BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

EU Data Protection

U.S. Discovery Rules

U.S. litigation discovery requirements are not necessarily antithetical to compliance with EU data protection law, the authors posit. They propose that three existing mechanisms—privacy notices, protective orders, and model contracts—could be adapted to form the basis for an international consensus on how to resolve tensions between the demands of U.S. discovery and EU data protection compliance.

A Path to Resolving European Data Protection Concerns With U.S. Discovery

BY STANLEY W. CROSLEY, ALAN CHARLES RAUL, EDWARD R. MCNICHOLAS AND JULIE M. DWYER

The amount of commentary regarding a conflict between European Union privacy regulations and U.S. discovery obligations is increasing every day. As the European Union's Article 29 Data Protection Working Party recently stated, ''[t]he issue of pre-trial discovery and the vulnerability of the corporate community of Europe to US court orders is a rapidly growing source of concern.''[1] Recent U.S. emphasis on the legal duty to retain all electronically stored information relevant to litigation has only exacerbated the perception.

EU operations of multinational corporations with U.S. ties are indeed often subject to U.S. discovery obligations that involve the personal data of their employees. These companies are bound to observe the laws of all jurisdictions in which they operate but, more and more, they find themselves embroiled in a conflict of legal obligations, as other commentators have noted.[2] When faced with impending U.S. discovery demands, these companies are presently compelled to devise individualized, expensive, ad hoc mechanisms—of perhaps questionable validity—in an attempt to provide required discovery while complying with the EU Data Protection

[1] Article 29 Data Protection Working Party, Press Release (Apr. 20, 2007), *available at* http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_20_04_07_en.pdf.

[2] Cate and Eisenhauer, ''Between a Rock and a Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements,'' *Privacy & Security Law Report (BNA)*, Vol. 6, No. 6, 2/05/2007 (6 PVLR 229, 2/5/07).

 ISSN 1538-3423

Directive[3] and related EU Member State legislation.[4] Without a doubt, a transparent, standardized framework that addressed the tensions between U.S. discovery and EU privacy requirements would significantly decrease the cost of compliance and increase the actual protections afforded to EU data subjects.

This article is intended to dispel unnecessary controversy and to stimulate the formation of an international consensus on a set of protocols that reconciles overlapping EU privacy and U.S. litigation obligations. The authors seek to facilitate the ability of multinationals to deploy standardized, fully adequate litigation protocols that comply with both U.S. and EU requirements. This prospective solution involves the development and EU approval of model ''legal process protocols'' for the collection, processing and transfer of EU personal data in connection with pre-trial discovery for U.S.-based litigation. Such protocols might include:

- an addendum to corporate privacy policies to provide multinationals' employees with clear, complete and robust advance notice of the prospect and implications of multinationals' involvement in U.S.-based civil litigation;
- a standardized Data Protection Protective Order, to be issued by the relevant U.S. court, that relies on numerous data protection and minimization procedures both to narrow the scope of disclosure and to ensure robust protections for any data that is collected or exchanged; and
- if necessary, an EU Model Contract for U.S. litigation that affords EU-equivalent rights in and protections for EU personal information throughout the litigation process.

Such protocols would in effect serve as a code of conduct for litigation and would provide assurances of adequate data protection for personal information while also allowing full compliance with U.S. discovery obligations.

This article first briefly reviews the general obligations under relevant U.S. and EU laws, and then suggests, contrary to most commentary, that U.S. discovery processes are not necessarily antithetical to EU data protection values. Based on this insight, the article proposes that thoughtful adaptation of three existing mechanisms—privacy notices, protective orders, and model contracts—can form the basis for an international consensus that resolves the rising global tensions regarding this issue.

Global Compliance with U.S. Discovery Is a Legal and Business Imperative

As is widely known to American litigating parties, U.S. civil litigation discovery rules compel the pre-trial collection, processing and disclosure of personal information to courts and opposing parties. In the course of pending or reasonably anticipated litigation, companies have an affirmative obligation to collect, preserve and/or produce all relevant records within the company's possession, custody or control.[5] Significantly, recent amendments to U.S. civil procedure rules have codified requirements that the scope of discovery includes electronically stored information. Failure to comply with a valid discovery request or court order can result in severe sanctions, including contempt proceedings, monetary fines, prosecution for obstruction of justice, prejudicial jury instructions, and dismissal of claims.

