction remains in force or is cancelled. (Para. 3) The injunction shall not prejudice the right of a third person to send and receive messages. It shall enter into force when the applicant provides the security to the execution officer. The interim injunction shall expire if a legal action has not been taken within one month from its issuing. (Para. 4)

On 26 October 2011, the Helsinki District Court ruled in favor of IFPI Finland. An interim injunction was issued and Elisa was obliged under the penalty of a fine (EUR 100,000) to remove TPB domains from its servers and to block access to IP-addresses used by TPB. The measures regarding subscriptions were taken in January 2012 following the enforcement order. Elisa appealed the ruling of the district court, but on 15 June 2012, the Helsinki Court of Appeal did not alter the decision. An interim injunction was found necessary in the view of the evidence on the effectiveness of legal measures and the accessibility of the alleged infringer. The court also stated that the interim injunction may become long term if the defendants in the main issue cannot be summoned. That however does not per se render it unlimited in duration. Elisa finally requested leave to appeal to the Supreme Court to obtain a judicial precedent, but it was not granted.

- *Helsingin käräjäoikeuden päätös, 26/10/2011, No 41552* (Decision of the District Court of Helsinki, 26 October 2011, No 41552)
  http://merlin.obs.coe.int/redirect.php?id=16227

- *Helsingin hovioikeuden päätös, 15/06/2012, No 1687* (Decision of the Court of Appeal of Helsinki, 15 June 2012, No 1687)

- *Korkeimman oikeuden päätös, 29/10/2012, No 2187* (Decision of the Supreme Court, 29 October 2012, No 2187)

IRIS 2013-1/18

France

Absence of Liability on the Part of an Internet Site Offering Access to Catch-up TV Programmes via Deep Hypertext Links

Amélie Blocman
Légipresse

In a decision delivered on 31 October 2012 the Court of Cassation rejected the appeal by the M6 group against the decision of the court of appeal rejecting all its applications in its dispute with the company that operates the TV-replay.fr site, which is an on-line guide to catch-up TV sites (see IRIS 2011-6/17). The M6 group, which operates a number of channels including M6 and W9 and their catch-up TV services M6replay and W9replay, complained that TV-replay.fr was giving direct access to its programmes by means of deep hypertext links without first directing viewers to the home pages of M6replay and W9replay. M6 claimed this violated the general conditions for using its catch-up TV services and infringed its rights as the originator and producer of a database, and felt that the behaviour of TV-replay.fr constituted unfair competition and free-riding.

The Court of Cassation firstly approved the court of appeal's acceptance that merely putting on-line the general conditions for using the M6 and W9 sites, which could be accessed by means of a half-concealed tab in the lower part of the screen, was not enough to place the users of the services offered under contractual obligation, and that the letter of formal notice the M6 group had sent to the defendant company, which edited the TV-replay.fr site, requiring it to observe the

general conditions for use did not give rise to any contractual obligation on the part of the latter to comply with them.

The Court of Cassation also found that the court of appeal had been right to state that the M6 group's production companies, which held the rights for the programmes broadcast, could not collectively claim the infringement of undifferentiated rights, and that they did not establish which of them held the rights for the works the defendant company was making accessible on its TV-replay.fr site after they had been broadcast on television. The Court also rejected the argument of infringement of the rights of the M6 group in its capacity as producer of databases. Lastly, the decision notes that users of the disputed site were directed to the programme sought, which was presented in a navigation window on the channels' catch-up TV sites giving access to all the functions of the sites and to their advertising banners. The court of appeal found that the complaint, based on the circumvention of the normal navigation process, was unfounded and that no proof of any free-riding activity had been provided, and used this as the legal grounds for justifying its decision. The Court of Cassation's decision puts an end to the dispute, which nevertheless raises the question of the means available to rightsholders to oppose access to their content via hypertext links.

• *Cour de cassation (1re ch. civ.), 31 octobre 2012 - Société Métropole Télévision* (Court of Cassation (1st civil chamber), 31 October 2012 - the company Métropole Télévision)

IRIS 2013-1/19

Court of Cassation Recalls that there is no General Obligation to Supervise the Network

Amélie Blocman
Légipresse

On 12 July 2012, the first civil chamber of the Court of Cassation delivered three important judgments, overturning the judgment of the court of appeal in Paris which had found that Google Images and Google Vidéo had not taken the necessary steps to make it impossible to put images and films that infringed copyright back on line. The Court of Cassation held that this was tantamount to requiring Google to observe a general obligation of supervision and demanding, out of proportion to the desired aim, the setting up of a blocking arrangement for an unlimited period of time.

The Court of Cassation was being called upon to deliberate in disputes between rightsholders (producers of the documentary films *Les Dissimulateurs* and *L'Affaire Clearstream*, and a photographer) and Google, after it had been noted that there were links on a number of sites accessible via Google Images and Google Vidéo that gave Internet users access free of charge to both the full version of the films, either as streaming or to download, and the disputed photograph. The court of appeal had found that, by enabling Internet users to view the disputed videos and photograph that had been put on-line on third-party sites directly on the pages of the sites Google Vidéo France and Google Images, Google was guilty of infringing copyright, for which reparation was required. The court also held that Google had not taken the necessary steps to ensure that it was not possible to put the films and photograph that had already been flagged as illegal back on-line. The company could not therefore claim the limitation of liability provided for in Article 6. I. 2 of the Act of 21 June 2004 and had therefore incurred its liability in this respect. Google contested the court of appeal's decisions, and applied to the Court of Cassation. The Court began by emphasising that Google was using links to the other sites to offer Internet users the possibility of viewing the films on its own Google Vidéo site and the photograph on Google Images. The court of appeal had been right in deducing from this that Google was using an active function that enabled it to capture content stored on third-party sites so that it could be represented directly on its own site, for the use of its own clients. The court of appeal, noting that Google was reproducing the film on its sites in this

way without the authorisation of the rightsholders, which was characteristic of infringement of copyright, found that Google was going beyond the implementation of a straightforward technical function, legally justifying its decision.

The Court of Cassation however then went on to overturn and cancel, in application of provisions I.2, I.5 and I.7 of Article 6 of the LCEN of 21 June 2004, the appeal judgments inasmuch as they refused the benefit of these provisions and stated that the applicant companies had not "adopted the necessary measures for preventing the items being put on line again", regardless of whether the films and the photograph had been accessible from addresses that were different to those indicated in the initial reports. The Court of Cassation held that imposing this decision on Google as the referencing service provider in order to prevent the disputed films and photograph being put on line again, without the company having been sent another proper notification, even though this was required by the Act, was tantamount to subjecting the company "to a general obligation of supervision of the images and films it stored, and an obligation to seek out illegal reproductions, and demanding, out of proportion to the desired aim, that it set up a blocking arrangement for an unlimited period of time."

• *Cour de cassation (1re ch. civ.), 12 juillet 2012 - Google c. Bach Films et a. (3 arrêts)* (Court of Cassation (1st civil chamber), 12 July 2012 - Google v. Bach Films et al. (3 judgments))

IRIS 2012-8/24

All TF1's Complaints against YouTube Rejected

Amélie Blocman
Légipresse

On 29 May 2012, in a judgment running to 34 pages, the regional court in Paris rejected the claims brought by TF1 and its subsidiaries (the channel LCI, TF1 Vidéo and TF1 International, responsible for video editing and acquiring and distributing rights) against YouTube on the grounds of infringement of copyright, unfair competition and parasitic use. In addition to requesting a ban, the channel was also claiming damages - calculated at EUR 150 million - for the prejudice caused by YouTube putting on-line a whole range of films, series, sports events and broadcasts it felt it had rights to, including some prior to any broadcasting or commercial use in France.

