European Commission
DG Internal Market and Services

Study on Online Copyright Enforcement and Data Protection in Selected Member States

Netherlands, Poland, United Kingdom

April 2010

Prepared by Hunton & Williams, Brussels
Christopher Kuner
Cédric Burton

For DG Internal Market and Services of the European Commission

With the assistance of
Annemarie Bloemen-Patberg, Houthoff Buruma N.V.
Xawery Konarski, Traple Konarski Podrecki Kancelaria Prawna sp.j.
Peter Hall, Wragge & Co LLP

HUNTON& WILLIAMS

TABLE OF CONTENTS

I. INTRODUCTION AND METHODOLOGY

This study is a follow-up to the previous study presented to the European Commission in November 2009[1] on the legal situation regarding the interaction between online copyright enforcement and data protection at the European Union (EU) level in six selected EU Member States, namely: Austria, Belgium, France, Germany, Spain and Sweden. The initial study has not been updated.

This follow-up study covers three additional EU Member States, namely: the Netherlands, Poland and the United Kingdom. It has been prepared on behalf of DG Internal Market and Services of the European Commission by the Brussels office of Hunton & Williams with the assistance of local counsel, and in the context of the "Stakeholders' Dialogue on Illegal Uploading and Downloading" organized by DG Internal Market and Services.

Hunton & Williams instructed local counsel, and coordinated and reviewed their contributions, which included clarification of important legal points, before finalizing them. This follow-up study is current as of April 1, 2010. In line with the previous study, it was purposely kept brief, and is not intended to provide an exhaustive analysis.

It is important to realize the limitations of this study. It does not constitute legal advice and decisions in a particular case should not be based on the study without consulting counsel. While great effort has been put into making the study as accurate as possible, many of the legal concepts and questions examined have not been the subject of authoritative decisions by courts or data protection authorities (DPAs) in some of the countries, so that there is a lack of legal certainty about them. In addition, certain concepts may be understood differently in different countries. Thus, some of the positions and descriptions contained in the follow-up study represent our interpretation of the legal situation, rather than a definitive statement of the law.

[1] Hunton & Williams, Study on Online Copyright Enforcement and Data Protection in Selected Member States, European Commission, DG Internal Market and Services, November 2009. The initial study is available at: http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf

II. AUTHORS OF THE STUDY

Principal Authors:

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Christopher Kuner, Partner (overall responsibility for the study)
E-mail: ckuner@hunton.com

Cédric Burton, LL.M., Avocat au Barreau de Bruxelles (coordination of the study)
E-mail: cburton@hunton.com

For the Netherlands:

Annemarie Bloemen-Patberg
Houthoff Buruma N.V.
Gustav Mahlerplein 50
1082 MA Amsterdam
The Netherlands
E-mail: a.bloemen@houthoff.com

For Poland:

Xawery Konarski
Traple Konarski Podrecki Kancelaria Prawna sp.j.
ul. Królowej Jadwigi 170
30-212 Kraków
Poland
E-mail: xawery.konarski@traple.pl

For the United Kingdom:

Peter Hall
Wragge & Co LLP
Colmore Row 55
Birmingham B3 2AS
United Kingdom
E-mail: Peter_Hall@wragge.com

III. EXECUTIVE SUMMARY

While there are a few differences among the three Member States analyzed in this follow-up study (i.e., Poland, the Netherlands and the United Kingdom), our general conclusions are similar to those of the initial study on Online Copyright Enforcement and Data Protection conducted in November 2009.[2]

The general rules laid down by the European Court of Justice in the Promusicae and Tele2 cases are applied differently in the three analyzed Member States. In particular, how to apply the proportionality principle in the context of online copyright enforcement and how to strike a fair balance between data protection law and online copyright enforcement seem to be left to the Member States.

Further, little consideration was initially given by the Member States to the interaction between data protection rules and implementation of the IP Enforcement Directive into their national law. However, the legal situation in the UK seems to be evolving due to the recent Digital Economy Act, although many issues still need to be clarified in a code of practice.

With regard to the specific questions examined in the three Member States, our conclusions are also to a large extent analogous to those in the previous study.[3]

[2] Hunton & Williams, Study on Online Copyright Enforcement and Data Protection in Selected Member States, European Commission, DG Internal Market and Services, November 2009. The initial study is available at: http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf

[3] See the Executive Summary on page 4 of the Study on Online Copyright Enforcement and Data Protection in Selected Member States.

IV. NATIONAL SITUATIONS IN SELECTED COUNTRIES

A. Netherlands

Prepared by:
Annemarie Bloemen-Patberg
Houthoff Buruma N.V.
Amsterdam, The Netherlands

Table of legislation

Denomination	Reference
DPA	College bescherming persoonsgegevens
Dutch Data Protection Act	*Wet bescherming persoonsgegevens*, entry into force on September 1, 2001
Dutch Telecommunications Act	*Telecommunicatiewet*, entry into force on December 15, 1998
Stichting BREIN	*Bescherming Rechten Entertainment Industrie Nederlands*
Dutch Telecommunications Data Retention Act	*Wet bewaarplicht telecommunicatiegegevens*, August 28, 2009

1. Nature of an IP address

1.1. Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

Personal data means any information relating to an identified or identifiable person (Article 1 sub a) of the Data Protection Act). In 2008, the DPA concluded that an IP address is personal data within the scope of the Data Protection Act (*Guidelines on the publication of personal data on the internet*, December 2007). The DPA argued that both static (permanent) and dynamic (temporary) IP addresses are personal data since a third party (i.e., an ISP) can easily discover the natural person using the IP address. Whether or not an ISP uses the IP address to identify a certain natural person is irrelevant; the possibility of identification is sufficient for the IP address to be considered personal data.

