PHILLIPS NIZER LLP

International e-Discovery Management

U.S. regulation vs. local privacy laws

Thomas G. Jackson

February 27, 2009

Court Plaza North • 25 Main Street • Hackensack NJ 07601
201.487.3700 Phone • 201.646.1764 Fax

600 Old Country Road • Garden City NY 11530
516.229.9400 Phone • 516.228.9612 Fax

666 Fifth Avenue • New York NY 10103
212.977.9700 Phone • 212.262.5152 Fax
www.phillipsnizer.com
Resourceful Representation®

Overview of Cross Border Discovery Issues:

The Conflict Between U.S. e-Discovery Rules and the EU Data Protection Directive – Part I

Managing e-discovery presents greater challenges to U.S.-based companies with foreign subsidiaries and U.S. companies with corporate parents overseas

Pre-trial Discovery:

- The U.S. has broad, wide-ranging pre-trial discovery
- EU member states and other countries have little or none

Privacy laws:

- In the U.S., an ad hoc, context-specific approach is taken in protecting privacy. In other countries, such as the member states of the European Union, privacy is recognized as a fundamental right and protected far more broadly
- In Europe, the EU Data Protection Directive (Directive 95/46/EC) provides a comprehensive regulatory framework for protecting personal data

Processing of personal data under the EU Data Protection Directive

Under Directive 95/46/EC:

- Generally, personal data may not be processed in the absence of a specific justification for its processing
- "Personal data" is defined as any information relating to an identified or identifiable natural person ("data subject")
- "Processing" is defined as any collection, use, storage or transfer of personal data
- "Data controllers" are the legal entities responsible for the processing of personal data under their control

Exemptions and justifications:

- For an exemption or justification to the non-disclosure rules to apply, it must be "'actually necessary for the achievement of the objective in question" and not "merely incidental to its achievement"
- Unless a justification exists for each and every processing event, personal data may not be processed

Transfers outside the EU:

- Transfers of personal data to a country outside the EU can only take place where the country ensures an "adequate level of protection" for the data
- The U.S. is not a country that is considered as having an adequate level of protection
- Any collection, use, storage or transfer of personal data without justification is a violation of the EU data protection laws

National legislation:
Additional restrictions are imposed by national data protection legislation implementing the principles of Directive 95/46/EC

Examples:

Germany:	Federal Data Protection Act (BDSG)
Italy:	Personal Data Protection Code (Codice in materia di protezione dei data personali) of 30 June 2003
France:	Law No. 2004-801 of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data (Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel)
United Kingdom:	Data Protection Act 1998

German Data Protection Legislation

German Data Protection Legislation

Sources:

- Federal Data Protection Act (Bundesdatenschutzgesetz-BDSG)
- Sector specific laws such as:
  Telemedia Act (Telemediengesetz-TMG)
  Telecommunication Act (Telekommunikationsgesetz-TKG)

Compliance is overseen by the Data Protection Commissioners in each Bundesland (German state); they have the power to investigate and impose sanctions if necessary

Data processing may include:

- Litigation holds
- Collection and review of data for purposes of discovery
- Transfer of data to the U.S.
- Transfer of data to an opposing party and to the court

⇨ German data protection law requires a justification for the transfer of data stored in Germany to the U.S. and any further use of the data in the course of U.S. discovery

⇨ Companies may only store data for a specific purpose and only to the extent required for that purpose. Neither discovery generally nor minimizing the risk of spoliation is considered a legitimate purpose under German law

Justifications for Data Processing Operations

Generally, under German law, personal data may be processed only if:

1. The legitimate interests of the data controller or third parties outweigh the interests of the data subject

   Issues:

   - If only the U.S.-based parent company is involved in litigation, then the data controller in Europe is not a party to the litigation
   - The more sensitive the data, the more likely that the balancing of interests as between the data controller or the third party and the data subject will be resolved in favor of the data subject

Justifications for Data Processing Operations

2. Processing is necessary for compliance with a legal obligation of a data controller

   Issues:

   - Non-EU legal obligations may not justify processing of personal data in an EU member state for purposes of litigation
   - Although Germany is a signatory to the Hague Evidence Convention, it has opted out of its pre-trial discovery procedures

3. Data subject gives unambiguous consent

   Issues:

   - Must be freely and unambiguously given, which is problematic in the case of consent given by employees where, as a result of an inherently coercive employer-employee relationship, employees may be considered unable to freely consent
   - Data subject must be informed about the exact purpose of the data transfer
   - Data subject may revoke his/her consent at any time

Transfer of Personal Data to the U.S.