The first stage in the proceedings involved the court examining whether the applicant companies had sufficiently and correctly identified the content at issue. It deliberated on this according to the qualities of the said companies and according to the grounds invoked (copyright and neighbouring rights) for each item of content at issue. It found that the applicant parties had not produced proof of the rights they invoked. Thus, contrary to its claims, TF1 Vidéo was not the economic beneficiary of the producers of the videograms at issue since it had only acquired the right to use them and failed to provide proof of the exclusivity it claimed. Similarly, the company TF1 Droits Audiovisuels, depending on the works involved, either did not establish its qualification as the producer of an audiovisual work or a videogram, or did not provide proof that it had reached an agreement with the other co-producers or had their authorisation to act alone. The applications brought by these two companies were therefore inadmissible. Concerning the channels TF1 and LCI themselves, as they were audiovisual communication companies, reproducing their programmes and making them available to the public were subject to their authorisation, in accordance with Article 216-1 of the Intellectual Property Code (CPI). The court recalled however that there was no presumption of ownership of rights as required in order to be able to benefit from this protection. It was for the party claiming it to demonstrate the existence of the programme and the proof that it had been broadcast before it was allegedly shown again on YouTube. In the present case, the court deemed the documents produced in favour of the channels (programme schedules, press files, etc.) insufficient, and the claims brought by the channels on the basis of Article L. 216-1 of the CPI

were declared inadmissible except for seven sports events for which the required elements of proof had been produced. Similarly, on the grounds of copyright, the channels did not provide proof of the originality of the programmes (including the television news) they claimed YouTube should not have put on-line.

Once the ownership of the rights had been examined, the court turned to the status of the video sharing platform. In a manner that has now become classic, the applicant parties claimed that the status of editor should apply to the platform, since it played an active part in users putting content on-line. YouTube claimed the status of host, within the meaning of Article 6-1-2 of the Act of 21 June 2004 (LCEN). In rejecting the claims brought by TF1 and LCI, and upholding YouTube's status as a host, the court recalled the provisions of the LCEN and the position adopted by the Court of Cassation in line with that of the CJEU, examined the conditions for using the service that were in force at the time proceedings were initiated, and recalled that hosts were within their rights to make use of advertising; doing so did not deprive them of their status. In application of Articles 6 and 7 of the LCEN, the court went on to examine the case brought against YouTube in its capacity as host and recalled the requirement to withdraw disputed content promptly once this has been notified. In the present case, the court found that YouTube had taken too long, taking five days "at best" to remove the videos of the seven sports events at issue, which "could not be qualified as reasonable" and was therefore at fault. In a final observation on this point, however, the court noted that in any event the conditions set out in Article L. 216-1 of the CPI were not met for noting fault on the part of YouTube, since the condition regarding payment of an entrance charge was not met, because no charge was made for accessing the site. In conclusion, the court observed that YouTube had concluded an agreement with TF1 on 16 December 2011 that permitted it access to the "Content ID" service which allowed rightsholders, once content had been notified, to achieve the definitive withdrawal of a video notified as being disputed. The applicants had not noted any infringement since that date. Did that mean the dispute was actually over? There is still the possibility of an appeal…

• *TGI de Paris (3e ch. 1re sect.), 29 mai 2012 - TF1, LCI et autres c/ Youtube* (Regional court in Paris (3rd chamber, 1st section), 29 May 2012 - TF1, LCI et al. v. YouTube)
http://merlin.obs.coe.int/redirect.php?id=15997

IRIS 2012-7/22

Penalty for Film on Video Platform Infringing Copyright

Amélie Blocman
Légipresse

On 9 May 2012, the court of appeal in Paris delivered its decision in the dispute between the producers of the film *Sheitan* and the video-sharing platform Dailymotion regarding five videos, corresponding to the entire film divided into five parts, that could be viewed on the platform using streaming despite an order issued by the regional court in Paris demanding communication of data allowing identification of the person who had broken the law by putting the videos on-line.

On 11 June 2010, the regional court in Paris had found the platform guilty of infringing copyright and had fined it EUR 15,000 in damages (see IRIS 2010-7/19), after noting its status as a host, which the film's producers refused to accept. The court did not however accept the company's argument that it was covered by the limited liability scheme instituted by Article 6-I-2 of the Act of 21 June 2004 (LCEN), since it had not "promptly" withdrawn the disputed content when it was reported by the producers. It should be recalled that according to this text the liability of natural or legal persons whose activity includes storing content may only be invoked "if (…) as soon as they have knowledge of the unlawful nature of stored content they take prompt action to withdraw the data or bar access to it". The platform had appealed against the conviction. In its decision on 9 May 2012, the court noted that, contrary to the initial proceedings, and in the light of jurisprudence

that was now well established, the parties were agreed in considering that Dailymotion met this definition of a host, since it provided the public with a service for storing audiovisual content (in the present case, personal programmes) supplied by the persons using the service, without being able to select the content. The parties therefore agreed that Dailymotion's liability was indeed incurred in the light of the provisions laid down specifically in the LCEN regarding the place where storage was provided. They did not agree, however, on whether the platform had fulfilled its obligations with regard to its status. Recalling these obligations, the court was to deal with the case in two stages. Firstly, in accordance with Art. 6-I-2 of the LCEN, it examined whether the platform had been "prompt" in withdrawing the content that infringed intellectual property rights as soon as it had been made aware of its existence. On this point, the court noted that the platform had written to the lawyers of one of the plaintiff production companies on the day the order was notified, providing all the data and statistics concerning the five videos at issue (date they were put on-line, IP address of their initiator and statistics). The decision added that there was therefore no justification in claiming "not without bad faith" that the elements of the order were insufficient to allow it to identify and locate the disputed content. Indeed it had allowed more than three months to pass after the date on which it had knowledge of the disputed content before withdrawing it, thereby failing in the obligation of prompt withdrawal incumbent on a storage provider.

Secondly, the court demonstrated that the platform had failed in its obligation under the LCEN to prevent further access on the host platform to content previously withdrawn. Contrary to Dailymotion's defence claims, the excerpts of the film available on the site after the initial withdrawal could not be considered as different content from the content that had been withdrawn. They therefore constituted a repeat infringement of the intellectual property rights in the same work.

Although the court confirmed Dailymotion's liability, it found that the prejudice suffered by the applicant production companies had been under-estimated in the initial proceedings. Noting that the unlawful content had not been withdrawn until three months after notification, that it had been reinstated after having been withdrawn, and that it had been viewed more than 12,000 times by the time it was withdrawn, the court ordered Dailymotion to pay each of the production companies EUR 30,000 in damages (compared with EUR 15,000 ordered in the initial proceedings).

- *Cour d'appel de Paris (pôle 5, ch. 1), 9 mai 2012 - Dailymotion c. SARL 120 Films et La chauve-souris* (Paris court of appeal (section 5, chamber 1), 9 May 2012 - Dailymotion v. 120 Films Sàrl and La Chauve-Souris)

IRIS 2012-6/17

United Kingdom

High Court Orders Internet Service Providers to Block Access to File-Sharing Sites

Tony Prosser
School of Law, University of Bristol

In its judgment of 28 February 2013, the High Court ordered six leading internet service providers (with a 94% market share of UK internet users) to block access to three peer-to-peer file-sharing websites called KAT, H33T and Fenopy. This follows earlier High Court decisions requiring blocking of other sites (see IRIS 2012-7/25 and IRIS 2011-9/21).