Traffic data are defined as data that are processed to transmit communication via an electronic communication network or for the invoicing thereof (Article 11.1 sub b) of the Telecommunications Act). According to the Explanatory Memorandum to this Article, IP addresses are deemed traffic data.

1.2. Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the users?

Data concerning criminal offences or the suspicion of criminal offences are deemed sensitive judicial data (Article 16 Data Protection Act). Certain forms of copyright infringement such as intentional infringement are considered to be criminal offences (Articles 31 to 36 under a) Copyright Act). Whether an IP address related to a user who is a natural person and who commits or facilitates copyright infringement is considered to be sensitive data depends on the nature of the infringement.

Judicial data may in principle only be processed by a controller for its own benefit in the limited circumstances listed in the Data Protection Act, for example, if the criminal data relate to offences committed within the controller's own organization against the controller or its employees (Article 22 Data Protection Act). If a controller wishes to process judicial data on behalf of a third party, such data may only be processed if appropriate and specific guarantees have been provided, and subject to the DPA conducting a prior investigation (Article 31 (1) Data Protection Act). This prior investigation consists of a review on the lawfulness of the processing by the DPA.

There are exemptions to the prohibition against processing sensitive data (including judicial data), for instance if (i) the processing is carried out with the consent of the data subject, (ii) the data have been manifestly made public by the data subject, or (iii) the processing is necessary for the establishment, exercise or defense of legal claims (Article 23 of the Data Protection Act).

We note that in the Netherlands no specific limitations are provided regarding data relating to administrative sanctions or judgments in civil cases (as described in Article 8 section 5 of the EU Privacy Directive 95/46/EC).

2. Processing and retention of IP addresses by ISPs

2.1. Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication?

IP addresses: An IP address is deemed traffic data within the scope of the Telecommunications Act (see 1.1 above). Generally, an ISP must anonymize traffic data if the data are no longer necessary for communication purposes, unless the traffic data are required for invoicing (Article 11.5 section 1 and 2 of the Telecommunications Act). In addition, an ISP may use traffic data for market research and sales activities in relation to electronic communications or related services, provided it has obtained the prior consent of the user of the traffic data (Article 11.5 section 3 of the Telecommunications Act).

In addition, traffic data must be retained for a period of twelve months for the purpose of the prevention, detection and prosecution of serious crimes (Article 13.2a of the Telecommunications Act as applicable since the Dutch Telecommunications Data Retention Act came into force as an implementation of the EU Data Retention Directive 2006/24/EC). The

adoption of the Dutch Telecommunications Data Retention Act by the Dutch Senate (*Eerste Kamer*) was subject to a future legislative amendment shortening the twelve month retention period to six months for Internet related data. This amendment has not yet been ratified because the Dutch Government resigned. The new Government (to be elected on June 9, 2010) will have to discuss the amendment.

Subscribers' details: Personal data may not be stored longer than is necessary for the purposes for which the data were collected or for which they are further processed (Article 10 of the Dutch Data Protection Act). The Exemption Decree to the Data Protection Act provides a number of limited storage periods which may be applicable to the processing of personal data by ISPs. Personal data of debtors and creditors may generally not be stored longer than two years after the last payment is made (Article 12 Exemption Decree) and the personal data of customers may generally not be stored longer than two years after the last transaction has been completed (Article 13 Exemption Decree). These storage periods are indicative: there are statutory obligations providing for shorter or longer periods of storage. For instance, the General Tax Act (*Algemene Wet Rijksbelastingen*) and Civil Code (*Burgerlijk Wetboek*) provide for a storage period of 7 years for certain company records – which may include personal data.

After the termination of the abovementioned purposes/retention periods, the ISP must anonymize or delete the IP addresses and subscribers' details.

2.2. If so, can the ISP keep the data for the purpose of fighting online copyright infringement?

IP addresses: ISPs may only process IP addresses for the purposes listed in Articles 11.5 and 13.2a of the Telecommunications Act (see above under 2.1). The processing for other purposes, such as to fight online copyright infringement, is not allowed under the Telecommunications Act.

Subscribers' details: As described above, personal data may not be stored longer than is necessary for the purposes for which the data were collected or for which they are further processed (Article 10 of the Dutch Data Protection Act). There are a limited number of exceptions (see under 1.2 for more information). None of them cover the fight against online copyright infringement.

2.3. If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

For the purpose of this question, a distinction should be made between (a) IP addresses that are stored for the purposes of processing as described in Article 11.5 of the Telecommunications Act (invoicing, market research, etc.) and (b) subscribers' details on the one hand, and IP addresses that are stored to comply with Article 13.2a of the Telecommunications Act (12-month data retention period within the scope of the prevention, detection and prosecution of criminal offences) on the other hand.

(1) Criminal enforcement by judicial authorities

(a) IP addresses stored on the basis of Article 11.5 Telecommunications Act and subscribers' details: Generally, ISPs must comply with all criminal enforcement related requests from supervisory authorities, police forces and judicial authorities in so far these are allowed under Dutch law. See under 4.2 for further details.

