Database Protection and Privacy Rights

An Analysis of EU and US National Law

http://www.palage.com/database-dataprivacy.pdf

Executive Summary

- The objective of this presentation is to highlight the differences between US and EU national laws in connection with database protection and data privacy.

- Resolution of the complexities surrounding accuracy and access to Whois data cannot be meaningfully achieved until the participants in this discussion fully appreciate the conflicting differences between national laws.

- Those parties which have a vested interest in the Whois discussion include: governments, law enforcement, registration authorities, intellectually property owners, businesses, and individuals.

Michael D. Palage
Michael@Palage.com

Executive Summary - European Union Overview

- The European Union currently encompasses approximately 375 million people living in the following fifteen (15) member states: Belgium, Germany, France, Italy, Luxembourg, Netherlands, Denmark, Greece, Spain, Ireland, Austria, Portugal, Finland, Sweden, and the United Kingdom.

- Under the Treaty of Nice, twelve (12) new member states are eligible to join the union.

  - In May 2004, ten (10) new members states with over 70 million citizens are expected to join: Latvia, Lithuania, Estonia, Poland, Hungary, the Czech Republic, Slovakia, Slovenia, Malta and Cyprus
  - In 2007 two (2) new member states are expected to join: Bulgaria and Romania.

- Turkey's application for membership is scheduled for review in December 2004.

- In order to join the European Union, would-be members must bring their national laws into conformity with the union strict criteria.

Michael D. Palage
Michael@Palage.com

US Database Protection – Historical Analysis

- The US Supreme Court decision in ***Feist Publications, Inc. v. Rural Telephone Service Co***., 499 U.S. 340, 1991 is currently the leading case on database compilations under US law.

- Prior to *Feist,* several US courts had granted copyright protection to authors if they expended a significant amount of time and effort in assembling the database. This protection was coined “sweat of the brow” protection.

- Feist had sought to compile a regional telephone directory combining yellow and white pages listing covering 11 different telephone service areas in 15 counties. Feist obtained licenses from all of the regional telephone monopoly operators except Rural Telephone Service.

- Feist and the regional telephone operators vigorously competed for business listings in the the yellow pages portion of the directory publication.

- Feist sought to independently verify the information contained in the Rural directory which comprised approximately 7,700 listings.

Michael D. Palage
Michael@Palage.com

US Database Protection – Historical Analysis

- Notwithstanding this attempt to independently verify this information, 1,309 of the 46,878 listings contained in Feist's directory matched the Rural directory, including four **red herring** database entries.

- The District Court granted summary judgment in favor of complainant Rural on its claim for copyright infringement, holding that telephone directories were copyrightable. The Court of Appeals affirmed.

- The Supreme Court reversed, finding that Rural 's white pages were not entitled to copyright protection and explicitly repudiated the "sweat of the brow" doctrine holding that "**copyright rewards originality not effort**."

  - Facts are not copyrightable as they do not owe their origin to an act of authorship;
  - Compilations of facts may qualify for copyright protection where the compiler undertakes a degree of creativity in the selection and arrangement of facts.

Michael D. Palage
Michael@Palage.com

US Database Protection – Post Feist

- Following the Supreme Court's decision in Feist, attorneys representing clients seeking to protect database works have resorted to a variety of legal theories, including:
  - Contract
  - "Hot News" Doctrine
  - Electronic Trespass
  - Deep Linking

Michael D. Palage
Michael@Palage.com

US Database Protection – under the theory of contract law

- In ***ProCD v. Zeidenberg***, 86 F.3d 1447 (7th Cir. 1996) Plaintiff, ProCD, had complied a comprehensive telephone directory database available on a 5 CD-ROM set that was marketed to businesses and consumers through different channels. ProCD had invested over $10 million dollars in the compilation of the database, and the data in the database was stored in a proprietary compressed format which also served as an encryption safeguard.

- Defendant, Zeidenberg, purchased a consumer copy of the ProCD software application and extracted all of the underlying data from the database and set up a competing telephone directory service on the Internet.

- Every box containing the consumer software application had a statement that the software comes with restrictions stated in an enclosed license.

- The license limiting the use of the application program and listings to non-commercial purposes was encoded on each of the CD-ROM disks, printed in the manual, and which appeared on the user screen every time the application was run.

Michael D. Palage
Michael@Palage.com

US Database Protection – under the theory of contract law

- The district court held the licenses ineffectual because the terms do not appear on the outside of the package. The district court also added that the second and third licenses stand no different from the first, even though they are identical, because they might have been different, and a purchaser does not agree to --- and cannot be bound by – terms that were secret at the time of purchase.