The case was brought by ten leading record companies on their own behalf and on that of other members of the recorded music trade associations. The three websites each operate a substantial profit-making business in file sharing, especially in music. Section 97A of the Copyright, Designs and Patents Act 1988, implementing the Information Society Directive, empowers the Court to

issue an injunction against a service provider 'where that service provider has actual knowledge of another person using their service to infringe copyright'. The Court considered that users of the websites with accounts with the defendants had been engaged in sharing, and so making unlicensed copies of, recordings. This was occurring on a large scale. The material was also communicated to a new public and, although the companies were based outside the UK, the websites were targeted at the UK. The entire purpose of each website was to permit copying. Although statements were made on the sites that their teams were against piracy, these were unconvincing given the quantity of material made available that infringed copyright, their ineffective responses to requests to remove the content and steps they had taken to avoid enforcement measures. Both users and operators of the websites used the service providers' services to infringe copyright, and the providers were notified weekly of infringing activities, thereby showing actual knowledge; indeed, none of the providers denied having such knowledge.

The Court also considered that the orders would be proportionate through balancing the property rights of the claimants against the right to freedom of expression. In this case, the service providers had agreed to the orders and had not sought to resist them on the grounds that they would be unduly burdensome or costly; though they could be circumvented, they could still be justified if they only prevent access by a minority of users. Evidence suggested that such orders are reasonably effective. The orders were narrow and targeted, and were necessary and appropriate to protect intellectual property rights. This clearly outweighed the freedom of expression rights of users who can obtain the material from lawful sources, and of the site operators who were profiting from the infringements.

- Emi Records and others v. British Sky Broadcasting Ltd and others, [2013] EWHC 379 (Ch)
  http://merlin.obs.coe.int/redirect.php?id=16413

IRIS 2013-5/29

High Court Orders Internet Service Providers to Block Access to The Pirate Bay

Tony Prosser
School of Law, University of Bristol

On 2 May 2012, the English High Court made an order under the Copyright, Designs and Patents Act 1988 to require the major internet service providers to block customer access to The Pirate Bay peer-to-peer file sharing website. The Act (as amended) implements the 2001 Information Society Directive 2001/29/EC. The case was brought by record companies on their own behalf and on behalf of the British Recorded Music Industry and Phonographic Performance Ltd.

The Act empowers the High Court to grant an order against a service provider where the latter has 'actual knowledge' of another person using their service to infringe copyright. The court had already made such an order in relation to the website Newzbin2, and in an earlier decision had determined that both the users and operators of The Pirate Bay infringed the copyrights of those seeking the orders (see IRIS 2011-9/21 and IRIS 2012-4/28). In this case, it considered that the ISPs had actual knowledge of the copyright infringement as this had been given to them by the record companies and in the earlier judgment. To grant the order would not be contrary to Art. 10 of the European Convention on Human Rights or Art. 11 of the Charter of Fundamental Rights of the European Union. The orders would represent a proportionate response as their terms had in fact been negotiated between the parties, who were professionally represented, and were proportionate in relation to the users of the ISP services for reasons given in the earlier cases. Thus orders were granted to require IP address blocking, which was feasible as The Pirate Bay did not share an address with anyone else.

• Dramatico Entertainment et al v. Brisith Sky Broadcasting et al, [2012] EWHC 1152 (Ch)
http://merlin.obs.coe.int/redirect.php?id=15944

IRIS 2012-7/25

High Court Orders Internet Service Provider to Hand Over Personal Details of Customers to Pornographic Film Producers Alleging Breach of Copyright

Tony Prosser
School of Law, University of Bristol

The English High Court has ordered the Internet Service Provider O2 to hand over the personal details of over 9,000 customers to a company acting on behalf of copyright owners and to a pornographic film production company, whilst rejecting similar claims by 12 other copyright owners.

Golden Eye International Limited, an organisation acting on behalf of copyright owners, and 13 pornographic film producers sought a 'Norwich Pharmacal Order' to compel O2 to give them the personal details of 9,124 O2 customers in order to demand GBP 700 each in damages for alleged copyright infringement, and to threaten to take court action and/or have the customers' internet service slowed down or cut off if they did not pay. The proposed letters also wrongly asserted that bill payers are liable for any copyright infringement that may have occurred on their internet connection, whether or not they committed the infringement. This tactic is known as 'speculative invoicing' and aims to intimidate consumers into paying without the need to go to court. The application was referred to the High Court, which was concerned that those consumers whose details would be released would not be able to challenge the application. It asked the consumer organisation Consumer Focus to represent their interests in court.

The High Court balanced the competing interests of copyright owners and the customer's right to privacy and protection of his or her personal data. In relation to Golden Eye and 12 of the copyright owners it concluded that the order should not be granted as this "would be tantamount to the court sanctioning the sale of the Intended Defendants' privacy and data protection rights to the highest bidder". This was because the owners had surrendered total control of the litigation to Golden Eye, which would receive around 75% of the proceeds. In relation to Golden Eye and one producer, Ben Dover Productions, which were bringing the litigation jointly, the Court held that it would be proportionate to order disclosure of the personal details of bill payers, as there was a good arguable case that many of the intended defendants had infringed copyright. However, the order and the proposed letter to the customers must be framed so as to safeguard properly the legitimate interests of consumers, particularly those who had not in fact committed the alleged copyright infringements. The proposed letters were objectionable in a number of respects, and should instead request customers who admitted copyright infringement for details of their P2P filesharing and then individually negotiate an appropriate settlement. The Court will hold a second hearing to impose conditions on the wording of the letters and order.

• High Court (Chancery Division), Golden Eye (International) and another v. Telefonica UK Ltd [2012] EWHC 723 (Ch), 26 March 2012
http://merlin.obs.coe.int/redirect.php?id=15817

IRIS 2012-6/21

ISPs Lose Challenge to Digital Economy Act in the Court of Appeal

Tony Prosser
School of Law, University of Bristol

BT and TalkTalk, internet service providers, were unsuccessful in their appeal against the decision of the High Court last year that provisions in the Digital Economy Act 2010 were not in breach of EU law (see IRIS 2011-6/20).

The provisions impose obligations on Internet Service Providers (ISPs) to notify subscribers if their internet protocol addresses are reported by copyright owners as being used to infringe copyright, and they must keep track of the number of reports about each subscriber and must compile on an anonymous basis a list of those reported on. After obtaining a court order to obtain personal details, copyright owners will be able to take action against those on the list. These obligations would only come into effect once an 'initial obligations code' made by Ofcom, the communications regulator, and approved by Parliament, has been brought into force. The ISPs argued that these requirements should have been notified to the European Commission under the Technical Standards Directive; that they were incompatible with provisions of the Electronic Commerce Directive; that they were in breach of the Data Protection Directive and the Privacy and Electronic Communications Directive; and that they were incompatible with the Authorisation Directive.