(b) IP addresses stored on the basis of Article 13.2a Telecommunications Act: ISPs may only comply with criminal enforcement related requests in as far as they concern serious crimes and the request is made by police forces or judicial authorities on the basis of their powers as laid down in the Criminal Prosecution Code (*Wetboek van Strafvordering*). The Explanatory Memorandum to this Article explains that this does not include requests of supervisory authorities (such as the Dutch telecommunication authority, the "OPTA") or third parties (on the basis of a court order).

Serious crimes include all crimes that are punished with a prison sentence of four years or more. Four years is the maximum prison sentence for professional infringement of copyright.

(2) Civil enforcement by RHs

(a) IP addresses stored on the basis of Article 11.5 Telecommunications Act and subscribers' details: ISPs are not allowed to store IP addresses and subscribers' details for the sole purpose of making these data available to RHs requesting the information for civil enforcement. If an information request concerns IP addresses or subscribers' details which at that time are stored by the ISP in accordance with the Telecommunications Act or the Data Protection Act, the ISP may provide the data to the RH for civil enforcement.

(b) IP addresses stored on the basis of Article 13.2a Telecommunications Act: ISPs may not provide these IP addresses to RHs for any reason.

2.4. Can ISPs process IP addresses to pass on infringement notices to users? If so, under what conditions (consent, etc.)?

ISPs may only process IP addresses for the purposes listed in Articles 11.5 and 13.2a of the Telecommunications Act (see above under 2.1). The processing for other purposes, such as the processing to pass on infringement notices, is not allowed under the Telecommunications Act.

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

The monitoring/processing/filtering of IP addresses will be deemed to be processing of sensitive data as it may concern data regarding criminal offences or data regarding the suspicion of criminal offences.

Monitoring by RHs: *Automatic* monitoring/processing/filtering activities will imply that the users of IP addresses will not be informed of the monitoring/processing/filtering. A RH may conduct such monitoring/processing/filtering for its own enforcement purposes, provided the activities have been subject to a prior investigation by the DPA, and the DPA has concluded such activities to be lawful (Article 31 (1) (b) Data Protection Act).

A RH may monitor/process/filter a *specific* IP address in as far as this is necessary for the establishment of a legal claim.

Monitoring by representatives: A representative may only conduct *automatic* monitoring/ processing/filtering activities for the benefit of third parties (i.e., RHs), if such activities have been subject to a prior investigation by the DPA, and the DPA has concluded such activities to be lawful (Article 31 (1) (c) Data Protection Act).

In April 2004, the results of a prior investigation by the DPA were published. The prior investigation concerned the monitoring/processing/filtering of IP addresses by Stichting BREIN, a Dutch organization representing the interests of RHs. Stichting BREIN was planning to search the Internet for infringing activities and collect the IP addresses of infringers. Stichting BREIN wished to use these IP addresses, among other things, to send infringement notices to infringers.

The DPA concluded that Stichting BREIN had a legitimate interest in protecting the rights of the RHs by collecting the personal data of potential infringers, provided that adequate measures for the protection of such data were implemented. In that respect, the DPA stated that the data subjects should be: (1) informed of the processing of their personal data by Stichting BREIN as soon as the interest of the investigation are no longer in danger and (2) able to exercise their rights of access, deletion and correction. In addition, the DPA concluded that Stichting BREIN was not allowed to transfer the personal data to the U.S., nor to store the personal data collected for a period longer than five years.

A representative may monitor/process/filter a specific IP address in as far as this is necessary for the establishment of a legal claim of the principal.

3.2. If so, can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

RHs can communicate the IP addresses they gathered to an ISP, provided that they have been collected in compliance with Dutch law and in particular with the results of the DPA's prior investigation. Note that a court rejected Stichting BREIN's request to ISPs to obtain the identity of the users of certain IP addresses because, among other grounds, the processing of the IP addresses by Stichting BREIN was unlawful as it was conducted in violation of the instructions of the DPA made in its prior investigation (Hof Amsterdam, 13 July 2006[4]).

[4] Computerrecht 2006/168

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntarily disclose the users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

ISPs can, under certain circumstances, disclose their users' personal data to RHs (i.e. disclose a user's details to RHs voluntarily without being liable for any damages suffered by the user as a result of such disclosure). Whether or not such disclosure is allowed was decided by the Dutch Supreme Court in 2005:

Lycos/Pessers, Hoge Raad, 25 November 2005:[5] The Dutch Supreme Court ruled that Dutch data protection law does not generally prohibit the disclosure of personal data by ISPs to third parties wishing to initiate civil proceedings. Whether or not such disclosure is allowed depends on the specific circumstances of the case, in particular: (i) it must be likely that the user acted unlawfully towards the applicant; (ii) the applicant must have a real interest in obtaining the name and address of the user; (iii) there may be no less intrusive means of tracing the data than through the ISP; and (iv) in light of a balancing of the interests involved, those of the applicant must prevail.

The criteria have been applied in several other court cases, but until now only the requests for disclosure of the personal data of a website owner, not of a website user, have been granted. Below are two other case-law examples:

Stichting BREIN/KPN, Rechtbank Den Haag, 5 January 2007:[6] Stichting BREIN requested KPN (an ISP) to disclose personal data of a website owner offering BitTorrent files (i.e., films, music, etc.) for downloading. The Court concluded that the unlawful actions of the website owner were obvious and that Stichting BREIN had made sufficient (unsuccessful) efforts to retrieve the personal data in another way.