- The Court of Appeal remanded with instructions to enter judgment for the plaintiff, holding that shrinkwrap licenses were enforceable since they were not unconscionable or violate a rule of positive law.

Michael D. Palage
Michael@Palage.com

US Database Protection – under the "hot news" doctrine

▪ The "hot news" doctrine was originally set forth in the 1918 Supreme Court decision of ***International News Service v. Associated Press***, 248 U.S. 215 (1918).

▪ In *INS,* the Supreme Court held that it was possible for a party to hold a property right in "hot news" that it acquired, and set forth the following criteria to consider in making this determination:

- plaintiff generates or collects information at some cost or expense, or the value of the information is highly time sensitive;
- defendant's use of the information constitutes free-riding on the plaintiff's costly efforts to generate or collect it;
- defendant's use of the information is in direct competition with a product or service offered by the plaintiff; and
- the ability of other third parties to free-ride on the efforts of the plaintiff would so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened.

▪ Many states have incorporated the INS misappropriation doctrine into their statutes.

Michael D. Palage
Michael@Palage.com

US Database Protection – under the "hot news" doctrine

- In ***NBA v. Motorola, Inc.*** 105 F.3d 841, (2d Cir. 1997) the NBA filed suit against Motorola for transmitting statistics on basketball games to pages alleging copyright infringement and misappropriation of their broadcast rights.

- The Second Circuit rejected the NBA's copyright claims holding that basketball games and other athletic events were not original works of authorship so that the scores were not protected by copyright.

- Applying the "hot news" doctrine, the Second Circuit held that the NBA did not show any direct competitive effect by Motorola's service, nor had it been shown that Motorola was enjoying a "free ride."

- However, in ***Morris Communication Corp., Inc. v. PGA Tour, Inc.*** 117 F.Supp. 2d 1322 (M.D.Fla. 2000) the court upheld a misappropriation claim based upon the hot news doctrine.

Michael D. Palage
Michael@Palage.com

US Database Protection – under the "hot news" doctrine

- In ***Morris Communication***, Plaintiff PGA Tour had developed a "Real Time Scoring System (RTSS) to compile golf scores in real time. The PGA Tour sponsors professional events held on private golf courses, in which the media is only permitted to attend under certain terms and conditions. Specifically, media companies are permitted to publish complied scores after a 30 minutes delay which grants the PGA Tour and its syndicated news outlets the right to publish these scores and statistics first.

- Morris had sought to obtain access to the RTSS information and publish in real time via the Internet. After being declined access. Morris filed suit against the PGA Tour alleging that they had engaged in unfair competitive practices. The PGA Tour responded by claiming a property right in their golf scores.

- The district court ruled that PGA Tour golf scores were protected under "hot news" doctrine. The district court distinguished the facts in this case from the *NBA* case, holding that in basketball there is one score available to all they viewers, whereas in golf there are multiple scores which are generally not available in real time.

Michael D. Palage
Michael@Palage.com

US Database Protection – under the theory of "electronic trespass"

- In ***Register.com Inc. v. Verio Inc.***, 126 F.Supp.2d 238 (S.D.N.Y. 2000) Register.com filed suit against Verio to enjoin it from accessing its online Whois database to obtain subscriber information.

- According to the Register.com Whois license, use of the Whois data was prohibited for unsolicited commercial advertisements via, direct mail, electronic mail, or by telephone.

- Verio utilized computer scripts to obtain the contact information in connection with recently registered domain, which Verio's sales staff then called to offer web hosting services.

- The district court granted Register.com request for a preliminary injunction to prohibit Verio's conduct. This case is currently on appeal to the Second Circuit.

- See also ***eBay Inc. v. Bidders Edge Inc.*** 100 F.Supp.2d 1058 (N.D.Cal. 2000) where the Court held that Bidders Edge's spidering of the eBay's auction website in violation of the **robots.txt** file constituted an electronic trespass.

Michael D. Palage
Michael@Palage.com

US Database Protection – under the theory of "deep linking"

- There have been a number of cases involving "deep linking" in which various legal claims such as copyright, trademark, and unfair competition have been raised.

- In ***Washington Post Co. v. Total News***, 97 Civ. 1190 (PKL) (S.D.N.Y. 1997), a group of media companies filed suit against defendant alleging unfair competition, trademark and copyright infringement in connection with framing plaintiffs' news articles within the web browser at the defendant's website. The case was settled after the defendant agreed to link directly to the news article instead of framing them in the browser window.