The Court of Appeal held that the provisions of the Act do not require notification as they do not have legal effect in themselves, being conditional on implementation through the code. They do not breach the Electronic Commerce Directive as they do not impose any liabilities on ISPs, and being concerned with copyright, are outside the 'coordinated field' under the Directive where restrictions on freedom to provide information society services are prohibited. The statutory provisions are not in conflict with the Data Protection Directive as the processing of data relates to legal claims, nor with the Privacy and Electronic Communications Directive as the limits to the confidentiality of data are to protect intellectual property rights. Finally, the Authorisation Directive does not require that all sector-specific rules be contained in a general authorisation rather than separate legislation. The Court also held that the exclusion of small ISPs and mobile network operators from the scheme was not disproportionate.

The ISPs had also challenged the draft costs order allocating the costs of running the system. The High Court had decided that requiring ISPs to pay part of the cost of establishing the system would breach the Authorisation Directive, and this point was not appealed. The Court of Appeal held that 'case fees' covering the costs of appeals were also incompatible with the Directive.

- R (on the application of British Telecommunications and TalkTalk Telecom Group) v. Secretary of State for Culture, Media, Olympics and Sport [2012] EWCA Civ 232, 6 March 2012
  http://merlin.obs.coe.int/redirect.php?id=15770

IRIS 2012-5/22

Operators of 'The Pirate Bay' Infringe Copyright

Tony Prosser
School of Law, University of Bristol

The High Court has decided that the operators of The Pirate Bay website and its users are both guilty of infringing the copyright of rightsholders in the music industry. This means that internet service providers can now be forced to block their customers' access to the site.

The case was brought by major record companies against the six major UK internet service providers. The Pirate Bay is a website which enables users to search for and download copyrighted material, including music and films, and the record companies sought an injunction from the court to force the service providers to block their customers from accessing the site. Under the Copyright, Designs and Patents Act 1988 (as amended to implement the EU Information Society Directive), such an injunction may be granted against an internet service provider if it has 'actual knowledge' that the service was being used to infringe copyright. This hearing concerned the preliminary issue of whether the users and operators of the site breached copyright.

The court decided that the users of The Pirate Bay were in breach of copyright because of the way in which they shared music files; this amounted to communicating the recordings to a new public, as required by the European Court of Justice in Case C-306/05 Sociedad General de Autores v. Editores de España (SGAE) v. Rafael Hoteles SA [2006] ECR I-11519 (see IRIS 2007-2/3). These infringements of copyright had been authorised by the operators of The Pirate Bay who were jointly liable for them; the name of the site and its funding by a Swedish anti-copyright organisation contributed to the Court's finding that such infringement was part of the operators' 'objective and intention'. The case thus cleared the way for a decision at a further future hearing to grant an injunction, following the precedent of the Newzbin2 case in which such an injunction was granted to force a leading internet service provider to block access to a site infringing the copyright of six major film studios (see IRIS 2011-9/21).

- Dramatico Entertainment Ltd v. British Sky Broadcasting Ltd [2012] EWHC 268 (Ch), 20 February 2012
  http://merlin.obs.coe.int/redirect.php?id=15726

IRIS 2012-4/28

Netherlands

Dutch District Court Orders ISPs to Block End-User Access to The Pirate Bay

Axel M. Arnbak
Institute for Information Law (IViR), University of Amsterdam

On 11 January 2012 the District Court of The Hague ordered two Dutch internet access providers to block access to The Pirate Bay. Furthermore, Stichting BREIN, a foundation protecting the interests of the Dutch copyright industry, has been granted a right to directly request the providers to block future IP-addresses and (sub) domain names that may refer to The Pirate Bay. The providers in question, Ziggo and XS4ALL, have already announced they will appeal the ruling. BREIN, on the other hand, has announced it will request similar measures from other providers.

The District Court found the legal basis for these orders in the Dutch implementations of Art. 11 of Directive 2004/48/EC (Enforcement Directive), Art. 8 (3) of Directive 2001/29/EC (Copyright Directive) and the recent European Court of Justice L'Oreal/eBay ruling (C-324-09), in which the ECJ held that injunctions against internet intermediaries may be aimed at preventing future copyright infringements. Earlier court proceedings in the Netherlands had been targeted at The Pirate Bay and ordered it to stop making infringing material available to the Dutch market. Since The Pirate Bay continued anyway, the Court found the BREIN injunctions legitimately aimed at the intermediaries in this particular case.

The District Court noted that it should exercise judicial restraint, as website blocking raises freedom of expression concerns as protected by Art. 10 ECHR. In assessing the proportionality and subsidiarity of website blocking by the two access providers, the District Court ruled that in this

particular case the measure was justified. Along with the limited effect of earlier rulings, it based its proportionality test on evidence provided by BREIN. The Court held that a sufficient proportion of customers had been using The Pirate Bay to download several Dutch movies. Furthermore, the legal material provided by The Pirate Bay would be available through other websites, which limits the effect of blocking on free speech in this instance. Lastly, the Court found that DNS- and IP-blocking of one particular website does not entail active surveillance of the contents of all end-user internet traffic with the help of Deep Packet Inspection technologies, which the ECJ had ruled illegal in its recent Scarlet/Sabam ruling (C-70/10).

Just on 20 December 2011, a Parliamentary majority spoke out against blocking for copyright enforcement purposes in a resolution. The judges considered the initiatives by the Dutch legislature, but found it too early to let their decision be influenced by it. Therefore, it will be noteworthy to follow whether the legislature follows up on its initiative any time soon and to see whether it may impact upon the appeal by the providers.

- *Rechtbank 's-Gravenhage, 11 januari 2012, LJN: BV0549, Stichting BREIN tegen Ziggo B.V. & XS4All Internet B.V.* (District Court of the Hague, 11 January 2012, LJN: BV0549, Stichting BREIN v Ziggo B.V. & XS4All Internet B.V.)
  http://merlin.obs.coe.int/redirect.php?id=15624

- *Tweede Kamer, 29 838 Auteursrechtbeleid, Nr. 35 Motie van het Lid Verhoeven* (Second Chamber, 29838, Copyright policy, Nr. 35, Motion by MP Verhoeven)
  http://merlin.obs.coe.int/redirect.php?id=15645

IRIS 2012-2/31

Russian Federation

Social Network VKontakte Fined for Piracy

Dmitry Golovanov
Moscow Media Law and Policy Centre

On 25 May 2012, the Thirteen Arbitrage Appeal Court of St. Petersburg (commercial court of second instance) upheld a ruling of the court of first instance that found the popular social network VKontakte liable for a violation of the intellectual property rights of two record label companies (S.B.A. Music Publishing and S.B.A. Production). A fine of RUB 210,000 (approximately EUR 5,000) was imposed upon VKontakte for the act of placing on the social network's website and making available to the public the music and phonograms of 17 songs of the Russian pop groups "Maksim" and "Infinity".

The act of posting content without the permission of the rightsholders (i.e., illegally) on the website vkontakte.ru was not denied by either the plaintiffs or the defendant, however the Court did not get a clear answer as to whether it was VKontakte's administration or a user of the social network who technically posted the counterfeit content. So far the central question of the court proceedings has become whether VKontakte's administration was liable for making illegal content available to the public (according to the Russian Civil Code's definitions, was it VKontakte's fault) or not.

The Court of Appeal reasoned its decision according to the guiding principles of the highest arbitrage instance - the Presidium of the Supreme Arbitrage Court - that were formulated in its Resolution of 1 November 2011. The latter decision introduced key points to be taken into consideration by the ordinary arbitrage courts when making decisions concerning the liability of Internet video hosting websites.