Stichting BREIN/Leaseweb, Hof Amsterdam, 3 July 2008:[7] Stichting BREIN requested Leaseweb (an ISP) to disclose personal data of a website owner intentionally improving P2P file sharing, and therefore facilitating, copyright infringement through its website. The Court of Appeal concluded that the unlawful nature of the activities was evident. It ruled that the interests of Stichting BREIN - the protection of copyright of the RHs - outweighed the interests of the website host, not wasting time assessing the legitimacy of the request of the RH.

According to a statement of the Minister of Justice, the Lycos/Pessers decision and following decisions are in line with the decision of the European Court of Justice regarding the obligation to disclose personal data in the context of civil proceedings on copyright infringement.[8]

---

[5] Rechtspraak van de Week, 2005/133

[6] Computerrecht, 2007/46

[7] Intellectuele Eigendom & Reclamerecht, 2008/67

[8] Judgment of the Court of Justice in Case C-275/06, 29 January 2008, *Productores de Música de España (Promusicae) / Telefónica de España SAU*

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

(1) Criminal procedure

Within the boundaries described above under 2.3.(1), ISPs are compelled to disclose the identity of Internet users suspected of online copyright infringement upon request of police forces and judicial authorities based on their authority laid down in the Criminal Prosecution Act. For instance, Articles 126n et seq. of the Criminal Prosecution Act provide that a Public Prosecutor can request an ISP to disclose details of the transmission of communications and details of the user in case of certain severe crimes.

(2) Civil procedure

There is no specific procedure other than a civil action to compel ISPs to disclose the identity of P2P users. In cases concerning the identity of an infringing website owner, such disclosure has already been ordered by courts (see Stichting BREIN/KPN 2007 case cited under 4.1). Although there has not yet been any court judgment ordering the disclosure of the identity of a P2P user**,** it is likely that a court will order such disclosure if the Lycos/Pessers criteria are applicable.

B. Poland

Prepared by:
Xawery Konarski
Traple Konarski Podrecki Law Office
Cracow, Poland

Table of legislation

Denomination	Reference
DPA	Inspector General for the Protection of Personal Data (Generalny Inspektor Ochrony Danych Osobowych – GIODO)
Data Protection Act	Ustawa o ochronie danych osobowych, dated 29 August 1997, unified text – Journal of Laws of July 6, 2002, No. 101, item 926 with amendments
Police Act	Ustawa o Policji, dated 6 April 1990, unified text – Journal of Laws of February 12, 2007, No. 43, item 277 with amendments
Telecommunications Act	Prawo telekomunikacyjne, dated 16 July 2004, Journal of Laws of August 3, 2004, No. 171, item 1800 with amendments
Act on Providing Services by Electronic Means	Ustawa o świadczeniu usług drogą elektroniczą, dated 18 July 2002, Journal of Laws of September 9, 2002, No. 144, item 1204 with amendments
Criminal Code	Kodeks Karny of 6 June 1997, Journal of Laws of August 2, 1997, No. 88, item 553 with amendments
Code of Criminal Procedure	Kodeks Postępowania Karnego of 6 June 1997, Journal of Laws of August 4, 1997, No. 89, item 555 with amendments
Copyright Act	Ustawa o prawie autorskim i prawach pokrewnych, dated 4 February 1994, unified text – Journal of Laws of May 17, 2006, No. 90, item 631 with amendments
Civil Code	Kodeks Cywilny of 23 April 1964, Journal of Laws of May 18, 1964, No. 16, item 93 with amendments
Civil Procedure Code	Kodeks Postępowania Cywilnego of 17 November 1964, Journal of Laws of December 1, 1964, No. 43, item 296 with amendments

1. Nature of an IP address

1.1. Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

An IP address may be personal data. An IP address is not considered to be personal data as such (i.e., only in relation to a specific computer/IT system). An IP address may become personal data when it is linked to a particular natural person (Article 6 Data Protection Act). The DPA has stated that "when an IP address is […] allocated to a specific equipment which, in turn, is

allocated to a specific user then such an address should be treated as personal data." This position has been accepted by the Supreme Administrative Court in a judgment dated 3 February 2010 (no. II SA/Wa 1598/09).

An IP address is considered to be transmission data. Transmission data are defined as: "data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services" (Article 159 (1) point 3 of the Telecommunications Act). Transmission data are protected by the secrecy of telecommunications (Article 159-175 of the Telecommunications Act). Therefore, an entity performing telecommunications activities on public networks (e.g., ISPs), and entities co-operating with the ISP, are bound by the same secrecy obligation (Article 160 (1) of the Telecommunications Act).

Data protected by the telecommunications secrecy cannot be used by any entity other than the message sender and recipient (Article 159 (2) of the Telecommunications Act). There are some exceptions to this provision, in particular when: (1) the sender and recipient consent to such use; or (2) it is necessary for specific reasons provided for in the Telecommunications Act or separate regulations, like the Code of Criminal Procedure. For example, data protected by telecommunications secrecy, including IP addresses, may be collected, recorded, stored, processed, changed, deleted or made available only if the processing is conducted in the course of providing a service to the user or when it is necessary to perform such a service (Article 161 (1) of the Telecommunications Act).

