The Coalition for Online Accountability

Participants:

American Society of Composers, Authors and Publishers (ASCAP)

Business Software Alliance (BSA)

Broadcast Music, Inc. (BMI)

Motion Picture Association of America (MPAA)

Recording Industry Association of America (RIAA)

Software and Information Industry Association (SIIA)

Time Warner Inc.

Walt Disney Company

---

c/o Business Software Alliance
50 Rue Wiertz
B-1050 Brussels Belgium
Tel: + 32 (0) 2 401 68 08
Fax: + 32 (0) 2 403 13 28

c/o Smith & Metalitz LLP
Suite 825
1747 Pennsylvania Avenue, NW
Washington, DC 20006-4637 USA
Tel: +1 202 833 4198
Fax: +1 202 872 0546

www.onlineaccountability.net

Counsel:

Smith & Metalitz LLP

Steven J. Metalitz
Email: metalitz@xxxxxxxxxxxxx

Ryan M. Lehning
Email: rlehning@xxxxxxxxxxxxx

Submission of the Coalition for Online Accountability

Public Consultation on Working Document 104

March 30, 2005

Introduction

The Coalition for Online Accountability (COA) welcomes this opportunity to participate in the public consultation on the Article 29 Working Party's Working Document on Data Protection Issues Related to Intellectual Property Rights ("Working Document").

The eight participants in COA (formerly the Copyright Coalition on Domain Names [CCDN]) are leading copyright industry companies, trade associations and member organisations of copyright owners. They include the American Society of Composers, Authors and Publishers (ASCAP); the Business Software Alliance (BSA); Broadcast Music, Inc. (BMI); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software and Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company. COA's goal is to enhance and strengthen online transparency and accountability by working to ensure that domain name and IP address Whois databases remain publicly accessible, accurate, and reliable, as key tools against online infringement of copyright, as well as to combat trademark infringement, cybersquatting, phishing, and other fraudulent or criminal acts online. All COA participants engage in substantial cross-border trade in copyrighted materials, including within the European Union, and all share significant interests in enforcement of copyright protection within the EU.

COA participants are strongly committed to data protection, both because privacy is critically important in its own right, and because we know that the Internet will flourish as a legitimate marketplace for copyrighted materials only if users are confident that their privacy is being protected. We believe that a constructive dialogue involving rights holders, privacy regulators, governments, law enforcement authorities and other key stakeholders is the most fruitful way to advance the common goals of establishing a balanced and workable data privacy regime that takes into account the full range of legal interests implicated by the

Internet. We welcome the contribution made by the Working Document to this dialogue, and commend the Working Party for initiating this consultation on it.

The Core Challenge

Our comments focus primarily on the portion of the Working Document that considers the data protection issues presented by protecting copyrighted material online, and in particular, the efforts of rights holders to investigate possible infringements of their protected works and take remedial action to stop that infringement (or enable law enforcement authorities to do so). This is an important issue for copyright owners, but it also bears critically on the future of the Internet as a venue for legitimate electronic commerce of all kinds. The application of data protection principles outlined in the Working Document would affect the enforcement of **all** laws applicable to online activity, including those prohibiting trademark infringement and counterfeiting, hacking, credit card fraud (*e.g.*, "phishing"), the distribution of racist material and material intended to incite hatred, child pornography, money laundering, and industrial espionage. There is nothing in EU data protection law that would justify treating enforcement of intellectual property law differently from the enforcement of any other law or regulation. Nor is there any basis for distinguishing between online and offline investigations in this regard.

The central conclusion of the Working Document seems to be that EU data privacy principles completely preclude rights holders, and by extension, other private actors, from engaging in affirmative efforts to rid the Internet of illegal content or to stop unlawful activity, to the extent that such efforts involve the processing of IP addresses and other investigative information that the Working Document treats as "judicial data". The Working Document states the view that "such investigations fall within the competence of judicial authorities" alone. This view, however, overlooks the critical role that private actors, both rights holders and other key industry players, can, do and must play in combating illegal and unwanted online content to advance the broader public good. As a practical matter, it would mean that individuals and companies are precluded from taking even the most rudimentary steps to protect their legal interests and the legal interests of others. Of course, data privacy must not be sacrificed to the enforcement of other laws and regulations. But we also believe that it is vitally important for regulators to make use of the flexibility in data protection law itself to facilitate, rather than undermine, online law enforcement.

For the reasons set forth below, we believe the Working Document does not strike the right balance in this regard, and should be re-examined.