The Court of Appeal put forward several basic positions in favour of finding the VKontakte administration at fault in this case. Firstly, the Court stated that the content was available to the general public, but not to specified groups of persons, as the defendant pleaded. The paid registration procedure, which is mandatory for vkontakte.ru users, is available and accessible to any representative of the general public and does not establish any specific target audiences or closed groups as being consumers of the content. Secondly, the Court dealt with the content uploading policy of the VKontakte website. Although due to user agreement provisions the participants of the online community vkontakte.ru are duly informed about their obligation to ensure the legality of the content that they upload, VKontakte provides a number of technical facilities that allow the uploading of counterfeit content. The existence of such facilities was considered to be proof of VKontakte's fault. The court also ruled that the existence of the above-mentioned facilities makes the website vkontakte.ru more preferable for advertising companies posting advertising materials on the World Wide Web and so far provides potential growth for Vkontakte's profits. The court emphasised that the existence of benefits (even potential ones) arising from the illegal use of intellectual property was to be considered as evidence of Vkontakte's fault.

Finally, the Court of Appeal underlined that VKontakte's reaction to the plaintiffs' demands to cease unlawful activities was passive and not effective. The defendant claimed that no information confirming that the plaintiffs were genuine rightsholders was provided in their official claims as delivered to VKontakte. The Court rejected this position and argued that the defendant had had opportunities to check the legal status of the plaintiffs (for instance, by requesting copies of license agreements and other necessary documents). Moreover, the defendant could not be uninformed of the illegality of the content, because the issue of dissemination of the counterfeit content on the VKontakte social network became a sufficient part of public discussion, including in the mass media.

The Decision of Thirteen Arbitrage Appeal Court of St. Petersburg may be appealed in the courts of higher instance.

- *Постановление Тринадцатого арбитражного апелляционного суда 25 мая 2012 года по делу № А56-57884/2010* (Decision of 25 May 2012 Thirteen Arbitrage Appeal Court of 25 May 2012 (Case No A56-57884/2010))
  http://merlin.obs.coe.int/redirect.php?id=15989

IRIS 2012-7/36

The Patriot Act & the Fourth Amendment

How the US Government is Secretly Expanding its Authority to Collect the Private Data of its Citizens

Jonathan Perl
*Locus Telecommunications, Inc.**

I. Introduction

In 2001, the US Congress passed the USA Patriot Act ("Act") in response to the 9/11 attacks in an effort to help law enforcement prevent future attacks.[1] The landmark act provided the federal government ("Government") with unprecedented authority to collect data by implementing sweeping changes to the laws that govern search and surveillance. While its implementation has been shrouded in secrecy, the scope of the Government's reliance on the Act to collect the private data of its citizens is beginning to come to light in the aftermath of the revelations made by NSA whistleblower Edward Snowden ("Snowden"). The resulting media scrutiny and Congressional inquiries have revealed that the Government is secretly expanding its authority to collect the private data of its citizens, often indiscriminately and in bulk, regardless of whether they are suspected of any wrongdoing.

II. The legal restrictions on the US Government for collecting data

The Government is restrained principally in its ability to collect private data by the Fourth Amendment to the United States Constitution, which provides that: "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause…particularly describing the place to be searched, and the persons or things to be seized."[2] It is founded upon the notion that "law enforcement officials can observe your home from the street, but in most cases they can't barge in unless they prove to a judge they need to."[3]

---

* Jonathan D. Perl works as Counsel for Regulatory Affairs at Locus Telecommunications, Inc. The views expressed in this article are those of the author and do not represent the views of, and should not be attributed to, Locus Telecommunications, Inc.

1) See USA PATRIOT Act of 2001, Pub. Law 107-56, 115 Stat. 272 (2001).

2) US Const., amend. IV.

3) Bob Sullivan, "Big Brother may not be listening, but he's watching: Why metadata snooping is legal", *NBC News*, 15 June 2013, available at: www.nbcnews.com/technology/big-brother-may-not-be-listening-hes-watching-why-metadata-6C10334990

The US Supreme Court ("Court") first applied the Fourth Amendment to information *about* telephone calls – part of what is now considered metadata – in a landmark case in 1979.[4] The Court held that the information about a call is not protected by the Fourth Amendment and distinguished it from the content of the phone call, which requires a warrant to access. The Court applied the "third-party doctrine", whereby an individual loses their expectation of privacy when they voluntarily give information to a third party, and held that there is no expectation of privacy over the phone numbers involved in a call because the information is voluntarily provided to the phone company by dialling the number.

Congress codified these findings in 1986 by passing the Electronic Communications Privacy Act ("ECPA").[5] The ECPA affirmed that law enforcement officials can acquire the information about a call via a "pen register"[6] and "trap and trace device"[7] with a subpoena without judicial review. "Pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication", whereas "trap and trace device" means "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication". The authors of the act noted in a US Senate report accompanying the ECPA that they do not envision an independent judicial review of whether the application meets the "relevance" standard but rather that judges are only permitted to review the completeness of the paperwork.[8] This has since been reaffirmed by a federal appeals court, which explained that the "judicial role…is ministerial in nature."[9] As a result, many judges have concluded they have virtually no ability to deny pen registers, leading one federal magistrate judge in Florida to bemoan that "[t]he court under the [ECPA] seemingly provides nothing more than a rubber stamp."[10]

In contrast, the Government is authorised to collect data on foreign nationals overseas by the Foreign Intelligence Surveillance Act of 1978 ("FISA Act")[11] and Executive Order 12333.[12] The FISA Act exempts communications of foreign nationals overseas from Fourth Amendment protections by allowing the Government to collect data for any communications as long as it has reasonable belief that one of the parties involved is a foreign national on foreign ground, and it is not required to identify its targets or the monitored facilities. The Act permits the Government to obtain a single court order from The Foreign Intelligence Surveillance Court ("FISA Court") through which it can monitor thousands, or even millions, of people, including "incidental" surveillance of American citizens.[13] While less is known about the workings of the FISA Court because of its secrecy, a former federal judge who served on the FISA Court, James Robertson, recently expressed his belief that the system is "flawed" because it does not allow legal adversaries to question the Government's actions and "has turned into something like an administrative agency."[14] Executive Order 12333 provides the Government with the authority to collect, retain, analyse, and disseminate foreign signals intelligence information from communications systems around the world.[15]

---

4) *Smith v. Maryland*, 442 U.S. 735 (1979).
5) Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522.
6) 18 USC § 3127 (3).
7) 18 USC § 3127 (4).
8) Declan McCullag, "Feds tell Web firms to turn over user account passwords", *CNET* (25 July 2013) available at: http://news.cnet.com/8301-13578_3-57595529-38/feds-tell-web-firms-to-turn-over-user-account-passwords/
9) *United States v. Fregoso*, US Court of Appeals, 8th Circ. (1995).
10) *Supra* note 8.
11) Foreign Intelligence Surveillance Act of 1978, Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. 36 ("FISA").
12) 46 FR 59941, 3 CFR, 1981, available at: www.archives.gov/federal-register/codification/executive-order/12333.html
13) Margot Kaminskijun, "PRISM's Legal Basis: How We Got Here, and What We Can Do to Get Back, A privacy scholar explains the recent news about government surveillance", *The Atlantic* (7 June 2013), available at: www.theatlantic.com/national/archive/2013/06/prisms-legal-basis-how-we-got-here-and-what-we-can-do-to-get-back/276667/
14) Associated Press, "Former judge admits flaws with secret FISA court", *CBS News*, (9 July 2013), available at: www.cbsnews.com/8301-250_162-57592836/former-judge-admits-flaws-with-secret-fisa-court/
15) *The National Security Agency: Missions, Authorities, Oversight and Partnerships*, National Security Agency (9 August 2013), available at: http://i2.cdn.turner.com/cnn/2013/images/08/09/2013_08_09_the_nsa_story1.pdf