An IP address is also traffic data. Traffic data are defined as: "data describing the way of using the service provided by electronic means by a service recipient [including] denotations identifying the telecommunications network terminal or a data transmission system, which have been used by a service recipient (…), information about commencement, termination and a range of every usage of the service provided by electronic means (…), information about using of the service provided by electronic means by a service recipient" (Article 18 (5) of the Act on Providing Services by Electronic Means). Note that other provisions may apply to the collection of IP addresses, for example Articles 266 and 267 of the Criminal Code.

1.2. Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the user?

Whether an IP address is considered to be judicial data is unclear, although we believe that IP addresses are not judicial data. Under Polish law, judicial data is a specific category of sensitive data and is defined as data "concerning sentencing, pronouncements on the imposition of punishment and fines and other pronouncements issued in court or administrative proceedings" (Article 27 (1) of the Data Protection Act). Since Article 27 (1) of the Data Protection Act concerns administrative matters, in our view it should be interpreted restrictively and be limited to information concerning previous convictions (Article 27 (1) of the Data Protection Act).

2. Processing and retention of IP addresses by ISPs

2.1. Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication? If so, can the ISP keep those data for the purpose of fighting online copyright infringement?

An IP address is considered to be transmission data (Article 159 (1) point 3 of the Telecommunications Act) and also traffic data (Article 18 (5) of the Act on Providing Services by Electronic Means). Pursuant to both the Telecommunications Act and the Act on Providing Services by Electronic Means, IP addresses may be lawfully processed by an ISP for the period needed to transfer a message or to perform online services. After that, IP addresses should be deleted. However, this rule is subject to exceptions.

IP addresses may be processed for the period needed for billing purposes (Article 165 (2) point 2 of the Telecommunications Act and Article 19 (2) point 1 of the Act on Providing Services by Electronic Means in relation to Article 118 of the Civil Code). However, the retention period cannot exceed three years from the recording of the data. IP addresses may also be processed for the period needed for marketing purposes (Article 165 (4) of the Telecommunications Act and Article 19 (2) point 2 of the Act on Providing Services by Electronic Means) with the subscriber's prior consent, unless consent is revoked.

IP addresses are subject to compulsory retention periods for national safety reasons. National safety reasons should be understood as including national defense, security and public safety, public order, obligations connected with a state of emergency, and the fight against serious crime. IP addresses must be retained for a 2-year (24 months) period from the recording of the data (Article 180a (1) point 1 of the Telecommunications Act).

According to the Copyright Act, disclosure of an individual's work in its original or in a derived form shall be subject to criminal liability. Thus, this form of copyright infringement now falls under the data retention legislation and ISPs must retain the data related to this type of copyright infringement. The retention obligation, however, relates only to ISPs which are "telecommunications entrepreneurs" and consequently only to ISPs which are registered with the Polish National Regulatory Authority ("Urząd Komunikacji Elektronicznej"), which are listed in the regulation of the Ministry of Infrastructure dated December 28, 2009 (Journal of Laws of December 31, 2009, No. 226, item 1828).

2.2. If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

(1) Criminal enforcement by judicial authorities

The retention of IP addresses is compulsory for national safety reasons, which includes, among others, criminal enforcement by judicial authorities.

(2) Civil enforcement by RHs

The processing of IP addresses for civil enforcement by RHs might be authorized on the grounds of Article 21 of the Act on Providing Services by Electronic Means, which reads as follows: "(1) If an electronic service provider becomes aware that a service recipient is using the service in violation of any regulations or applicable laws (e.g., copyright laws), it may process the latter's personal data to the extent that is necessary to establish the recipient's liability, provided that it has collected evidence of the misuse; (2) the service provider may notify the service recipient of his illegal activities and order that the recipient stop them immediately (...)." However, we must emphasize that there is controversy surrounding the issue of whether ISPs may disclose IP addresses to a third party in the context of civil proceedings (see below under 4.2(2)).

2.3. Can ISPs process IP addresses to pass on infringement notices to users? If so, under what conditions (consent, etc.)?

There is no special cooperation procedure between ISPs, RHs and the DPA. Passing on infringement notices to users by ISPs, which includes matching the details of the infringement and IP address to a particular subscriber, should be treated as personal data processing, and as such is subject to the regulations mentioned above.

In accordance with the general rules of the Data Protection Act, ISPs have to process the data on legitimate grounds. However, it is highly uncertain whether ISPs will be able to find a legitimate ground for the processing. In particular, it is unclear whether the balance of interest test (i.e., processing is necessary for the pursuit of the controller's legitimate interests) would be considered to be a legitimate ground (Article 23 (1) point 5 of the Data Protection Act). ISPs may process the data after obtaining the user's consent separately through the contract between the ISP and the subscriber, but not through the ISP's terms and conditions.

Please note that the processing of IP addresses in order to pass on infringement notices to users might be allowed pursuant to Article 21 of the Act on Providing Services by Electronic Means mentioned above. This issue is however unclear.

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

Under Polish law, the automatic monitoring of IP addresses which generates a list of copyright infringers is exclusively reserved to judicial authorities. RHs may only monitor copyright violations when the data are anonymized. As regards the filtering of IP addresses (which constitutes personal data processing), the same rules apply because filtering involves the processing of IP addresses. Regarding the communication of IP addresses collected by ISPs (but not RHs), Article 18 (6) of the Act on Providing Services by Electronic Means states that an ISP must provide the information on [traffic] data to the State authorities for the purposes of legal proceedings carried out by them.