Transfer of data to the U.S. is generally prohibited because U.S. standards of data protection are considered to be inadequate, in the absence of such additional safeguards as:

- Safe Harbor Principles: allowing data transfers from the EU to U.S. companies that agree to meet certain privacy protection standards

⇨ Financial institutions are excluded from the Safe Harbor Agreement

- EU Commission-approved Standard Contractual Clauses

⇨ Must be part of a signed agreement between the data controller and the non-EU recipient; does not apply to transfers to or access by third parties

- Binding corporate rules defining data processing activities and policies applied among entities within a corporate group

⇨ Only allows transfers of data between international offices within the corporate group

Transfer of Personal Data to the U.S.

- Consent by the data subject, who must be informed of the identities of all recipients

⇨ Primary concern: None of these safeguards permit disclosure to the court, the jury or the opposing parties unless each of the data subject has given his/her informed consent

⇨ Conclusion: The transfer and use of data in the U.S. for the purpose of discovery is likely to be found to be illegal under German data protection laws

PORTOLANO COLELLA CAVALLO
STUDIO LEGALE

PHILLIPS NIZER LLP
Resourceful Representation®

Italian Data Protection Legislation

Italian Data Protection Legislation

Legislative Decree of 30 June, 2003, no. 196 (the Italian Data Protection Code - IDPC)

- applies to the processing of personal data by individuals or entities established in Italy and by data controllers established outside the EU if equipment located in Italy is used for the processing of such data
- requires a non-EU data controller to appoint a national representative for data protection purposes in Italy
- gives data subjects the right to access, update and correct their data

Generally, data controllers must:

- provide data subjects with oral or written notice which must contain details concerning the controller and the purposes and means for processing the data (section 13 of the IDPC)
- with certain exceptions, obtain the consent of the data subjects in order to lawfully process their data or to transfer their data outside the EU (sections 23, 24 and 43 of the IDPC)
- obtain the written consent of the data subjects and the Data Protection Authority's authorization in order to lawfully process sensitive personal data (Section 26 of the IDPC)
- Adopt the security measures specified in the IDPC

e-Discovery and Privacy Issues

- Under the IDPC, in the case of processing for the purpose of exercising a right before a court or in connection with a criminal proceeding, the following exemptions apply:
- The controller is exempted from providing a data subject with notice
- The controller is exempted from obtaining the data subject's consent in order to process their data for those purposes
- The controller is exempted from obtaining the data subject's consent in order to transfer their data outside the EU

e-Discovery and Privacy Issues

These exemptions apply only if there is an actual purpose of exercising a right before a court and not for purposes of collecting or using the data in anticipation of future litigation

- Because a U.S. company is subject to preservation obligations for purposes of discovery not only in the event of actual litigation but also in anticipation of reasonably foreseeable litigation, there may be a conflict between U.S. e-discovery obligations and Italian data protection laws

- Under Italian law, personal data can be retained only for specific purposes. Using such data in anticipation of future litigation, where this purpose is in addition to the one for which data have been originally collected and retained, may be unlawful

These exemptions apply only to the controller of the data. If the controller is an Italian company and the data are necessary in the context of a U.S. litigation in which a U.S. parent company is involved, then any transfer from Italy to the U.S. must be carried out in compliance with the IDPC

e-Discovery and Privacy Issues

In the absence of the data subject's consent – which may not be considered "sufficient" in the case of a transfer to a non-EU member country such as the U.S. with an inadequate level of protection – data may be transferred only if one of the following requirements is met (section 44 of the IDPC):

- the U.S. company adheres to Safe Harbor Principles
- the transfer is made in compliance with the Standard Contractual Clauses approved by the EU Commission
- the transfer is carried out within companies that have adopted binding corporate rules

Overview of Cross Border Discovery Issues:

The Conflict Between U.S. e-Discovery Rules and the EU Data Protection Directive – Part II