Congress relied on these distinctions when designing the Patriot Act's three new and updated tools to collect data: (1) Business Records Orders ("Section 215"), (2) Sneak and Peek Warrants, and (3) National Security Letters ("NSL").[16] The Section 215 orders have been used to request customer information like license records, hotel records, car-rental records, apartment-leasing records, credit card records, and books, and come with a "gag" order that prohibits the recipient from telling anyone that they received one. The Act also allows the Government to petition for a Sneak and Peek Warrant to briefly review a variety of records, including phone records to bank account information; while an NSL allows law enforcement to raid a suspect's house without notifying the recipient of the seizure for months, including accessing a suspect's computers. The National Security Agency ("NSA"), the Government agency that "collects, processes, and disseminates intelligence information from foreign electronic signals for national foreign intelligence and counterintelligence purposes and to support military operations,"[17] relies mostly on Section 215 because it allows them to collect "any tangible things" in connection with an authorised investigation to protect against international terrorism or clandestine intelligence activities if "there are reasonable grounds to believe that the tangible things sought are relevant to an authorised investigation" via a secret order issued by the FISA Court. An analysis by the American Civil Liberties Union ("ACLU") showed that there were approximately 192,000 NSLs issued between 2003 and 2006 which collectively resulted in one terror conviction and 3,970 Sneak and Peek Warrants issued in 2010 alone, of which only less than 1% involved terrorism.[18]

III. The scope of data collection

On 6 June 2013, *The Guardian* published five pages of a power point presentation drafted by the NSA that describes a top secret domestic intelligence programme titled PRISM.[19] The release of this top secret document triggered a cascade of leaked documents that showed the extent of the Government's access, collection, and use of private data.

The revelations have made clear that the American public has not yet been privy to the full extent of the surveillance and data collection or the dozens of legal opinions – some of which are hundreds of pages – justifying these actions. According to the NSA's own estimates there were 117,675 active surveillance targets in PRISM's counterterrorism database which has resulted in 24,005 reports in 2012, "over 2,000 Prism-based reports" every month,[20] more than 77,000 intelligence reports that have cited the PRISM programme, 850 billion "call events" collected and stored in the NSA databases, close to 150 billion Internet records, and 1-2 billion records added each day. Even more chilling, the NSA recently acknowledged that it "touches" an estimated 1.6% of the Internet data and selects 0.025% of Internet data for review.[21]

a. PRISM

The top secret documents leaked by Snowden revealed that PRISM "allows an analyst to look at, collate, monitor, and cross-check the content of email, video and voice chat, videos, photos, voice-over-IP (Skype, for example) chats, file transfers, and social networking details"[22] of any data accessed from the servers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and

16) *Reclaiming Patriotism, A Call to Reconsider the Patriot Act*, American Civil Liberties Union, (March 2009), available at: www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf
17) *Frequently Asked Questions*, National Security Agency, available at: www.nsa.gov/about/faqs/index.shtml
18) *Surveillance Under the Patriot Act*, American Civil Liberties Union, (October 2011) available at: https://www.aclu.org/national-security/surveillance-under-patriot-act. See also *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, Office of the Inspector General, U.S. Department of Justice, (March 2008).
19) Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian* (6 June 2013), available at: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
20) Ibid.
21) *Supra* note 15.
22) *Supra* note 19.

Apple[23] that is "relevant" to foreign intelligence. After an NSA analyst accesses the data from the servers, they can open an investigation on an individual by issuing a report to a supervisor. The request will be approved if there is "reasonable belief" that the specified target is a foreign national who is overseas at the time of collection, which is defined as 51 percent confidence.[24]

The Director of National Intelligence acknowledged that the NSA's broad interpretations result in "incidentally acquired"[25] data of US citizens even though PRISM *targets* only "non-U.S. persons located outside the United States." However, he also stressed that the NSA has implemented "minimisation procedures," whereby PRISM flags it as an incidental over-collect and deletes it from the analyst's workspace and an analyst must manually segregate the data if it doesn't happen automatically.[26] Then again, the Director admitted in a letter to Senator Ron Wyden that on "at least one occasion" the FISA Court found that "minimisation procedures" used by the Government were "unreasonable under the Fourth Amendment."[27] This acknowledgement underscores the concern that the data will remain in the possession of the Government but "not be logged, indexed, or put into a report."[28] There is also concern whether and how the data is shared. If an analyst believes that a citizen evidences criminal activity or criminal intent it triggers a process that sends the information to the Federal Bureau of Investigation (FBI) to begin its own investigation using the NSA tip as probable cause.[29] However, each analyst is called upon to subjectively distinguish between relevant and non-relevant communication and decipher a citizen's intent often with minimal context. Furthermore, the information can be shared with any of the scores of federal agencies, many of which are increasingly requesting data from the NSA.

Microsoft, Yahoo, Google, Facebook and PalTalk have denied that they "participated knowingly" in PRISM.[30] However, it should not be forgotten that the gag order prohibits them from even acknowledging the existence of the programme. Such co-operation, if true, would not be in contrast with past practices since they acknowledged in 2006 that they participated voluntarily in an earlier version of the programme until it was revealed by the New York Times;[31] a revelation that was subsequently confirmed when Congress provided them blanket immunity in the FISA Amendments Act of 2008.[32]

b. Bulk call logs – "Nobody is listening to your phone calls"

The leaks also revealed that in April 2013, the FISA Court approved a request by the NSA for access to all telephone numbers of Verizon – one of the largest telecommunications providers in the US – indiscriminately and in bulk, regardless of whether the subscribers are suspected of any wrongdoing. Pursuant to the order, Verizon was required to provide the NSA electronic copies of

23) See "NSA slides explain the PRISM data-collection program", *The Washington Post* (6 June 2013), available at: www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
24) *Supra* note 15 (the leaked NSA guidelines are at: www.documentcloud.org/documents/727943-exhibit-a.html).
25) *Supra* note 11.
26) Marc Ambinder, "Solving the mystery of PRISM", *The Week* (7 June 2013), available at: http://theweek.com/article/index/245360/solving-the-mystery-of-prism
27) Spencer Ackerman, "U.S. Admits Surveillance Violated Constitution At Least Once", *Wired* (20 July 2012), available at: www.wired.com/dangerroom/2012/07/surveillance-spirit-law/; see also http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393/
28) Eli Lake, "THE SURVEILLANCE SCANDALS, Former NSA Director Michael Hayden Responds to Edward Snowden Claim", *The Daily Beast* (12 June 2013) (Citing a case, *U.S. v. Sattar,* where the Government produced thousands of hours of intercepted communications that were minimised but not destroyed).
29) *Supra* note 27.
30) Chris Gayomali, "Here are the tech companies denying involvement with the NSA's PRISM program", *The Week* (7 June 2013), available at: http://theweek.com/article/index/245325/here-are-the-tech-companies-denying-involvement-with-the-nsas-prism-program.
31) Barton Gellman, "U.S. surveillance architecture includes collection of revealing Internet, phone metadata", *The Washington Post* (12 March 2004), available at: www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html?hpid=z1
32) FISA Amendments Act of 2008, Pub.L. 110–261, 122 Stat. 2436, H.R. 6304 (2008).