3.2. If so, can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

There is no special cooperation procedure between ISPs, RHs and the DPA. There is also no Internet service provider association which deals specifically with illegal activities on the Internet, however, some initial activities in this regard are being taken by the IAB (Interactive Advertising Bureau Poland).

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntarily disclose users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

ISPs may (and must) disclose personal data to a third party in the context of judicial civil proceedings **(**DPA's Decision GI-DEC-DS-28/04). However, this decision has been criticized in Poland by legal commentators, who maintain that ISPs may not disclose users' data to RHs in order to bring civil actions.

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

(1) Criminal procedure

In criminal proceedings, ISPs may be obliged to disclose users' details. The Code of Criminal Procedure and the Police Act may apply and require ISPs to disclose the identity of Internet users suspected of online copyright infringement to judicial authorities.

In particular, Article 14 of the Police Act requires data controllers to disclose personal data to judicial authorities. The procedure compelling ISPs to disclose the identity of Internet users suspected of online copyright infringement is detailed in the Prime Minister's Regulation of March 8, 2002 (Journal of Laws of 2002, No. 24, item 245).

(2) Civil procedure

ISPs may (and must) disclose personal data to a third party in the context of judicial civil proceedings (DPA's Decision GI-DEC-DS-28/04).

The case involved an online operator who had initially refused to make personal data available to a third party seeking to bring an individual civil action against a data subject. The case was submitted to the DPA which decided that "*the purpose of bringing individual civil action constitutes a legitimate interest*" and the operator (i.e., personal data controller) cannot refuse to disclose the data processed in case they are necessary to pursue a legal claim. In its decision, the DPA justified its conclusion by indicating that Article 126 (1) point 1 of the Civil Procedure

Code allows data controllers (e.g., ISPs) to disclose the data necessary to bring an individual civil action.

However, this decision has been criticized in Poland, on the grounds that ISPs may not disclose users' data to RHs in order that they may bring civil actions for the following reasons: (1) Article 126 (1) point 1 of the Civil Procedure Code might not be a valid legal ground because it only covers pleading requirements (i.e., the items to be included in a pleading, such as the names and surnames of the defendants); (2) the DPA failed to consider other legal instruments (in particular the Telecommunications Act and the Act on Providing Services by Electronic Means) that protect the privacy and confidentiality of data subjects; and (3) the impact of the decision should be limited to the specific elements of the case. The case centered around a libelous statement that was made on an Internet forum, on the basis of which the applicant (i.e., the person trying to identify the forum user) was seeking to bring an individual civil action as well as a private criminal prosecution in accordance with the Criminal Code. Thus, the reasoning of the DPA's decision remains controversial.

C. United Kingdom[9]

Prepared by:
Peter Hall
Wragge & Co LLP
Birmingham, United Kingdom

Table of legislation

Denomination	Reference
ICO	Information Commissioner's Office
CA 2003	Communications Act 2003
Data Retention Regulations	Electronic Communications Data Retention (EC Directive) Regulations 2009
DPA 1998	UK's Data Protection Act 1998
DEA 2010	Digital Economy Act 2010
DEA Code	Online Copyright Infringement Initial Obligations Code
RIPA	Regulation of Investigatory Powers Act 2000
CDPA	Copyright, Designs and Patents Act 1988
CPR	Civil Procedure Rules
ATCSA	Anti-Terrorism, Crime and Security Act 2001
LBP Regulations	Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Telecoms and Privacy Regulations	Privacy and Telecommunications (EC Directive) Regulations 2003
OFCOM	Office of Communications

[9] The Draft Online Copyright Infringement Initial Obligations Code was published on May 28, 2010, and could thus not be discussed in the study.

1. Nature of an IP address

1.1. Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

Whether IP addresses are considered to be personal data is unclear and open to debate in the UK. An IP address will constitute personal data where a data controller has some means of linking it to a particular individual, whether through other information held or from information publicly available on the Internet. The ICO has published guidance confirming that whether or not an IP address may be considered to be personal data depends on the type of IP address. This guidance states that it is unlikely that the DPA 1998 covers dynamic IP addresses without any other identifying or distinguishing information. On the other hand, where a link is established, and profiles are created based on static IP addresses, the addresses and the profiles are personal data and are covered by the DPA 1998.

Arguably, an IP address is considered to be 'traffic data'. 'Traffic data' is defined as communications data which: (a) identifies, or appears to identify, any person, equipment or location to or from which a communication is or may be transmitted; (b) identifies or selects, or appears to identify or select, transmission equipment; (c) comprises signals that activate equipment used, wholly or partially, for the transmission of any communication; or (d) identifies data as data comprised in or attached to a communication (Section 21(5) RIPA). This would include IP addresses if they are required for conveyance of an e-mail or other communication. According to the UK Home Office's Draft Code of Practice entitled "Acquisition and Disclosure of Communications Data" (the "Code"), examples of traffic data include: (a) routing information identifying equipment through which a communication is or has been transmitted (for example dynamic IP address allocation); and (b) web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed.

1.2. Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the users?

An IP address that is personal data may be sensitive personal data under the DPA 1998 if that data is also connected to information which reveals that the data subject has committed, or allegedly committed, a criminal offence (see Section 2 (g) DPA 1998). As it can be a criminal offence to commit or to facilitate copyright infringement (Section 117 of the Copyright, Designs and Patents Act 1988 - CDPA), personal data linked to that activity may be sensitive personal data. However, such data will probably be processed as a result of a criminal investigation and the DPA 1998 provides some exemptions from many of the obligations for processing personal data for the purpose of a criminal investigation (section 29 DPA 1998), including non-disclosure obligations. Schedule 2 DPA 1998 allows sensitive personal data to be processed for the purpose of any legal proceedings, which means that the data subject's consent is not required.