This power of U.S. courts to compel companies to collect, preserve and produce records can extend to foreign subsidiaries or affiliates, or records otherwise stored outside the United States, depending on the U.S. court's jurisdiction over the entity at issue. An EU entity may avoid U.S. discovery requirements if the EU entity successfully establishes that it is not subject to U.S. personal jurisdiction and that its U.S. affiliate lacks custody or control over documents held in the EU. Nonetheless, integrated, globalized information technologies frequently make EU-derived documents readily accessible in the United States, and the legal duty of multinational companies to collect, process and transfer information thus frequently extends to the entire corporation. To the extent that this information encompasses personal data subject to EU data protection laws, multinational companies must find a means of achieving full compliance under both sets of legal rules in a manner that respects the authority and values of both.

Respecting EU Concerns with U.S. Discovery Is Also Essential

Under the EU Data Protection Directive, data processing is considered to be legitimate if it is necessary to enable compliance with a legal obligation of the data controller or to serve a data controller's legitimate interests (except where such interests are overridden by the interest in protecting the fundamental rights and freedoms of the data subject).[6] Nevertheless, EU data protection authorities have questioned the legitimacy of processing conducted for the purpose of fulfilling *foreign* legal obligations. Authorities have also raised concerns in this context with respect to proportionality and notice to data subjects.

The text of the Data Protection Directive itself expressly acknowledges that companies have a valid interest in using information for international litigation, in that the Directive provides for a derogation from the restrictions on transfers of personal data to third countries which do not ensure an adequate level of protection under Article 25 where the transfer is ''necessary for the establishment, exercise or defense of legal claims.''[7] While EU authorities have not applied this exemption in the context of litigation outside the EU, companies with an EU presence have an indisputable interest in being able to both maintain and defend against U.S. suits. In fact, participation in discovery is necessary to protect both the offensive and defensive interests of any company that is subject to U.S. litigation, regardless of the company's location.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281, 23.11.1995, p. 31–50* [hereinafter EU Data Protection Directive].

[4] The Data Protection Directive imposes obligations on Member States, who must implement the principles of the Directive in their national laws. National laws in turn impose obligations on the individuals and entities to whom they apply.

[5] *See* Fed. R. Civ. P. 26, 34.

[6] EU Data Protection Directive, art. 7(c) and (f).

[7] *Id.* art. 26(1)(d).

  PVLR ISSN 1538-3423

EU Data Protection Authorities have, without question, highlighted important concerns with respect to the legitimacy of data processing conducted in response to demands for information based on foreign law. For instance, the Article 29 Working Party has reviewed the actions of the Belgian-based Society for Worldwide Interbank Financial Telecommunication (SWIFT) in providing the personal data of EU citizens to the U.S. Department of Treasury in response to administrative subpoenas issued during an anti-terrorism investigation. The Working Party has also assessed the data protection implications of the internal whistle-blowing systems required under the U.S. federal Sarbanes-Oxley Act (SOX).[8] In its opinions in both the SWIFT and SOX matters, the Working Party noted that '' 'an obligation imposed by a foreign legal statute or regulation . . . may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate.' ''[9] In particular, the EU authorities expressed concerns with unilateral, non-transparent approaches to data processing and transfers.[10] And, indeed, SWIFT has apparently despaired of achieving compliance with both sets of laws and is reported to be spending €150 million [$212.7 million] to move segments of its network to Switzerland in order to address such EU concerns.