"all call detail records or 'telephony metadata' created by Verizon for communications between the United States and abroad" or "wholly within the United States, including local telephone calls on an ongoing daily basis" from the date of the order to 19 July 2013.[33] Specifically, it required Verizon to include "session identifying information" such as "originating and terminating numbers," the duration of each call, telephone calling card numbers, trunk identifiers, International Mobile Subscriber Identity (IMSI) numbers, and "comprehensive communication routing information." It is unclear whether the order was a one-off or merely the latest in a series of similar orders. It also remains unclear whether Verizon is the only carrier subjected to such an order. However, a report in 2006 by *USA Today* revealing that the NSA implemented a bulk collection programme of domestic telephone, Internet and e-mail records of customers of AT&T, Verizon and BellSouth that was secretly authorised by President Bush suggests that the NSA has collected cell records from all major mobile networks in the past.

c. XKeyscore

It has also been revealed that the NSA also operates a data collection programme called XKeyscore, which it boasts is its "widest reaching" system of "developing intelligence from computer networks."[34] In training materials that were leaked, the NSA explained that it covers "nearly everything a typical user does on the internet", including the content of e-mails, websites visited and searches, as well as their metadata, including "real-time" interception of an individual's Internet activity. Analysts use it to mine enormous agency databases giving only a broad justification for the search, which is not reviewed by a court or any NSA personnel before it is processed. An NSA tool called DNI Presenter also enables an analyst using XKeyscore to read the content of chats or private messages. Content remains on the system for only three to five days, while metadata is stored for 30 days.

IV. The Government's legal justifications of its secret programmes

In response to the increased media scrutiny and public debate, President Obama released a 22-page White paper that explained the legal basis for the various NSA surveillance programmes.[35] It explained that the programmes are justified because they meet a broadened definition of "relevance" under Section 215. It argued that the definition of "relevance" should be interpreted "at least as broad[ly]" as it has been in a series of cases involving the discovery of documents in "ordinary civil discovery and criminal and administrative investigations," because "the 'relevance' standard affords considerable latitude, where necessary, and depending on the context, to collect a large volume of data in order to find the key bits of information contained within." It also argues that all telephone metadata is relevant under Section 215 because somewhere within that vast dataset there may be individual data elements that are, in fact, relevant. Although the Government cautioned that this may seem to provide broad authority to collect other types of data such as medical information or library records, it noted that it is refraining from seeking that type of information for counterterrorism purposes because these categories of data are not in general comparable to communications metadata as a means of identifying previously unknown terrorist operatives or networks. This interpretation is troubling, however, because it is essentially arguing that "we don't think bulk collection of medical records is necessary to stop terrorism, but if we did, we could collect it." In such an event "…it would allow the government to sweep up almost any data on the basis that some of it might prove relevant later" such as "billions of medical records or book or library records without a warrant – the textbook definition of an unconstitutional fishing expedition."[36]

33) Glen Greenwald, "NSA collecting phone records of millions of Verizon customers daily", *The Guardian* (5 June 2013), available at: www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
34) Glen Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet", *The Guardian* (31 July 2013), available at: www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
35) Administration White Paper, "Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act" (9 August 2013), available at: http://big.assets.huffingtonpost.com/Section215.pdf
36) Jeffrey Rosen, "The Lies Aren't What Make Obama's NSA Stance So Awful", *The New Republic* (12 August 2013), available at: www.newrepublic.com/article/114276/obama-surveillance-comments-dishonesty-isnt-only-problem

President Obama promised to reform Section 215 of the Patriot Act. Specifically, he explained that the reforms will include a new website that will teach Americans and people around the world more about the surveillance programmes, an outside advisory panel to review the surveillance programmes, a privacy officer at the NSA, and an independent attorney to challenge the Government's arguments and policies in court.[37] The proposals met with criticism from senior Republicans in Congress, who warned that an advocate in the proceedings of the secret court that oversees the agency's sweeping phone-data collection would slow down antiterrorism efforts when time is of the essence.[38]

V. Government acknowledgement of overreach

In August 2013, an NSA internal audit was leaked that revealed the agency broke privacy rules and overstepped its legal authority thousands of times each year.[39] The audit, dated May 2012, counted 2,776 incidents of unauthorised collection, storage, access to or distribution of legally protected communications in the preceding twelve months alone, and while it found that most were unintended, many involved failures of due diligence or violations of standard operating procedures. Notable examples include a violation of a court order and unauthorised use of data about more than 3,000 Americans and green-card holders, typographical errors that resulted in unintended interception of US e-mails and telephone calls, and even a decision that it did not need to report the unintended surveillance of Americans. The audit also cited violations going as far back as 2008, including the interception of a "large number" of calls placed from Washington when a programming error confused the US area code 202 for 20, the international dialling code for Egypt. Another violation was revealed by the FISA Court finding that the NSA acted unconstitutionally by failing to disclose to the court a new collection method until it had been in operation for many months. Another example of overreach is the diversion of large volumes of international data passing through fiber-optic cables in the United States into a repository where the material could be stored temporarily for processing and selection. The number of violations is likely to be significantly higher, since the audit counted only incidents at the NSA's Fort Meade headquarters and omitted other NSA operating units and regional collection centers.

VI. Conclusion

The supporters of the programmes argue that they are not invasive because the Government does not actually view the content. However, even if this were true for all of the NSA's programmes, this is increasingly becoming a distinction without a difference because metadata can be, in the words of an expert, often "much more intrusive than content."[40] In practice, it allows the Government to "learn immense amounts of proprietary information."[41] For example, a pattern of phone calls from key executives can reveal impending corporate takeovers; calls to a gynecologist, oncologist, and then close family members can reveal a sensitive medical condition; and information from cell-phone towers can reveal the caller's location and movements. These examples are buttressed by the findings of numerous studies, including that an individual can be indentified simply by knowing where they were on four separate occasions[42] and that a person's preferences, political leanings, and

37) See Obama announces NSA surveillance reform RT (9 August 2013), available at: http://rt.com/usa/obama-nsa-statement-transparency-308/
38) Janet Hook and Sarah Portlock, "Republicans Warn on NSA Changes", *The Wall Street Journal* (11 August 2013), available at: http://blogs.wsj.com/washwire/2013/08/11/republicans-warn-against-nsa-changes/?mod=WSJ_hpp_MIDDLENexttoWhatsNewsForth
39) http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/
40) Nidhi Subbaraman, "Facebook forensics? What the feds can learn from your digital crumbs", *NBC News* (8 June 2013), www.nbcnews.com/technology/facebook-forensics-what-feds-can-learn-your-digital-crumbs-6C10240840
41) Bob Sullivan, "Big Brother may not be listening, but he's watching: Why metadata snooping is legal", *NBC News* (15 June 2013).
42) Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, "Unique in the Crowd: The privacy bounds of human mobility", *Scientific Reports* (25 March 2013).

a host of other character details can be learned from only their Facebook "likes."[43] This new reality has made "the line between knocking on your door and barging in much more complicated."[44]

It is unclear yet what type of remedial actions Congress or the Court may take. However, even supportive members of Congress have expressed concern. Some complained that they were not fully informed about the dragnet collection,[45] while others like one of the authors of the original Patriot Act, lamented that "the secret interpretation was not in keeping with the original intent of the legislation." Four bills have been introduced to fix the problem, each of which takes a different tact: heightening the standard by requiring "specific and articulable facts" and that "each of" the business records are related to an investigation;[46] requiring evidence that the records are "material" or significantly relevant to an investigation; mandating that every order include why the records "pertain to" an individual or are "relevant to" an investigation;[47] and the most recent one to come to a vote, requiring the NSA to have a specific target if it is seeking phone records.[48] While the most recent bill failed to pass by a 205-to-217 vote, it demonstrated that support for limiting the NSA's authority is growing and may yet eventually pass because the traditional bipartisan lines are not being drawn on this issue. The support of conservative and liberal members as cosponsors and the close vote were especially surprising since the leadership of both parties opposed the bill.