2. Processing and retention of IP addresses by ISPs

2.1. Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication?

Regulation 7 of the Telecoms and Privacy Regulations states that traffic data processed and stored by public communications providers that relates to subscribers or users, should be deleted (or modified, so that it does not constitute personal data) when no longer required for the purpose of transmission of the communication. Regulation 8 does, however, permit the retention of traffic data for one or more of the following purposes: (1) the management of billing or traffic data; (2) customer enquiries; (3) the prevention and detection of fraud; or (4) the marketing of electronic communications services or the provision of a value added service. There is no prescribed retention period under these Regulations and traffic data should not be retained once these reasons no longer apply. These regulations, therefore, allow an ISP to store traffic data (including an IP address) for limited purposes.

However, the Secretary of State has introduced a voluntary code of practice relating to the retention of communications data (Part 11 of ATCSA): the Retention of Communications Data (Code of Practice). Communications data as defined under the Code include IP addresses. The Code of Practice sets out how communications service providers can retain data for extended periods of time based on one of the following purposes: (1) safeguarding national security; (2) assisting the prevention or detection of crime; or (3) aiding the prosecution of offences which may relate directly or indirectly to national security. The data that is retained can then be obtained by agencies under the Regulation of Investigatory Powers Act 2000. This voluntary Code of Practice does not prescribe a retention period.

Furthermore, if IP addresses are considered to be personal data, ISPs must comply with the general data protection principles. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or those purposes (second data protection principle). In addition, personal data that is processed for a specific purpose must not be kept for any period longer than is necessary for that purpose (fifth data protection principle). ISPs must therefore ensure that any IP addresses and subscribers' details are stored for a lawful purpose and that they are not kept any period longer than is needed to achieve this purpose. There is no prescribed period under the DPA 1998 for storage of personal data.

2.2. If so, can the ISP keep those data for the purpose of fighting online copyright infringement?

Under the Data Retention Regulations, ISPs must retain the following information relating to Internet access:

- The date and time of the log-in and log-off from the Internet access service;

- The IP address, whether dynamic or static, allocated by the Internet access service provider to the communication; and

- The user ID of the subscriber or registered user of the Internet access service.

This data must be retained for 12 months from the date of communication (the Internet access).

Access to that data may be obtained only in specific cases (i.e., on a case-by-case basis) and in circumstances where disclosure is permitted or required by law (e.g., by court order). If a court has granted a court order requiring the ISP to provide access (e.g., pursuant to a *Norwich Pharmacal* order - see 4.2. (2) below), this will allow the disclosure, as will any request by law enforcement authorities investigating copyright infringement. The new obligations of ISPs under the DEA 2010 also will constitute a legal basis for the disclosure of the data for the purpose of fighting copyright infringement.

2.3. If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

(1) Criminal enforcement by judicial authorities

Under the voluntary Retention of Communications Data Code of Practice, pursuant to ATCSA (see point 2.1), ISPs can retain IP addresses and subscribers' details if the ISP is satisfied that this is "necessary" to safeguard national security, assist in the prevention or detection of crime or aid the prosecution of offences that relate to national security. The Code does not deal with disclosure of this information.

Disclosure of this information to the following agencies is permitted under the Code of Practice to: (1) the police; (2) the Serious Organized Crime Agency (SOCA); (3) HM Revenue and Customs; (4) the Security Service; (5) the Secret Intelligence Service; and (6) the Government Communications Headquarters. Despite the voluntary nature of the Code of Practice, it is worth emphasizing that these agencies can require the disclosure of information under RIPA. Under the DPA 1998, personal data can be disclosed if the disclosure is required by or under an enactment, by any rule of law or by the order of a court.

(2) Civil enforcement by RHs

In order to justify the ISP's disclosure of an IP address to a claimant under civil enforcement proceedings, the claimant will normally require a *Norwich Pharmacal* order (see for example the *Motley Fool* case (see 4.2 below). However the DEA 2010 has introduced a new set of obligations on ISPs in relation to copyright infringement and aimed particularly at P2P activities and illicit file sharing. The DEA 2010 have been introduced as amendments to the CA 2003. These include:

- An obligation on ISPs to notify Internet subscribers, within one month, if the IP addresses associated with them have been reported by copyright owners as infringing their copyright. Copyright owners may make a copyright report to ISPs if and when a code of practice, approved by OFCOM, is introduced under the new provisions introduced by the DEA 2010.

- An obligation on ISPs to provide copyright owners with copyright infringement lists which "sets out, in relation to each subscriber, which of the copyright infringement reports […] relate to that subscriber, but (b) DOES NOT enable the subscriber to be identified" (i.e., an anonymized list of alleged serial copyright infringers). A copyright owner could then seek a *Norwich Pharmacal* order to obtain names and addresses of the relevant subscribers.

These obligations are subject to further clarification in the Online Copyright Infringement Initial Obligations Code (DEA Code). The terms of reference for that Code were published by OFCOM in April 2010. The draft DEA Code was published on May 28, 2010, and is now open for consultation until July 30, 2010.[10] It must be finalized by January 8, 2011, unless the Secretary of State extends that deadline. The draft DEA code includes a subscriber appeals mechanism.

