The Coalition for Online Accountability

August 30, 2005

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 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@smimetlaw.com

Ryan M. Lehning
Email: rlehning@smimetlaw.com

COA Comments on auDA Whois Policy Review

The Coalition for Online Accountability (COA) consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners. They are 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.

AuDA (.au Domain Administration Ltd.) is seeking comment on its review of the auDA Whois Policy for the Australian country code Top Level Domain (ccTLD). *See* Whois Policy Review - Aug 2005, *at* http://www.auda.org.au/reviews/whois-2005/. At this point, auDA is not proposing a policy change with respect to Whois, but is simply seeking comment on the policy it currently has in place. *See* Whois Policy (2003-08), *at* http://www.auda.org.au/policies/auda-2003-08/.

COA appreciates this opportunity to comment on auDA's Whois policy. We urge the organization to expand the scope of public access to Whois information. As in other Top Level Domains, such Whois information is a critical tool for providing transparency and accountability on the Internet.

Why Public Access to Whois Data is Vital

Public, real-time access to accurate and reliable Whois data in all domain name registries, including country-code Top Level Domains (ccTLDs), is a vital concern for all Internet stakeholders, including intellectual property owners, law enforcement, and the public at large.

Copyright owners face an epidemic of online piracy. In the online environment, near limitless numbers of unauthorized, digital copies of music, movies, and software can be made and distributed worldwide with the stroke of a key. Whois is a key tool for investigating these cases and identifying the parties responsible. Though no piracy case can be resolved through the use of Whois alone, nearly every case involves the use of Whois at some point.

Many copyright owners are likewise trademark owners, and the use of Whois for trademark enforcement is equally important. Trademark owners use Whois to combat cybersquatting, the promotion of counterfeit products online, and a wide range of other infringement problems. Trademark-owning businesses also depend on accurate and publicly accessible Whois for a number of other critical business purposes, such as trademark portfolio management, conducting due diligence on corporate acquisitions, and identifying company assets in insolvencies and bankruptcies.

Law enforcement also needs quick, real-time access to publicly available Whois in order to swiftly investigate online crimes. And while Whois is by no means the sole tool used by law enforcement investigators, many, if not most, online criminal investigations employ the Whois database to determine who is operating sites engaged in illegal conduct. Importantly, in the context of many investigations, law enforcement relies heavily on the private sector to bring information and build cases in advance of criminal and civil enforcement proceedings. Open access to Whois information for all users, the public and law enforcement alike, goes a long way to combating illegal online activity.

Finally, and perhaps most importantly, individual Internet users need access to publicly available Whois information. Consumers visiting websites, shopping or conducting other transactions over the Internet have a strong interest in avoiding fraud. The recent epidemic of "phishing" attacks gives credence to this concern as a number of institutions have been the victims of corporate identity theft. Such harms directly affect individuals who pass on sensitive, personal financial information believing they are in contact with trusted banks, credit card companies, or retail institutions. Publicly available Whois information is an important tool in combating such fraud by empowering consumers to verify the identity of the sites soliciting their information.

AuDA's Current Whois Policy

Whois Policy (2003-08) covers the collection, use, and disclosure of Whois information in five open second level domains under the .au ccTLD: .asn.au (associations); .com.au (commercial interests); .id.au (individuals who are residents or citizens of Australia); .net.au (commercial entities);[1] and .org.au (non-profit organizations). *See* Whois Policy (2003-08), *at* http://www.auda.org.au/policies/auda-2003-08/.