Blocking statutes:
Enacted largely to defeat U.S. discovery obligations, more than a dozen countries have enacted "blocking" statutes forbidding their nationals from cooperating with American discovery requests or orders

- The French blocking statute prohibits French residents and nationals and the employees, agents or officers of French companies from disclosing "to foreign public authorities documents or information of an economic, commercial, industrial, financial or technical nature" when such disclosure is liable to affect French sovereignty, security or "fundamental economic interests"

- In 2007, the highest court in France upheld the criminal conviction and 10,000 euro fine of a French lawyer, hired by a U.S. law firm representing the California Insurance Commissioner in an investigation of a French insurance company, who made a telephone call in an attempt to obtain information informally from a former employee of the French company for use in a litigation to be brought in the U.S. (Cour de Cassation Chambre Criminelle [Cass. Crim.], Paris, Dec. 12, 2007, Juris-Data no. 2007-332254)

Hague Evidence Convention:
Discovery under the Hague Evidence Convention is more cumbersome and often more limited than under the Federal Rules of Civil Procedure

Requests for documents:
Made through letters of requests issued by U.S. courts to foreign authorities

- National law may be far more restrictive than U.S. law, e.g., French law requires that requests identify documents with reasonable specificity, bear a direct connection to the matter in dispute and be limited in time and scope

Depositions:
Foreign nationals and residents may be deposed before a U.S. diplomatic or consular officer or person commissioned by a U.S. court upon prior authorization of foreign authority

- This procedure may result in delay or denial of request, e.g., under French law all documents relevant to the case must be provided to the Ministry of Justice at least 45 days in advance of the deposition to obtain prior authorization

(Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, 847 U.N.T.S. 231, reprinted at 28 U.S.C. § 1781)

Cases:

Société Nationale Industrielle Aerospatiale v. United States District Court, 482 U.S. 522 (1987): Hague Evidence Convention does not deprive a court of its jurisdiction under the Federal Rules of Civil Procedure to order a foreign national to produce evidence physically located within a signatory nation

Factors considered in determining whether documents and information protected by foreign law are discoverable

- the importance to the litigation of the documents or other information requested
- the degree of specificity of the request
- whether the information originated in the United States
- the availability of alternate means to secure the information
- the extent to which noncompliance with the request would undermine important American interests or compliance with the request would undermine important interests of the state where the information is located

(*Aerospatiale*, 482 U.S. at 544 n.28)

Additional factors

- hardship to the party from which discovery is requested
- party's good faith in resisting discovery

(*First American Corp. v. Price Waterhouse LLP,* 154 F.3d 16, 22 (2d Cir. 1998))

Cases requiring use of Hague Evidence Convention procedures:

In re Perrier Bottled Water Litigation, 138 F.R.D. 348 (D. Conn. 1991): requiring use of Hague Evidence Convention procedures to obtain discovery from defendant, citing French blocking statute

Hudson v. Hermann Pfauter GmbH & Co., 117 F.R.D. 33 (N.D.N.Y. 1987): requiring use of Hague Evidence Convention procedures to obtain discovery from a German defendant

Cases compelling production of evidence despite possibility of violating a foreign blocking statute:

Enron Corp. v. J.P. Morgan Securities, Inc., No. 01-16034 (Bankr. S.D.N.Y., July 18, 2007): Possibility of violating the French blocking statute does not relieve a party of its e-discovery obligations

Columbia Pictures Industries v. Bunnell, 2007 U.S. Dist LEXIS 46364 (C.D. Cal., May 29, 2007): requiring RAM and server log data stored on computers located in the Netherlands to be produced; "foreign blocking statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce ... evidence even though the act of production may violate that statute"

Strauss v. Credit Lyonnais SA, 242 F.R.D. 199 (E.D.N.Y. 2007): Production required where there is no significant risk of prosecution

In re Vivendi Universal, S.A. Securities Litigation, 2006 U.S. Dist LEXIS 85211 (S.D.N.Y., Nov. 16, 2006): Production required where there is only a "speculative possibility of prosecution"

Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., 2005 U.S. Dist. LEXIS 20049 (N.D. Ill., Sept. 12, 2005): Federal Rules of Civil Procedure apply despite the claim under Italian law that Italy has a legitimate national interest in preventing pre-trial discovery