The Status and Treatment of "Judicial Data"

1. Overview of WP's Position: In suggesting that online investigative activities by private parties may violate EU data protection principles, the Working Document relies heavily on Article 8 of Directive 95/46/EC, which it asserts is applicable whenever rights holders collect and process IP addresses or other personal information as part of their Internet monitoring

efforts. Article 8 was meant to create additional protections for personal data deemed to be "special", and so meriting additional protection. This includes so-called "judicial data", or "data relating to offences, criminal convictions or security measures". Specifically, Article 8(5) provides that:

Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be carried out under the control of official authority. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

According to the Working Document, IP addresses collected and processed by rights holders when monitoring the Internet for evidence of copyright theft, together with the related evidence of that theft, constitute personal information that is also "judicial data" and thereby qualify for additional protection.[1] The Working Document states that:

While any individual obviously has the right to process judicial data in the process of his/her own litigation, the principle does not go as far as permitting in depth investigation, collection and centralisation of personal data by third parties, including in particular, systematic research on a general scale such as the scanning of the Internet or the request of communication of personal data detained by other actors such as ISPs or controllers of Whois registries. Such investigation falls within the competence of judicial authorities.

The Working Document's conclusion is far too sweeping. It means that rights holders and other private parties are completely banned from gathering IP addresses and related evidence of infringement to enforce their rights (or for other law enforcement purposes) because such addresses constitute judicial data whose collection is impermissible <u>even</u> <u>if</u> right holders were to observe all other data protection principles in gathering and processing them (for example notice and proportionality). The Working Document appears to say that the gathering of IP addresses and other information relating to possible infringement is the <u>exclusive</u> province of law enforcement authorities. COA respectfully disagrees with this conclusion. In our view, it is unsupported by the text, context, or apparent intent of Article 8.

We also believe that the interpretation espoused by the Working Document would seriously impede the enforcement of a wide range of laws – including but certainly not limited to intellectual property laws – in the online environment. With respect to intellectual property

[1] Much of the analysis in the Working Document seems to rest on the unstated premise that IP addresses constitute personal data with respect to the activities addressed in the Working Document. In the view of COA participants, this premise is open to question, and we urge that it be re-examined. As a general rule, COA participants and others who seek to track infringing or other illegal behavior online lack the capability to link an IP address to any identifiable individual. An interpretation of the Data Protection Directive that treats IP addresses, standing alone, as personal data in these circumstances would needlessly raise a number of serious questions about the data protection implications of a host of commonplace online activities in which the processing of IP addresses is unavoidable.

rights in particular, this interpretation seems difficult to square with the strongly and repeatedly expressed view of EU institutions on the importance of civil enforcement of copyright by rightholders, including in the online environment. One recent formulation of this view can be found in the Intellectual Property Enforcement Directive, which focuses almost exclusively on civil enforcement, and which declares, "the means of enforcing intellectual property rights are of paramount importance for the success of the internal market". Council Directive 2004/48/EC, recital 3, **2004 O.J. (L157) 45, 46.**

2. Definition of Judicial Data: In our view, it is clear from the text and legislative history of Article 8 that the term "judicial data" has a much narrower scope than the Working Document gives it. "Judicial data" was intended to apply only to criminal records and registers indicating that a person is or has been involved in formal criminal proceedings. It does not apply to mere investigative data that is readily accessible to any Internet user, such as the IP addresses and related information at issue here.

a. The Text and Meaning of Article 8. The text of Article 8(5) explicitly refers to data on "offences" (**not** allegations, charges, or the suspicion of criminality) and "criminal convictions," as well as "registers" of criminal convictions. It also can be extended to include "administrative sanctions," and "judgements" in civil cases – all the final results of a formal adjudicative process. The import of this language is clear – for data to be "judicial data", it must arise in or directly from judicial proceedings. It does not apply to IP addresses or related evidence of infringement collected by rights holders that could, but may not necessarily, play a role in future legal proceedings.

This narrower application of Article 8(5) comports with common sense. The Working Party does not explain exactly how IP addresses and the related information collected by rights holders qualify as "judicial data", but presumably it reaches this result because such information *potentially* could be used in future criminal or civil proceedings to establish that a person or persons have committed copyright infringement. But, if information were to qualify as "judicial data" on this basis, it effectively would mean that any organisation that engages in even the most tentative investigation into potential wrongdoing, whether in its own workplace, online or anywhere else for that matter, would be involved in the improper processing of "judicial data". That would be an absurd result. In this respect, the Working Document explicitly states that "in depth" investigations online are unlawful, creating the impression that in its view, more cursory reviews might be allowed. But there is nothing in Article 8 that would justify such a distinction, and it would make no sense to conclude that an investigation into possible wrongdoing is allowed only to the extent that it is ineffective or incomplete.

b. The Legislative History of Article 8. The legislative history of Article 8(5) also indicates that "judicial data" should be understood in this narrower sense. Precursors to Article 8(5) appearing in early drafts of the Directive, including the EU Commission's initial proposal in 1990, the amended Commission proposal in 1992, and the compromise text prepared by the EU Presidency, directly referred to "data concerning criminal convictions". Although this language later was modified into its current form, the underlying concern of the drafters was by then very clear – to restrict the ability of unofficial bodies and private parties to collect and process

information which revealed that persons had committed, or were being prosecuted for committing, a criminal offence or civil violation. In light of how damaging such information can be to an individual with respect to their employment, family relations and in other legal proceedings, it is hardly surprising that the Directive's drafters decided to include this provision.