As it currently stands, the contact information provided in the .au Whois is much less robust than that provided in the gTLD environment and covered by ICANN's Registrar Accreditation Agreement. According to Whois Policy (2003-08) the following contact information is provided in .au Whois: registrant name (presumably a person or organization name); registrant ID; registrant contact name (name of a contact for the registrant); registrant email address; technical contact name; technical contact ID; and technical email address. *Id*. at Schedule A. In comparison, the Registrar Accreditation Agreement (RAA) requires ICANN accredited registrars to provide the following contact information in the Whois database: the name and address of the registrant; name, address, email address, telephone and (where available) fax numbers of the administrative and technical contacts. *See* Registrar Accreditation Agreement, Secs.3.3.1.6-3.3.1.8, *at* http://www.icann.org/registrars/ra-agreement-17may01.htm. COA notes that the data publicly available in the .au Whois database is extremely limited, whether the registrant is a multi-million dollar corporation doing business with thousands of consumers, or a single registrant who is posting information on a non-commercial, personal website. Clearly, the privacy concerns are minimal if non-existent in the former context at least. Thus the restrictive character of au

[1] According to AuDA's website, the requirements for registration in .com.au and .net.au appear identical. *See* .au Second Level Domains (2LDs), *at* http://www.auda.org.au/domains/au-domains/.

DA's current policy on public access to Whois is particularly problematic with respect to .asn.au, .com.au, and .net.au.

It seems that auDA's rationale for so striking a limitation on available Whois data arises from perceived incompatibility with Australian privacy laws. *See, e.g.,* Whois Policy (2003-08), Sec. 4.2 ("In order to comply with Australian privacy legislation, the street address, telephone and facsimile numbers of registrants will not be disclosed."). Furthermore, auDA claims that it has crafted its policy in order to weigh the interests of: registrants, in the use of their personal data; auDA in fomenting a competitive domain name industry; and "law enforcement agencies in accessing information about domain names for consumer protection and other public interest purposes." *Id*. at Sec. 2.2(a)-(c). COA respectfully disagrees with these assessments, finding no rationale in Australian privacy legislation that would prohibit auDA from making more robust Whois information publicly available. We also note that auDA has failed to weigh, in its policy calculus, the strong public interest in public access to Whois data, for all the reasons summarized in the preceding section of this submission. We submit that, if this public interest were considered, a different balance would be struck.

In addition, COA is concerned about auDA's prohibition on the use of Whois data "to allow, enable or otherwise support the transmission of unsolicited communications to any person, by any means." Whois Policy (2003-08), Sec. 5.1(a). While we believe auDA's intent is to limit unsolicited bulk email (e.g., spam), we believe this phrasing is far too broad, and may unintentionally encompass important enforcement activities, such as contacting those engaged in online copyright infringement or other illegal activities. COA recommends this provision be significantly narrowed to make clear that prohibitions on use cover only spam.

Australian Privacy Legislation and Whois

The Privacy Act of 1988 governs the collection and disclosure of personal information in a variety of contexts. *See* Privacy Act 1988, Act. No. 119 of 1988 as amended. The National Privacy Principles, as codified in the Privacy Act, govern the way in which private sector organizations, including domain name registrars and registries, can collect and disclose personal information, unless that organization is covered by a binding, approved privacy code. *See id*. at Pt. III, Div. 3, Sec. 16A; *id*. at Schedule 3: National Privacy Principles.[2]

Under National Privacy Principle 2.1, organizations are generally prevented from "disclos[ing] personal information about an individual for a purpose (the *secondary purpose*) other than the primary purpose of collection." National Privacy Principle 2.1. The auDA Whois Policy (2003-08) states in Section 2.1: "The purpose of the WHOIS service is to allow users to query a domain name to find out the identity and contact details of the registrant." If this is the primary purpose for which Whois data is collected, it does not appear that there would be any legal impediment to making publicly accessible a broader range of Whois data (as has always been the case in the gTLD environment), as this would enhance the ability of the service to achieve its purpose: enabling members of the public c to contact the registrant.