Possible solutions:

The Eli Lilly initiative: Exploring in collaboration with EU Data Protection Commissioners such steps as

- Designating as EU Confidential data involved in cross-border discovery from EU member states
- Developing EU-specific provisions for federal and state protective orders and for case management orders restricting further transfer of EU Confidential data and safeguards against unauthorized disclosure, use or retention of such data, beyond its specified purpose or time, allowing data owner access to inspect the data, and requiring destruction or return of personal data when the specified purpose was fulfilled
- Developing EU-approved protocols and processes for pre-filtering of personal data in the host country to ensure that only relevant personal data is transferred for cross-border discovery purposes

(The Sedona Conference Working Group on International Electronic Information Management, Discovery and Disclosure, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery at 28 (Public Comment Version, Aug. 2008)

The Sedona Conference protocol:

"[B]alancing ... the needs, costs and burdens of the discovery with the interests of each jurisdiction in protecting the privacy rights and welfare of its citizens," taking into account such factors as :

- the data privacy obligations in the jurisdiction where the information is located and the obligation to preserve and produce relevant information in the jurisdiction where the litigation is pending
- the extent of the custody and control of the responding party over the requested information
- the nature and complexity of the proceedings
- the amount in controversy
- the importance of discovery in resolving critical issues
- the burden and cost of collecting, processing, reviewing and producing relevant information taking into account accessibility, volume, location, and ability to identify information subject to foreign privilege and work product protection

(The Sedona Conference Framework for Analysis of Cross-Border Discovery Conflicts at 29-30)

Article 29 Data Protection Working Party Document 1/2009 on Pre-trial Discovery for Cross Border Civil Litigation, adopted 11 February 2009

Key guidelines:

- Use should be made of "anonymized data" (personal data from which information identifying the data subject is removed) or "pseudonymized data" (personal data from which the data subject's name is removed and replaced with a unique code or pseudonym)
- "Filtering" should be carried out in the country where the personal data is found before data that is deemed relevant is transferred to another jurisdiction
- A "trusted third party" in the EU member state with sufficient knowledge of the litigation but no role in the litigation itself may be appropriate to determine the relevance of the data
- Data protection officers of the EU data controllers should involve themselves at the earliest stage to explain EU data protection issues to the U.S. courts and apply for protective orders where necessary to comply with EU data protection obligations
- With limited exceptions, notice should be given at the earliest stage to data subjects of the identity of any recipients, the purposes of the processing, the categories of data concerned and the existence of their rights
- Data security obligations should apply to law firms dealing with the litigation, litigation support services and others involved with the collection or review of the information
- Binding corporate rules or adherence to Safe Harbor Principles should be considered where large amounts of data are to be transferred
- Hague Evidence Convention procedures should be considered first as a method for transferring information for litigation purposes and additional time should be "built in" by the U.S. courts to accommodate delays

Practical considerations in managing cross-border discovery:

- Document retention policies: Consider storage practices, retention periods and policies and legal consequences of outsourcing to foreign vendors
- Review policies and procedures, for example, for archiving and retrieving e-mail messages and for using, logging, archiving and retrieving instant messages
- Litigation holds: Address U.S. requirements and foreign laws that may be in conflict
- Responding to discovery requests: Consult with foreign counsel knowledgeable in areas of data protection and develop consistent strategies for litigation preparedness on a country-by-country basis

Thomas G. Jackson, *Partner*

Phillips Nizer LLP
666 Fifth Avenue
New York, NY 10103-0084
212.841.0765 Direct Tel
212. 262.5152 Facsimile
tjackson@phillipsnizer.com
www.phillipsnizer.com

Thomas Jackson is a partner in the New York office of the Phillips Nizer law firm and heads the Firm's Technology Group. His practice includes the representation of software developers and distributors, new media companies, Internet service and content providers and users of Internet-based products and services. He has been involved in a wide variety of matters in the technology field, including software licensing and software development agreements, information technology services agreements, software distribution agreements and technology transfers.