The Working Party has also raised concerns about proportionality and notice where data is sought pursuant to foreign legal authority. In the context of SWIFT, for example, the Working Party observed that the scope of the information sought by the U.S. Department of Treasury was extremely broad and lacked reasonable limitations.[11] Significantly, a U.S. federal court considering privacy challenges to the SWIFT program has also expressed similar concerns and declined to dismiss a privacy complaint against SWIFT.[12] To address EU concerns, in both its SWIFT and SOX opinions, the Working Party emphasized the need to enhance transparency by providing affected data subjects with notice in the form of ''clear and complete information about the scheme,''[13] and by notifying data protection authorities of data processing.[14]

U.S. Discovery Processes Are Not Necessarily Antithetical to European Values

While the experiences of the SWIFT and SOX matters have made clear that European and U.S. legal systems achieve their respective goals in different ways, the debate has vastly overstated these differences, particularly with respect to routine pre-trial civil discovery. The U.S. discovery rules create no irreconcilable public policy conflict with EU data protection principles. To the contrary, United States and EU information gathering processes share common truth-seeking features and legitimate goals of ensuring the just and rapid resolution of disputes, and are in fact used cooperatively to resolve cross-border legal disputes in many circumstances. As the following examples make clear, it surely overstates the issue—and inhibits mutual understanding—to suggest that there is an intractable conflict between EU and U.S. approaches to personal privacy during litigation.

U.S. Discovery Procedures Share Common Features with European Methods for Information Gathering. U.S. discovery procedures cannot be reflexively equated with excessive and unreasonable encroachments on privacy. Although some view U.S. discovery as tantamount to mere ''fishing expeditions,'' in fact, U.S. discovery is conducted under judicial supervision with every incentive for a party to seek redress from the court if discovery requests are excessive. Although discovery under the U.S. rules extends to all information reasonably likely to lead to admissible evidence, U.S. discovery also routinely protects privacy interests—such as those with respect to financial or medical matters—through the use of protective orders and other judicial interventions.

Moreover, U.S. and EU information gathering systems indeed share similarities. The European Anti-Fraud Office (OLAF), for example, has extensive regulatory authority to preserve and collect information in the course of conducting internal administrative investigations into fraud or corruption on the part of public officials and other government staff.[15] In assessing OLAF's powers, the European Data Protection Supervisor himself has expressly found that these discovery-like document preservation and production measures do not run afoul of EU protections for personal data, *provided the investigating agency takes steps to ensure*

---

[8] Pub. L. No. 107-204 (2002).

[9] Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 01935/06/EN, WP 128, at 17-18, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf [hereinafter SWIFT Opinion] (quoting Article 29 Data Protection Working Party, Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, 00195/06/EN, WP 117, at 8, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf [hereinafter SOX Opinion]).

[10] For example, the SWIFT Opinion noted disapproval of the ''non-transparent'' manner in which SWIFT provided information to U.S. regulators, *id.* at 11, expressing ''regret[ ] that no prior consultation, formal or informal, was effected . . . with the data protection authorities,'' *id.* at 20. Similarly, with respect to U.S.-EU negotiations over transfers of airline PNR data, the Working Party bristled at not having been ''consulted or asked for advice on the data protection elements of the agreement.'' Article 29 Data Protection Working Party, Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, 01646/07/EN, WP 138, at 3, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_en.pdf.

[11] SWIFT Opinion, *supra* note 9, at 8.

[12] *See Walker v. S.W.I.F.T. SCRL*, 491 F. Supp. 2d 781 (N.D. Ill. 2007) (largely denying SWIFT's motion to dismiss, but granting petition to transfer case to Eastern District of Virginia).

[13] SWIFT Opinion, *supra* note9, at 19; SOX Opinion, *supra* note 9, at 13.

[14] SWIFT Opinion, *supra* note 9, at 19-20; SOX Opinion, *supra* note 9, at 17.

[15] *See* Regulation (EC) No. 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), *OJ L 136, 31.5.1999, p. 1–7*, art. 4(2). While this regulation is in the process of being amended, no changes have been proposed to Article 4(2).

respect for this data throughout the investigation process.[16]

As with U.S. discovery rules, certain EU regulations also impose data preservation and production requirements on the private sector to facilitate legal processes. In the context of private civil litigation, the laws of certain EU Member States, most notably the United Kingdom, afford litigating parties fairly broad rights of pretrial disclosure. Other EU countries may not afford private parties such rights, but instead look to judicial investigators to gather relevant information. Indeed, the European Commission itself has extensive powers to compel private companies to ''provide all necessary information'' to the Commission, including ''business records contained in any medium.''[17] Similarly, France's Conseil d'Etat, the nation's highest administrative court, has recently determined to be consistent with personal privacy rights the new data retention and disclosure rules requiring Internet and telecommunications service providers to make certain user communication data available to law enforcement for counterterrorism purposes.[18]