- Similarly in ***TicketMaster Corp. v. Microsoft Corp***, 97-3055 DPP (C.D.Cal. 1997) complaint by plaintiff alleging trademark dilution and unfair competition was settled after defendant removed the deep links.

- However, in ***TicketMaster Corp. v. Tickets.com Inc.***, 54 U.S.P.Q.2d 1244 (C.D.Cal. 2000) the court held that the defendants deep linking did not constitute copyright infringement nor unfair competition.

Michael D. Palage
Michael@Palage.com

US Database Protection – Possible Legislation

- There have been several legislative proposals introduced before the United States Congress over the years to provide new protection for database works.

- In May 1996, Representative Carlos Moorhead introduced the first database protection bill, entitled the Database Investment and Intellectual Property Anti-Piracy Act of 1996 (HR 3531)

- In October 1997, Representative Howard Coble introduced the "Collections of Information Antipiracy Act" (HR 2652). Although this bill passed the House in May 1998, the Senate did not take it up. Subsequently, the text of HR2652 was included into the Digital Millennium Act (HR2281). However, the final DMA bill that passed into law did not include the database language.

- In January 1999, Representative Coble re-introduced the Collections of Information Antipiracy Act" (HR 354).

- In May 1999, Representative Tom Bliley introduced the Consumer and Investor Access to Information Act of 1999 (HR1858)

Michael D. Palage
Michael@Palage.com

EU Database Directive

- In 1996, the European Union promulgated the European Parliament and Council Directive on the Legal Protection of Databases ("EU Database Directive") to provide new legal protection for databases.

- The EU Database Directive defines a database as any "**collection of independent works, data or other material arranged in a systematic or methodical way and individual accessible by electronic or other means**"

- The protection under the EU Database Directive extends to both electronic and non-electronic databases.

- This EU Database Directive sought to harmonize European copyright law with regard to the protection of databases (Chapter II), while simultaneously granting sui generis protection to databases (Chapter III).

- The EU Database Directive includes a reciprocity provision that does not extend protection to databases created in non-member states that do not offer equivalent protection.

Michael D. Palage
Michael@Palage.com

EU Database Directive – Copyright Protection

▪Chapter II, Article 5 of the EU Database Directive harmonizes European copyright protection on databases by granting the author of a database the exclusive right to carry out or to authorize:

(a) temporary or permanent reproduction by any means and in any form, in whole or in part;
(b) translation, adaptation, arrangement and any other alteration;
(c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;
(d) any communication, display or performance to the public;
(e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b).

Michael D. Palage
Michael@Palage.com

EU Database Directive – Copyright Protection

- Article 6, paragraph 2 sets forth one of the limitation of rights conveyed in Article 5:

Member States **shall have the option** of providing for limitations on the rights set out in Article 5 in the following cases:
(a) in the case of reproduction for private purposes of a non-electronic database;
(b) where there is use for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and **to the extent justified by the non-commercial purpose to be achieved**;
(c) where there is use for the purposes of public security of for the purposes of an administrative or judicial procedure;
(d) where other exceptions to copyright which are traditionally authorized under national law are involved, without prejudice to points (a), (b) and (c).

- France, Greece and Italy have not incorporated the fair use provision set forth in Article 6, paragraph 2(b).

- The scientific and academic community have argued that this fair use provision should be mandatory, not optional.

Michael D. Palage
Michael@Palage.com

EU Database Directive – Sui Generis Protection

▪Chapter III, Article7 of the EU Database Directive grants sui generis rights to "the maker of a database which shows that there has been qualitative and/or quantitatively a **substantial investment** in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database."

▪ Article 9 places the following limitation on sui generis rights:

Member States **may** stipulate that **lawful users** of a database which is made available to the public in whatever manner may, without authorization of its maker, extract or re-utilize a substantial part of its content:
(a) In the case of extraction for private purposes of the contents of a non-electronic database;
(b) In the case of extraction for the purpose of illustration for teaching or scientific research, as long as the source is indicated and **to the extent justified by the non-commercial purpose to be achieved;**
(c) In the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure.

Michael D. Palage
Michael@Palage.com

EU Database Directive – Sui Generis Protection

- "**lawful user**" versus "**user**"

- The term of protection under Chapter III is for fifteen (15) years, however, Article 10, paragraph 3 provides that "**any substantial change**" to the contents of the content in the database "**would result in the database being considered to be a substantial new investment**."

- The law firm of Nauta Dutilh has been retained by the European Union to conduct an independent evaluation of EU Database Directive by the end of 2002. The EU Commission is scheduled to issue a draft report by early 2003, with a final report being submitted to the European Parliament sometime in 2003.