3. Safeguards for Judicial Data: Even if IP addresses and other investigative information were "judicial data" within the meaning of Article 8, the Directive calls for "appropriate safeguards" to be applied to their processing, not an outright ban. Indeed, the Directive specifically refers to the adoption of "suitable specific safeguards" – not once, but twice – in instances where Article 8(5) is implicated. In this respect, the Working Document represents a missed opportunity of considerable proportions. It could have been used to articulate the safeguards that are appropriate to protect judicial data consistently among the member states. Given the critical importance of investigative data to enforcement not only of intellectual property rights but all laws regulating the Internet, such a clarification could be of immense value to all Internet stakeholders[2].

The Working Document also quotes extensively from the Working Party's previous opinion (Opinion 2/2003, 10972/03/EN final, WP 76) regarding Whois directories. That opinion raises questions about whether the use of Whois data to ascertain the parties responsible for infringing activity online is compatible with the purposes for which the data was collected. In the view of COA participants, there is no incompatibility here: since their inception, the information in Whois databases (at least in the environment of generic Top Level Domains) has always been collected and made available to the public primarily for the purpose of enabling contact with the operators of online resources to which domain names resolve. This is essentially the same use to which right holders put this data today. While it is regrettable that the Working Party chose, in 2003, to issue its opinion without the public consultation process which it commendably is employing with respect to the current Working Document, COA participants would welcome the opportunity for further discussion with the Working Party and interested members on the issue of Whois data.

Digital Rights Management

COA offers the following brief comments on the portion of the Working Document that addresses digital rights management (DRM). DRM systems are already in widespread use, including by many COA participants. These systems have generally been well received by consumers, and are already beginning to realize their potential to greatly increase authorized public access to materials protected by copyright and neighboring rights, while providing greater security against infringing uses. Applicable European legislation, notably the Copyright Directive, provides legal protection for DRMs, with the goal of promoting their uptake.

---

[2] The Working Document's reference to the Intellectual Property Enforcement Directive does nothing to strengthen its argument. Article 8 of that Directive sets forth the conditions under which Member States may order a party connected with infringement to produce information relevant to that infringement. But Article 8 does not in any way constrain the ability of a rights holder to conduct its own investigation to obtain such information, nor was it meant to. It would misconstrue the Enforcement Directive to cite it as authority for the proposition that its enactment was meant to make it more difficult for rights holders to protect their works online.

The discussion in the Working Document of the data protection implications of DRM is at a high level of generality. Of course the operation of DRM systems must respect applicable data protection rules, but COA participants do not believe that, to date, there has been much difficulty in achieving this goal. We observe that, in most cases, DRM is employed within the context of licensed access to protected materials, and therefore whatever processing of personal data is involved could, in principle, be justified by the user's informed consent. As the role of DRMs in the marketplace develops further, it may be useful for the members of the Working Party to exchange ideas and experiences with developers and users of these systems to ensure that, in practice, these systems are deployed and operated in a manner that respects data protection principles.

The Broader Issues at Stake

1. The Internet and the Public Good: By any measure, the Internet has contributed enormously to advancing the public interest, inspiring some of the most dramatic examples of technological, social and economic progress in modern history. Unfortunately, in addition to creating immense opportunities, the borderless and anonymous character of the Internet also makes it an attractive medium for those who wish to disseminate unlawful content or engage in illegal activities, which can cause actual harm to users. These activities also have far-reaching economic consequences. For example, the software industry alone estimates that it lost over €10 billion to piracy in 2002, much of it due to online piracy. The effects of online piracy have also hit the music industry. Illegal file-sharing has been a key factor in the recording industry's 25% global decline over 1999-2004, and potential losses to the industry from file-sharing in 2004 alone have been independently estimated at €1.7 billion. Losses of this sort have an impact not only on copyright industries and their ability to invest in the creation of additional works, but also on European economies, which incur losses in the form of lost jobs and lost tax revenues. These problems have not escaped the attention of EU lawmakers. In announcing its 2004 "Safer Internet Plus Program", the European Commission noted that Internet users increasingly must contend with unsuitable and illegal content, such as spam and computer viruses.