2.4. Can ISPs process IP addresses to pass on infringement warning notices to users? If so, under what conditions (consent, etc.)?

See section 2.3 in relation to the new obligations of ISPs under the DEA 2010 on notification of users as to copyright infringements.

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

RHs and ISPs cannot monitor IP addresses or filter IP addresses for copyright enforcement purposes if the only way that they can obtain that data is to carry out unlawful interceptions or covert monitoring of IP traffic. Any form of surveillance of Internet traffic must only be carried out in accordance with RIPA and the LBP Regulations.

Under RIPA it is a criminal offence to intercept communications (i.e., telephone calls, e-mails and Internet use) taking place on a public telecommunications system. Interception on public networks is only permissible where lawful authority (i.e., a warrant under RIPA or the LBP Regulations) is obtained. On private networks, it is an offence for someone who does not control the system, or has not obtained express or implied consent from the parties to the communications, to intercept communications.

Section 17 of the DEA 2010 allows the "Secretary of State to make provisions about the granting by a court of a blocking injunction in respect of a location on the Internet which the court is satisfied has been, is being or likely to be used for copyright infringement." The Secretary of State can only make such regulations if satisfied that:

- The use of the Internet for copyright infringement is having a serious adverse effect on businesses or consumers;

[10] The draft Online Copyright Infringement Initial Obligations Code is available at http://www.ofcom.org.uk/consult/condocs/copyright-infringement/

- The making of regulation is proportionate;

- The making of regulations does not prejudice national security or the prevention of crime.

Prior notice of the blocking injunction must be given to the ISP and website operator.

3.2. If so, can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

See section 2.3 above in relation to the new obligations of ISPs under the DEA 2010 on notification of users as to copyright infringement.

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntarily disclose the users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

See section 2.3 in relation to the new obligations of ISPs under the DEA 2010 on notification of users as to copyright infringement.

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

(1) Criminal enforcement by judicial authorities

IP addresses fall within the definition of "traffic data", which in turn falls within the scope of the definition of "communications data", the collection and disclosure of which is regulated by RIPA. Communications data may only be obtained or disclosed by designated persons, which are individuals holding offices, ranks or positions within public authorities such as the police force, Commissioners of Her Majesty's Inland Revenue, the Financial Services Authority and Her Majesty's armed forces. Such designated persons may only obtain and disclose communications data after obtaining a warrant**,** when it is necessary, for example: (1) in the interests of national security; (2) for the purposes of preventing or detecting crime or of preventing disorder; or (3) in the interests of public safety (Sections 21-25 of RIPA).

(2) Civil enforcement by RHs

See section 2.3 in relation to the new obligations of ISPs under the DEA 2010 on notification of users as to copyright infringement.

ISPs can only disclose their users' details to RHs in order to bring a civil action if a court orders ("Norwich Pharmacal orders") the ISPs to make such a disclosure (Section 35 DPA 1998). Below, we provide details on some of the relevant case law on this topic.

Norwich Pharmacal Co. v Customs and Excise Commissioners [1974] AC 133: A Norwich Pharmacal order enables potential claimants to obtain information from third parties, which in

turn may enable the claimant to identify wrongdoers and trace the proceeds of wrongdoing. In recent years, Norwich Pharmacal orders have been the subject of case law developments, as illustrated below.

AXA Equity & Law Life Assurance Society plc v National Westminster Bank plc [1998] CLC 1177: Disclosure can be ordered where the claimant requires the disclosure of crucial information in order to bring a claim or where the claimant requires a missing piece of the information.

Totalise Plc v Motley Fool Ltd and another [2001] EWCA Civ 1897: Website operators should disclose the identity of wrongdoers (in this case, an offender posting defamatory material on a website operator's discussion board). The House of Lords emphasized that the Norwich Pharmacal line of authority, developed by 2001, was not restricted by Section 35 of the DPA 1998. It remains in the court's discretion whether or not to grant a Norwich Pharmacal order, which depends, among other things, on the strength of the claimant's case and whether the defendant had a confidentiality policy for website users.

Mitsui Limited v Nexen Petroleum UK Limited [2005] EWHC 625 (Ch): The following conditions must be satisfied before a Norwich Pharmacal order can be granted: (1) a wrong must have been carried out or allegedly carried out by a wrongdoer; (2) there must be the need for the order to enable action to be brought against the wrongdoer; and (3) the person against whom the order was sought must be somehow involved in the wrongdoing so as to have facilitated it, and must be able or likely to be able to provide the information necessary to enable the wrongdoer to be sued.

Helen Grant v Google UK Limited [2005] EWHC 3444 (Ch), 17 May 2005: The claimant, Helen Grant, was the trustee of the Individual Self-Discovery Trust (the "Trust"). The defendant was Google UK Limited. The Trust owned the copyright in a literary work called *Unlock Reality*, scheduled for UK and US publication in September and October 2006, respectively. The Trust discovered that an earlier draft of the work was available for free download on the Internet, through an advertisement generated by the Google Internet search engine, which used the name of the Trust's work. Having failed to discover the identity of the website's owners, the Trust asked for Google's help in identifying the advertiser. Google declined to assist. The Trustee applied for a Norwich Pharmacal order, requiring Google to disclose the identity of the advertiser. Google was ordered to disclose the identity of the advertiser responsible for the advertisement on its search engine. However, the Trustees were ordered to pay Google's costs.