Tom is also a member of the Firm's Litigation Department and has litigated and tried major cases for over 30 years. He concentrates his litigation practice in the fields of technology law, antitrust, unfair competition and trade association law, privacy and information law, class action defense and commercial litigation. He has handled litigations, alternative dispute resolution proceedings and settlements in the areas of mergers and acquisitions, employer liability, taxation, securities law and copyright and trademark law, as well as cases involving computer software acquisitions, licensing and royalties disputes, Internet-related trademark and domain name disputes and other areas of the information technology field.

He advises attorneys in the Firm's Litigation and Corporate Departments and in other practice areas on electronic discovery issues and has written and spoken on the subjects of e-Discovery and data and privacy protection. He recently co-authored the article "E is Key – Electronic Discovery," which appeared in *The New York Law Journal*.

M Law Group

PHILLIPS NIZER LLP
Resourceful Representation®

Dr. Stephan Appt, LL.M., *Rechtsanwalt*

Stephan Appt focuses his practice on advising and representing German and international clients on all intellectual property matters, in particular with regard to licensing, technology transfers, information technology and data protection and distribution law.

Stephan received his law degree and doctorate in law from the University of Freiburg and an LL.M degree from the University of Edinburgh, Scotland. As part of his studies, he attended the University of Lausanne, Switzerland. Before joining MLawGroup, he worked for a US law firm in Munich and a Belgian law firm in Brussels. He was admitted to the bar in 2004.

MLawGroup

Maximilianstraße 31,
80539 München, Deutschland

+49 89 24 213 102 Tel
+49 89 24 213 213 Fax

stephan.appt@mlawgroup.de

www.mlawgroup.de

PORTOLANO COLELLA CAVALLO
STUDIO LEGALE

PHILLIPS NIZER LLP
Resourceful Representation®

Laura Liguori, *Partner*

Laura Liguori is a partner in Portolano Colella Cavallo Studio Legale where she concentrates her practice in the fields of media law and commercial contracts.

Laura advises Internet companies on the legal aspects of commercial transactions and B2B and B2C online transactions, as well as data protection and consumer protection laws.

She is the author of articles on e-commerce, data protection law and Internet law and is a contributor to the websites of two of the major online legal publishers, International Law Office (www.internationallawoffice.com) and Mondaq (www.mondaq.com). She is a member of the American Bar Association, International Bar Association and ITechlaw Association.

Laura graduated *cum laude* with a law degree from Luiss Libera Università Internazionale degli Studi Sociali Guido Carli in Rome, Italy in 1996.

Portolano Colella Cavallo Studio Legale

Via Santa Maria in Via, 12
00187 Roma, Italia

+39 06 69 76 541 Tel
+39 06 69 76 544 Fax

lliguori@portolano.it

www.portolano.it

PORTOLANO COLELLA CAVALLO
STUDIO LEGALE

PHILLIPS NIZER LLP
Resourceful Representation®

Micael Montinari, *Partner*

Micael Montinari assists both domestic and foreign companies in the fields of commercial litigation and intellectual property law. He is involved in both litigations and arbitration proceedings in connection with commercial and corporate matters, including IP and media related matters.

He also focuses on insurance matters connected to the media and IP as well as corporate disputes.

The litigation group led by Micael is ranked by “Legal500” and “Which lawyer?”

Micael speaks at conferences on litigation and commercial issues hosted by various organizations.

He teaches business and civil procedure law with the Rome Chamber of Commerce and Luiss Business School Guido Carli professional education programs.

He is member of the American Bar Association, International Bar Association, International Trademark Association and International Chamber of Commerce.

Portolano Colella Cavallo Studio Legale

Via Santa Maria in Via, 12
00187 Roma, Italia

+39 06 69 76 541 Tel
+39 06 69 76 544 Fax

mmontinari@portolano.it

www.portolano.it

PHILLIPS NIZER LLP

International e-Discovery Management

U.S. regulation vs. local privacy laws

Thomas G. Jackson

February 27, 2009

Court Plaza North • 25 Main Street • Hackensack NJ 07601
201.487.3700 Phone • 201.646.1764 Fax

600 Old Country Road • Garden City NY 11530
516.229.9400 Phone • 516.228.9612 Fax

666 Fifth Avenue • New York NY 10103
212.977.9700 Phone • 212.262.5152 Fax
www.phillipsnizer.com