2. The Importance of Public-Private Partnerships: Faced with these challenges, the private sector, with the encouragement, cooperation and support of lawmakers and law enforcement agencies, plays an indispensable role in protecting Internet users and dealing with illegal activities online. This role is carried out not only by copyright owners, but also by financial institutions, telecommunications providers, Internet service providers (ISPs), and others. The global banking community, for example works diligently to rid the Internet of those engaged in identity theft and online fraud. Firms offering online security are similarly engaged, working to identify networks of compromised computers (*i.e.*, "botnets") used to launch attacks on web sites or distribute unsolicited mail that frequently contains computer viruses and worms. Online auctioneers have been involved in detecting and disabling "spoofing" web sites intended to elicit personal and financial information from unsuspecting Internet users. Pharmaceutical firms are now pro-actively searching the Internet for evidence of counterfeit medicinal products, including counterfeit prescription drugs. And, as the Working Party is aware, intellectual property rights holders invest significant resources in an effort to prevent the online distribution of counterfeit and unauthorised copies of their works. Yet if the interpretation of data protection principles

espoused in the Working Document were to be adopted, it would bring an end, for practical purposes, to all these varied initiatives of Internet stakeholders. That could not fail to set back all efforts to rid the Internet of illegal content and unlawful activities, and to protect online security that prevents hackers from gaining illegal access to individual's personal information.

COA participants, as well as other rights holders, continue to work with governments, law enforcement agencies and industry colleagues to address the key challenges arising from illegal uses of the Internet, including copyright infringement, spam and online child safety. The software industry, for instance, recently collaborated with the UK's National Hi-Tech Crime Unit (NHTCU), the Federation Against Copyright Theft (FACT), the US Federal Bureau of Investigation and US Department of Justice to trace and prosecute online software piracy rings in 8 EU Member States, including Belgium, France, Germany and the UK. The music industry has also recently cooperated closely with governments and local enforcement agencies to combat online piracy. Collaboration in the litigation and prosecution of online infringement cases has recently taken place in several countries, including Germany, France, Austria and Italy. These activities are important facets of good corporate citizenship and, more importantly, they make a material and irreplaceable contribution to society's overall efforts to make the Internet environment safer, more productive, and more beneficial to consumers throughout Europe and beyond.

3. The Long Term Impact of the Working Party's Paper: By broadly defining "judicial data", imposing an outright ban on collection of such data by private parties, and ignoring the explicit provisions of EU legislation looking to the adoption of safeguards to facilitate the collection of judicial data while at the same time protecting it, the Working Document's approach would effectively shut down private-public partnerships to ensure the safety and security of the Internet. The fact is that law enforcement bodies often simply lack the necessary resources or technical sophistication to combat effectively criminal activities perpetrated online. Although law enforcement agencies often are willing to act on the evidence that rights owners have amassed through their own investigative efforts, they are unlikely -- and often unable -- to dedicate their own scarce resources to pro-active investigations into online copyright theft or other online criminal activity. Simply put, without the private sector investigative activity that the Working Document appears to condemn, enforcement of the laws in the online environment would be greatly hampered.

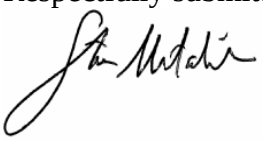
The net result of the Working Document would be to suspend altogether these and other valuable private-sector initiatives to advance the public good by promoting an Internet free of illegal or undesirable content, whether it be counterfeit products, computer viruses, child pornography or a host of other online ills. Moreover, it would do so on the basis of what remains a controversial application of EU data privacy principles that deems IP addresses to be protected personal data, adopts a sweeping and unjustified definition of judicial data, and gives law enforcement agencies the exclusive authority to search for evidence of online violations. We do not believe that the Working Party intends this result, and we urge it to continue to explore and examine these issues rather than finalizing the Working Document in its current form. Although rights holders agree that EU privacy principles have an important role to play in shaping the permissible bounds of such private-sector initiatives, we believe it essential that those principles

be applied in a way that takes account of this "bigger picture", for the good of all. In our view, the Working Document falls well short in this regard.

* * *

COA strongly agrees that EU data protection law applies to personal information that is gathered in the course of an investigation of possible wrong doing. We believe however that EU law does not preclude the processing of such investigative information, but instead envisions the application of principles and safeguards to protect it in an appropriate way. By applying the flexibility envisioned in EU data protection law, the Working Party can strike an appropriate balance between effective law enforcement on and offline, while respecting individual privacy. We urge it to engage in further dialogue with all interested parties with the goal of striking a more appropriate balance than is reflected in the Working Document.

Respectfully submitted,



Steven J. Metalitz
Counsel, Coalition for Online Accountability
Email: metalitz@smimetlaw.com