Cross-Border Information Gathering Systems Have Been Used to Mutual Advantage. Cross-border information gathering mechanisms also have proved complementary in resolving international disputes. Traditional principles of international comity favor aiding foreign dispute resolution processes and assisting foreign tribunals in gathering evidence. Indeed, a long-standing provision of U.S. federal law expressly permits U.S. courts to order discovery specifically for use in a foreign proceeding, and many EU litigants have availed themselves of this privilege.[19] In *Intel Corp. v. Advanced Micro Devices Inc.*,[20] for example, the U.S. Supreme Court upheld the right of a company pursuing an antitrust complaint before the European Commission's Directorate-General for Competition to seek discovery in the United States. Indeed, that case recognized that private parties could seek information relevant to both administrative and judicial proceedings in the EU, even prior to the actual initiation of such proceedings.

European courts and authorities, likewise, have made similar accommodations in aid of U.S. proceedings, even where the data protection scheme in question differs from that of the EU. In one recent case, an English court granted a U.S. request for disclosure of documents containing the personal medical information of U.K. citizens (which had been produced in an earlier English case).[21] After imposing certain measures to protect the data, the court noted that any potential risk of infringement on the individuals' data protection rights and human rights was justified in light of the foreign litigant's important right to a fair trial. Similarly, in a proposed Council Framework Decision on the protection of personal data in the context of police and judicial cooperation on criminal matters, the Portuguese Presidency noted a ''growing consensus'' for allowing transfers of personal data to non-EU states even where the ''adequacy'' requirement has not been met.[22] Under the Council's proposed framework, such transfers would be permitted, provided that the recipient country used appropriate safeguards for the data.[23]

The EU Should View Data Processing Pursuant to Legal Process Protocols as Legitimate

The solution to what many have feared is some deep cultural divide may be to recognize that both the U.S. discovery process and the EU privacy regulatory process intentionally contain significant flexibility which can be used to accord greater respect to each system. During discovery, litigants have the freedom to negotiate protective orders and contracts that are tailored to the particular facts and circumstances of the litigation. In addition, U.S. courts are bound by principles of international comity to limit discovery obligations in cross-border cases so as to ''demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state.''[24] EU data protection laws also allow for such comity. As the Article 29 Data Protection Working Party has recently observed, ''flexibility is embedded in the text [of the Directive] to provide an appropriate legal response to the circumstances at stake.''[25] To date, reliance upon this flexibility has allowed litigants in particularly complex cases to achieve ad hoc solutions, often at great cost, to the underlying tensions between the two approaches. But the key to a long-term solution to this issue is to achieve an understanding that the processing of EU personal data in compliance with U.S. discovery rules should be treated as legitimate when conducted within a framework of stringent legal process data protection controls.

A standardized set of ''legal process protocols'' could thus provide a cost-effective, consistent solution that effectuates important EU data protection values of legitimacy, proportionality, and notice while respecting the truth-seeking and dispute resolution functions of the U.S. litigation system. Such protocols should include a regime of extensive advance notice and disclosure to employees (and any other data subjects), a model, com-

[16] *See* Opinion on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on OLAF internal investigations, Case 2005-418 (2006), *available at* http://ec.europa.eu/dgs/olaf/data/doc/interninvestig.pdf.

[17] *See* Council Reg. (EC) No. 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, *OJ L 1, 4.1.2003, p. 1–25*, (Regulation 1/2003) arts. 18, 20.

[18] *Association des Fournisseurs d'Accès et de Services Internet (AFA) v. Ministere de l'Interieur* (Conseil d'Etat Aug. 7, 2007).

[19] *See* 28 U.S.C. § 1782.

[20] 542 U.S. 241 (2004).

[21] *See Paul Sayers & Others v. Smithkline Beecham PLC & Others*, [2007] EWCH 1346 QB.