Michael D. Palage
Michael@Palage.com

EU Database Protection – BHRB v. William Hill

- The British Horse Racing Board (BHRB) invested over four (4) million pounds annually maintaining a database of horse racing statistics which it licensed to third parties.

- William Hill Organization Limited 2001 obtained statistics from a licensee of BHRB and then published them on an Internet web site without authorization.

- BHRB sued alleging violation of database rights.

- In finding that William Hill violated the database rights of BHRB, the court held that (1) “extract” merely meant a transfer from one medium to another and (2) the importance of the information to the alleged infringer is a determining factor in the “substantial part” analysis.

- The case has been referred to the European Court of Justice (ECJ) for an interpretation of the database directive.

Michael D. Palage
Michael@Palage.com

EU Database Protection – Deep Linking

- In Danish Newspapers Publishers' Association (DNPA) v. Newsbooster.com, plaintiff filed suit against defendant for providing subscribers a search interface to query plaintiff's web site and return article titles and corresponding deep links.

- DNPA obtained a preliminary injunction, for an unofficial translation see **http://www.newsbooster.com/?pg=judge&lan=eng**

- In Algemeen Dagblad et al. v. Eureka Internetdiensten, plaintiffs, a collection of newspaper publications, filed suit against defendant for operating a service that provided a daily index of the titles of news reports and articles on the plaintiffs' web sites. This index was available on a web page or via e-mail.

- The court denied plaintiffs' claim holding that the indexes were now provided protection under the database act because the newspapers did not invest substantially in creating these indexes. For an unofficial translation of the court's opinion se **http://www.ivir.nl/rechtspraak/kranten.com-english.html**

Michael D. Palage
Michael@Palage.com

Privacy Issues – Overview

- Privacy is an important yet illusive concept in law.

- The right to privacy is recognized in several broad based international agreements:

  - Article 19 of the Universal Declaration of Human Rights states that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

  - Article 12 of the Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

  - See also the International Convention on Civil and Political Rights and the Office for Economic Co-Operation and Development Guidelines Governing the Protection of Privacy and Transboarder Flows of Personal Data.

Michael D. Palage
Michael@Palage.com

US Privacy Issues – Overview

- As Justice Hugo Black wrote "'Privacy' is a broad, abstract and ambiguous concept." *Griswold v. Connecticut*.

- The term "privacy" does not appear in the U.S. Constitution or the Bill of Rights.

- However, Courts derived privacy rights from the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments to the Constitution.

- There is no comprehensive national law providing individuals with data privacy rights, however, there are a number of federal and state laws that do offer some protection.

- The Privacy Act of 1974 and Computer Matching and Privacy Act were two of the more significant laws regarding to the use of personal information by the federal government. However, these laws did not extent to the collection and use of personal information by other private and public sector entities.

- These protections afforded under these laws have recently been amended in connection with the 2001 USA Patriot Act and the 2002 Homeland Security Act.

Michael D. Palage
Michael@Palage.com

US Privacy Issues – ECPA

- The Electronic Communications Privacy Act (ECPA) traces it origins to the anti-wiretapping act enacted after the Watergate scandal of the late 1960's. Originally this statute prohibited government interception of telephone conversations without a judicial warrant.

- In 1986, Congress passed the ECPA which vastly expanded the original anti-wiretapping laws in the following manner:

  - now covers all forms of digital communication, including text and visual images, not just voice communications on a telephone;
  - prohibits the unauthorized eavesdropping by all persons and businesses, not just the government; and
  - not only prohibits the interception of messages in transmission, but also unauthorized access to stored messages on a computer system.

- Under the ECPA, a prevailing plaintiff has a right to have the public posting removed, recover monetary damages, as well as recover attorney fees.

Michael D. Palage
Michael@Palage.com

US Privacy Issues – Miscellaneous other Statutes

- Although there currently exists no comprehensive national law to protect, Congress has passed a

  - The Fair Credit Report Act (1970)
  - Family Education Rights and Privacy Act (1974)
  - Rights to Financial Privacy Act (1978)
  - Privacy Protection Act of 1980
  - Cable Communication Policy Act of 1984
  - Video Privacy Protection Act of 1988
  - Telephone Consumer Protection Act of 1991
  - Driver's Privacy Protection Act of 1994
  - Communications Assistance for Law Enforcement Act of 1994
  - Telecommunication Act of 1996
  - Health Insurance Portability and Accountability Act of 1996
  - Children's Online Privacy Protection Act (COPPA) of 1998
  - Financial Modernization Act (Graham-Leach-Bliley Act) (2000)

- The ConsumerPrivacy Guide web site provides an informative summary of each statute, for additional information please visit http://www.consumerprivacyguide.org/law/

Michael D. Palage
Michael@Palage.com

EU Privacy Issues – Overview

- In stark contrast to US data protection, the EU has enacted omnibus legislation that regulates both public and private sectors.