There are also recent indications that the US Supreme Court may not rule on the constitutionality of these programmes. In February 2012, the Court found that the plaintiffs – lawyers, journalists and human rights advocates – in a lawsuit that challenged the constitutionality of the law that authorises PRISM lacked standing because they could not show that they had been personally injured by it.[49] The Court explained that the alleged surveillance was too speculative and that the surveillance of the plaintiffswas not "certainly impending." While the new revelations may "show that surveillance is 'certainly impending' because we now know that the PRISM program exists," there is still doubt whether it may be enough to show the Government spied on them "in particular."

However, a demand for a special congressional investigatory committee, more transparency and more accountability is slowly growing. The movement is spearheaded by a coalition of over 100 civil liberties groups.

43) Michal Kosinski, David Stillwell, and Thore Graepel, *Private traits and attributes are predictable from digital records of human behavior*, Proceedings of the National Academy of Sciences of the United States (12 February 2013).
44) *Supra* note 3.
45) *Supra* note 38.
46) Mark M. Jaycox, "Bills Introduced by Congress Fail to Fix Unconstitutional NSA Spying", *Electronic Frontier Foundation* (15 July 2013), available at: www.eff.org/deeplinks/2013/07/bills-fail-fix-unconstitutional-nsa-spying
47) Electronic Communications Privacy Act Amendments Act of 2013, Amendments Act of 2013 Senate Report with Additional Views Accompanying S. 607, Committee on the Judiciary (16 May 2013), available at: www.fas.org/irp/congress/2013_rpt/ecpa_amend.html
48) Ginger Gibson, Justin Amash, "John Conyers introduce NSA bill", Politico (18 June 2013), available at: www.politico.com/story/2013/06/justin-amash-john-conyers-nsa-bill-92982.html#ixzz2bUBXZXie
49) Cindy Cohn and Trevor Timm, "Supreme Court Dismisses Challenge to FISA Amendments Act; EFF's Lawsuit Over NSA Warrantless Wiretapping Remains", *Electronic Frontier Foundation*, (27 February 2013), available at: www.eff.org/deeplinks/2013/02/supreme-court-dismisses-challenge-fisa-warrantless-wiretapping-law-effs-lawsuit

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

Information services for the audiovisual sector

It is the task of the European Audiovisual Observatory to improve transparency in the audiovisual sector in Europe. It does this by collecting, processing and publishing up-to-date information about the various industries concerned.

The Observatory has adopted a pragmatic definition of the audiovisual sector in which it works. Its principal areas of interest are film, television, video/DVD, on-demand audiovisual media services and public policy on film and television. In these five areas, the Observatory provides information in the legal field as well as information about the markets and financing. As far as its geographical scope is concerned, the Observatory monitors, records and analyses developments in its member states. In addition, data on non-European countries is also made available when judged appropriate. The various stages involved in providing information include the systematic collection and processing of data as well as its final distribution to our users in the form of print publications, information on-line, databases and directories, and our contributions to conferences and workshops. The Observatory's work draws extensively on international and national information sources and their contributions of relevant information. The Observatory Information Network was established for this purpose. It is composed of partner organisations and institutions, professional information suppliers and selected correspondents. The Observatory's primary target groups are professionals working within the audiovisual sector: producers, distributors, exhibitors, broadcasters and other media service providers, international organisations in this field, decision-makers within the various public bodies responsible for the media, national and European legislators, journalists, researchers, lawyers, investors and consultants.

The European Audiovisual Observatory was established in December 1992 and is part of the Council of Europe thanks to its status as a "partial and enlarged agreement". Its offices are in Strasbourg, France. The Observatory's membership currently comprises 39 European States and the European Union, which is represented by the European Commission. Each member appoints one representative to its board, the Executive Council. An Executive Director heads the international Observatory team.

The Observatory's products and services are divided into four groups:

- **Publications**
- **Information on-line**
- **Databases and directories**
- **Conferences and workshops**

European Audiovisual Observatory
76 Allée de la Robertsau – F-67000 Strasbourg – France
Tel: +33 (0) 3 90 21 60 00 – Fax: +33 (0) 3 90 21 60 19
www.obs.coe.int – E-mail: obs@obs.coe.int

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Legal Information Services from the European Audiovisual Observatory

Order:
- **online at http://www.obs.coe.int/about/order**
- **by email: orders-obs@coe.int**
- **by fax: +33 (0) 3 90 21 60 19**

IRIS Newsletter

Legal Observations of the European Audiovisual Observatory

Online, free of charge!

The IRIS Newsletter is a topical and reliable monthly information service covering all legal developments in Europe relating to the audiovisual sector. IRIS covers all areas of law relevant to the audiovisual sector. The main emphasis of the IRIS articles is on legal developments in the fifty or so countries that make up greater Europe. IRIS reports on media legislation in the broadest sense, as well as major developments in case law, important administrative decisions, and policy decisions which will potentially affect legislation in this field.
A free subscription and the complete IRIS newsletter are available from the IRIS website: http://merlin.obs.coe.int/newsletter.php

IRIS *plus*

A legal hot topic examined from different angles

Legal, technological or economic developments in the audiovisual sector generate immediate priority information needs for professionals. IRIS *plus* identifies these issues and provides the relevant legal background. It features a combination of a lead article, related reporting and a *Zoom* section, comprising overview tables, market data or practical information. This brand new format provides you with the knowledge to follow and join in the latest and most relevant discussions concerning the audiovisual sector.
For more information: http://www.obs.coe.int/irisplus

IRIS Merlin

Database on legal information relevant to the audiovisual sector in Europe

The IRIS Merlin database enables you to access over 6,500 articles reporting on legal events of relevance to the audiovisual industry. These articles describe relevant laws, decisions of various courts and administrative authorities, and policy documents from over 50 countries. They also report on legal instruments, decisions and policy documents of major European and international institutions.
Free access at: http://merlin.obs.coe.int

IRIS *Special*

Comprehensive factual information coupled with in-depth analysis

The themes chosen for our IRIS *Special* publications are all topical issues in media law, which we explore from a legal perspective. IRIS *Special* publications offer detailed surveys of relevant national legislation facilitating the comparison of the legal frameworks in different countries, they identify and analyse highly relevant issues and outline the European or international legal context that influences national legislation. IRIS *Special* publications explore their legal themes in an extremely accessible way. You don't have to be a lawyer to read them! Every edition combines a high level of practical relevance with academic rigour.
For a list of all IRIS *Specials*, see: http://www.obs.coe.int/oea_publ/iris_special/index.html

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS *plus* 2013-6
How Private is Personal Data?
25,50 € - ISBN 978-92-871-7791-9