[22] Council of the European Union, Brussels, 4 September 2007, 12154/07 LIMITE, Note from Presidency to Coreper/Council, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters – Agreement on certain questions, at 3, *available at* http://www.statewatch.org/news/2007/sep/eu-dp-12154-07.pdf (referring to an ''adequacy'' requirement patterned after that in the EU Data Protection Directive, 95/46/EC, art. 25).

[23] *See id.* at 5.

[24] *Société Nationale Industrielle Aé rospatiale v. U.S. Dist. Ct.*, 482 US 522, 546 (1987).

[25] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, at 4, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

  PVLR ISSN 1538-3423

prehensive EU Data Protection Protective Order, and, if necessary, an EU Model Contract for data transfers incident to discovery. We address each element in turn.

■ Advance Notice and Complete Disclosure Through a Privacy Policy Addendum

The first element of these protocols should directly address EU concerns about notice to data subjects. ''Clear and complete''[26] disclosures to EU employees of multinationals—the individuals whose personal information is most likely to be processed during discovery—would avoid the defects that have troubled EU authorities. As the SWIFT Working Party Opinion noted, ''the controller is obliged to inform data subjects about the existence, purpose and functioning of its data processing, the recipients of the personal data and the right of access, rectification and erasure by the data subject.''[27] And nothing in the U.S. civil litigation framework would necessarily preclude such notice.

Protection of employees' rights during discovery requires ensuring that individuals are fully informed of the implications of involvement in U.S. litigation, and employees should receive appropriate disclosures as early in the employment process as possible. Multinationals should be charged with explaining, in privacy policies and by other means, that the company is routinely involved in U.S. litigation, and thus is required to collect and process personal data for legitimate business purposes that include compliance with U.S. litigation obligations.

These disclosures should describe data processing methods, identify prospective data recipients, and inform data subjects of their rights under applicable U.S. law and EU data protection laws, as implemented by Member States, as well as provide guidance on the means for enforcing those rights. Such disclosures may most easily take the form of a special section of, or addendum to, the company's privacy policy, but the disclosures should focus on providing data subjects with clear, complete and robust advance notice of the data subjects' rights under applicable EU data protection laws and U.S. laws.

■ Data Protection Protective Orders

The second element of any comprehensive set of protections would be a special protective order, issued by the U.S. court, specifically to address EU data protection concerns about the processing of personal data during litigation. Reflecting EU values of legitimacy, proportionality and notice, such an order would employ several protection and minimization procedures both to narrow the scope of the data subject to disclosure and to ensure robust protections for any data that is collected or exchanged.

During U.S. discovery, the parties routinely negotiate the terms of protective orders that account for the sensitivity of the information at issue and that limit the scope of and access to the information collected. Typically, protections for trade secrets, commercially sensitive information, financial information, health information, and other information that may raise privacy concerns are included in protective orders. The U.S. discovery process thus inherently affords more than adequate flexibility to introduce procedures that can be used to protect EU personal data.

To effectuate the proportionality principle, which requires that data be ''adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed,''[28] the protective order could restrict the scope of the disclosures ordinarily allowed under U.S. discovery rules, possibly by allowing processing of EU documents containing personal data only when they are demonstrated to be directly relevant to the issues presented, as opposed to being merely ''reasonably calculated to lead to the discovery of admissible evidence.''[29] Similarly, the order could constrain the amount of personal data subject to third-country processing by imposing minimization requirements that direct an initial review of materials in Europe to cull non-responsive and unnecessary documents prior to any international transfer.[30] In order to maintain separate processing, such an order could also isolate EU data from other data produced through discovery, allowing EU data to benefit from specific, heightened protections, such as extra restrictions on service providers and others regarding access to, storage, transfer, use and disposal of such data.

To ensure transparency both to data subjects and EU data protection authorities, the order could also appoint a special discovery master to monitor compliance with EU data protection requirements. Such a master also may provide special review of discovery requests that call for the production of sensitive personal data and ensure that the relevant data protection authorities receive notice of the litigation, including information on the general categories of documents to be produced.