However, even if broader disclosure would be considered as advancing a "secondary purpose" under the National Privacy Principles, personal information may be disclosed under those principles if "the individual has consented to the use or disclosure." *Id*. at 2.1(b). "Consent" is defined quite broadly

[2] For the purposes of this comment we assume that auDA, as a private organization, is covered by the National Privacy Principles.

under the Privacy Ac, to include either "express consent or implied consent." Privacy Act, Sec. 6(1) (definition of consent). In short, there is nothing in Australian law that would prohibit a registrar or registry from disclosing information in a Whois database so long as a registrant has given express or implied consent to such disclosure. [3]

In addition to other permitted disclosures, the National Privacy Principles provide that an organization may disclose personal information, as a part of its own investigation pursuant to a belief that an individual is involved in illegal activity. *See id.* Sec. 2.1(f). Under Principle 2.1(f),

> An organisation must not use or disclose personal information about an individual for a purpose (the *secondary purpose*) other than the primary purpose of collection unless. . . the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities. *Id*.

This provision would allow a registrar to disclose personally identifiable information about a user if the registrar has reason to believe the user was engaged in illegal activity, such as copyright infringement. Notably, it seems the registrar would not need the user's prior consent to disclose for this purpose. This comports with the provisions, applicable in the gTLD environment, of Sec. 3.7.7.3 of the ICANN Registrar Accreditation Agreement, which allow registrars to offer so-called "proxy" registration services so long as they reveal the identity of the actual registrant when presented with "reasonable evidence of actionable harm." COA believes that such proxy registration systems, which replace registrant contact data with registrar data, may provide one reasonable alternative to a policy which would remove important Whois data from the publicly accessible database altogether. We note, however, that such proxy registration systems are only effective if actual registrant data is verified at the time the registration occurs, and such data is promptly disclosed when the registrar or registry is presented with reasonable evidence of illegal activity.

AuDA's Balance of Interests

Finally, while COA appreciates auDA's attempts at crafting a carefully balanced policy, we are concerned that auDA appears to have ignored a vast set of Whois users whose access is vital to the Internet economy as whole: ordinary individuals, consumers, and other private, non-governmental actors.

Under Sec. 2.2(c) of Whois Policy (2003-08), law enforcement agencies are identified as an interest group which needs "access[] to information about domain names for consumer protection and other public interest purposes." This implies that only law enforcement needs access to Whois data and that law enforcement agencies, alone, have the resources to conduct all consumer protection and other enforcement activities. Resources are scarce for law enforcement agencies worldwide; they rely on private parties to collect information and bring evidence not only for criminal enforcement proceedings,

[3] Australia's Telecommunications Act, to the extent it is applicable to auDA, similarly is not a bar to providing more detailed contact information in the Whois database. The Act allows information to be disclosed if "the information or document relates to the affairs or personal particulars" of an individual, and the individual consents, or if that individual "is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned." Telecommunications Act 1997, Pt. XIII, Div. 3, Sec. 289(b). A similar provision allows for implied consent for disclosure of certain information if "it might reasonably be expected that the sender and the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use." *Id*. at Sec. 290.

but for civil proceedings as well. COA's participating organizations have considerable experience in cooperating with law enforcement, in Australia as well as in other jurisdictions, in investigations aimed both at enforcing intellectual property rights, and at protecting consumers against misrepresentations and fraud. Furthermore, the ability of consumers and other members of the public to investigate and seek civil redress for illegal online practices that adversely affect them conserves law enforcement resources for the more serious, complex and dangerous cases. In sum, it seems incontrovertible that broader public access to a more robust set of Whois data will materially assist law enforcement agencies in their task of combating phishing, fraud, and other illegal activities carried out online, and will vindicate other important public interests as well.

Conclusion

COA urges auDA to consider expanding the amount of Whois data displayed in the publicly accessible database, and to ensure access to that data for all Internet stakeholders, not just law enforcement. COA would welcome the opportunity to discuss these and any other proposals with auDA, and appreciates the opportunity to submit these comments.

Respectfully submitted,

Steven J. Metalitz
Counsel
Coalition for Online Accountability

Smith & Metalitz LLP
1747 Pennsylvania Ave., NW, Suite 825
Washington, DC 20006 USA
tel: (+1) 202/833-4198
fax: (+1) 202/872-0546
e-mail: metalitz@smimetlaw.com
web: www.onlineaccountability.net