  - The Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data;
  - Directive 95/46/EC of the European Parliament and of the Council of 24 October on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data; and
  - Directive 2002/58/EC of the European Parliament and of the Council of July 12 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

- EU data protection laws provide individuals with a comprehensive series of rights including, but not limited to:

  - to receive certain information whenever data is collected;
  - to access personal data, and if necessary to correct inaccurate data; and
  - to object to certain types of data processing.

Michael D. Palage
Michael@Palage.com

EU Directive 95/46/EC - Scope

- Article 3, Paragraph 1 states in relevant part that: "[t]his Directive shall apply to the **processing** of **personal data** wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."

  - **processing** – shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

  - **personal data** – shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or in directly, in particular by reference to an identification number or to one or more factors specified to his physical, physiological, mental, economic, cultural or social identity.

  - **controller** – shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Michael D. Palage
Michael@Palage.com

EU Directive 95/46/EC - Data Accuracy & Collection

- Article 6, Paragraph 1 requires that personal data shall be:
  - ➢ **processed fairly** and **lawfully**;
  - ➢ **collected for specified, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
  - ➢ adequate, relevant and **not excessively in relation to the purposes for which they are collected** and/or for which they are further processed;
  - ➢ accurate and, where necessary, kept up to date; **every reasonable step must be taken to ensure that data which are inaccurate or incomplete**, having regard to the purposes for which they were collected or for which they are further processed, **are erased or rectified**;
  - ➢ **kept in a form** which permits identification of data subjects for **no longer that is necessary** for the purposes for which the data were collected or for which they are further processed.

Michael D. Palage
Michael@Palage.com

EU Directive 95/46/EC - Data Processing

- Article 7, states that personal data shall only be processed under the following conditions:

  - the data subject has **given** his **consent unambiguously**; or

  - processing is **necessary for the performance of a contract to which the data subject is party** or in order to take steps at the request of the data subject entering into a contract; or

  - processing is **necessary** for **compliance with a legal obligation to which the controller is subject**; or;

  - processing is **necessary** in order to **protect the vital interests of the data subject**; or

  - processing is **necessary** for the performance of a task carried out in the **public interest** or in the **exercise of official authority** vested in the controller or in a third party to whom the data are disclosed; or

  - processing is **necessary** for the purposes of the **legitimate interests** pursed by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)

Michael D. Palage
Michael@Palage.com

EU Directive 95/46/EC - Data Subject Rights

- Article 12, provides data subjects the **right to obtain** from the controller:
  - 1. without constraint at reasonable intervals and **without excessive delay or expense**:
    - confirmation as to whether or not data relating to him are processed and information at the least as to the purpose of the processing, the categories of the data concerned, and the recipients or categories of the recipients to whom the data are disclosed;
    - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;
    - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1).
  - 2. as **appropriate the rectification, erasure or blocking of data**, the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
  - 3. notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with paragraph 2, unless this proves **impossible or involves a disproportionate effort;**

Michael D. Palage
Michael@Palage.com

EU Directive 02/58/EC - Overview

- During the summer of 2002, the EC adopted a directive on privacy and electronic communications, which Member States are required to implement into nation law before October 31, 2003.

- The topics covered under this new privacy directive include:

  - Security (Article 4);
  - Confidentiality of communications (Article 5);
  - Traffic data (Article 6);
  - Itemized billing (Article 7);
  - Location data (Article 9);
  - Directories of,subscribers (Article 12); and
  - Unsolicited communications (Article 13)

Michael D. Palage
Michael@Palage.com

Safe Harbor

- EU directives on data privacy prohibit the transfer of personal data to non-European Union nations that do not meet European "adequacy" standard for privacy protection.

- The U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework for US companies to avoid interruptions in their business dealings with EU Member States.

- Information about the program, and a list of companies participating in this program can be found online at http://www.export.gov/safeharbor.

- This is a voluntary program, and those participating must comply with the safe harbor requirements and public declare that they do.

- Disney Worldwide Services, Inc is a participant in this program and the data privacy policies are available online.

Michael D. Palage
Michael@Palage.com

Conclusion

- Until all of the participants acknowledge the fundamental differences in database and data privacy protection in the US and EU, there is little likelihood that a framework can be established to resolve the complexities of access and accuracy of Whois data.

Michael D. Palage
Michael@Palage.com