Most significantly, however, such an order could expressly recognize data subjects' rights in their personal information and require parties to demonstrate that data subjects have received adequate notice of the litigation, discovery requests, and data access rights. The requirements for such notice could mirror the requirements of the EU Data Protection Directive, and inform the data subjects as to ''the identity of the [data] controller,'' ''the purposes of the processing,'' ''the categories of data concerned,'' ''the recipients or categories of recipients of the data,'' and ''the existence of the right of access to and the right to rectify the data.''[31]

■ An EU Model Contract for Litigation

As a final element, such legal process protocols may also need to address data protection concerns related to the data transfers that may be required to litigate a U.S. case. The protocols could do so by requiring the litigating parties to execute an EU Model Contract.[32] Indeed,

[26] SWIFT Opinion, *supra* note 9, at 19; SOX Opinion, *supra* note 9, at 13. Other individuals about whom the organization may possess personal data could be able to review the litigation Privacy Policy Addendum from the organization's public website, although such individuals would rarely be subject to the jurisdiction of the U.S. court.

[27] SWIFT Opinion, *supra* note 9, at 19.

[28] EU Data Protection Directive, art. 6(1)(c).

[29] Fed. R. Civ. P. 26.

[30] *See* SWIFT Opinion, *supra* note 9, at 20-24 (criticizing SWIFT for failing to use measures to limit third-country processing); SOX Opinion, *supra* note 9, at 16 (stating that, where possible, EU companies should address whistleblowing reports locally to avoid automatic transfers of information).

[31] EU Data Protection Directive, arts. 10, 11.

[32] *See* Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, 2004/915/EC, *OJ L 385,*

in the SWIFT matter, the Working Party criticized SWIFT's failure to ensure protections for data transferred to the United States and noted that '' 'appropriate contractual clauses' '' can provide adequate safeguards for transfers.[33] Of course, such a contract may not be necessary for parties that already have in place a specific mechanism for legitimating the data transfer, such as Safe Harbor membership or Binding Corporate Rules. A model contract, however, would facilitate full compliance with EU data transfer requirements and is the only compliance mechanism well-suited to the transfer of a discrete data set during a particular case.

Such a model contract would afford EU data subjects EU-equivalent rights in and protections for data exchanged between litigants and transferred to the U.S., and would also create an enforcement mechanism for data retention and secure information handling measures. Data subjects would be able to enforce their rights under the model contract as third-party beneficiaries against the parties to the model contract, in accordance with its terms, as well as in the appropriate EU and U.S. courts.

Toward a Transparent and Systematic Consensus

A scheme of legal process protocols could well form the basis to initiate a dialogue with EU authorities, and the concerted involvement of data protection authorities in arriving at a practical solution for U.S. discovery and EU data protection compliance may be the best path forward. Ongoing cross-border cooperation efforts on data protection matters provide a strong foundation for such further engagement. To facilitate information sharing in the context of public security, for example, government representatives have recently formed the U.S.-EU High Level Contact Group on data privacy and law enforcement cooperation. Key multilateral organizations such as the Organization for Economic Cooperation and Development (OECD) have also promoted cross-border cooperation on privacy enforcement and have envisioned a significant role for the private sector in achieving this objective.[34] Significantly, the EU's Article 29 Data Protection Working Party has also recently expressed a desire to collaborate with U.S. authorities such as the Federal Trade Commission to produce global improvements to data protection.[35] Such efforts will indeed perform a significant service if they are able to publish standardized conditions under which U.S. discovery-related processing may be viewed as legitimate without the need for individualized EU approval.

29.12.2004, p. 74-75, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf.

[33] SWIFT Opinion, *supra* note 9, at 22 (quoting 95/46/EC, art. 26).

[34] *See* OECD, Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy (2007), *available at* http://www.oecd.org/dataoecd/43/28/38770483.pdf; OECD, Report on the Cross-Border Enforcement of Privacy Laws (2006), *available at* http://www.oecd.org/dataoecd/17/43/37558845.pdf.

[35] *See* Article 29 Data Protection Working Party, Report 1/2007 on the first joint enforcement action: evaluation and future steps, 01269/07/EN, WP 137, at 8-9, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp137_en.pdf.

   ISSN 1538-3423