

Reconciling European Data Privacy Concerns with US Discovery Rules: Conflict and Comity

By

Alan Charles Raul, Edward McNicholas and Elisa Jillson


Reprinted from **Global Competition Litigation Review**
Issue 3, 2009

Sweet & Maxwell
100 Avenue Road
Swiss Cottage
London
NW3 3PF
(Law Publishers)

SWEET & MAXWELL

Reconciling European Data Privacy Concerns with US Discovery Rules: Conflict and Comity

*Alan Charles Raul, Edward McNicholas and Elisa Jillson**

 Comity; Discovery; EC law; Electronic disclosure; Litigation; Personal data; Privacy; United States

The need for multinational corporations to prepare for, manage and vigorously prosecute transnational litigation is often in tension with cultural norms. Few areas have provoked as much attention as the recent conflict between the intensely adversarial truth-seeking function of US litigation and European efforts to protect spheres of personal privacy.

The conflict has come to a head in part because recent amendments to US discovery rules have emphasised that electronic discovery will be part of essentially every significant commercial dispute involving the United States. At the same time, the ubiquity of email, the proliferation of new forms of social media and the advent of cloud computing have dramatically altered the concept of a “business record”, particularly in a world in which personal and business documents are intermingled on mobile devices that travel seamlessly from the boardroom to the breakfast table.¹

Employees, however, have continued to demand recognition of some areas of personal space that can

stand as a bulwark against the complete conflation of the personal and the professional. Such cries for the recognition of spheres of personal privacy and autonomy finds one of their most assertive expressions in the European Union’s Data Protection Directive (“EU Directive”),² which guarantees an individual’s right to control the use of his or her personal information.

Multinationals are thus faced with the daunting task of navigating between the Scylla of trampling on employees’ privacy in their personal data, and the Charybdis of inadvertently failing to ensure a vigorous corporate litigation defence. In this context, companies without skilled guidance could easily find themselves in a situation in which they are denied important evidence as a result of their mishandling of EU privacy issues.

Without clear guidance on reconciling US and EU law, some multinationals and commentators have considered this a Hobson’s choice³ that compels ad hoc compromises of dubious legal validity, often based on the nations’ respective enforcement budgets and attitudes of the respective regulators. No responsible company, however, wants legal “compliance” that consists of erring on the side of violating the law of whichever country is less likely to discover and penalise non-compliance. Indeed, this compelled calculation creates incentives for a race among nations to increase the vigour of enforcement and the severity of penalties. Without resolution, companies could be in an even worse situation, in which countries with ever more unrelenting norms have incentive to impose ever-harsher penalties for non-compliance.

As a theoretical matter, attempting to reconcile US and EU conceptions of privacy would be as futile—and fruitless—as reconciling French and US attitudes towards rodeos. Whereas EU law identifies privacy as a fundamental human right, US law conceives of

2 Personal data, broadly defined as “any information relating to an identified or identifiable natural person”, may only be “processed” (i.e. collected, used or disclosed) for one of several legitimate grounds for processing specified in art.7 of the Directive. Council Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

3 See Carla L. Reyes, “The U.S. Discovery-EU Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy” (2009) 19 *Duke Journal of Comparative & International Law* 357 (recounting such conflict in the context of US civil discovery); similarly Fred H. Cate and Margaret P. Eisenhauer, “Between a Rock and a Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements” (2007) 7 *BNA Privacy & Security Law Report* 229 (February 5).

* Alan Raul and Edward McNicholas are partners, and Elisa Jillson is an associate, in the Privacy, Data Security, and Information Law practice in the Washington, DC offices of the international law firm of Sidley Austin LLP.

1 See *Mintel Int’l Group Ltd v Neergheen*, 2009 WL 249227 at [2], No.08-CV-3939 (N.D. Ill. February 3, 2009) (rejecting plaintiff’s efforts to secure a court order to search the computers of defendant’s employer after plaintiff discovered that defendant sent strategic business information to his personal email account).

privacy as one interest among others. Europeans recoil at anonymous denunciation, while Americans reward similar “denunciation” as laudable whistle-blowing. Americans resist a mandated national identity card; Europeans accept requests for such papers. American privacy law stems from the Constitutional restriction on governmental searches of private information, while Europeans have long warned of the dangers of corporate access to personal data. In light of these differences, numerous commentators have asserted the problem’s intractability.⁴

Such a dire conclusion is not inevitable. While the theoretical differences do not make for ready resolution, homogeneity is not a prerequisite for common understandings and policy. Indeed, the diversity of the potential legal approaches to these issues should be recognised as a valuable resource. As several international bodies have demonstrated, common ground, based on the longstanding principles of international comity, can support pragmatic solutions to address the conflict between US discovery and the EU Directive. The clearest expression of this new comity stems from a working document on “pre-trial discovery for cross border civil litigation” adopted on February 11, 2009 by the EU’s art.29 Data Protection Working Party to offer initial guidance regarding compliance with EU privacy law during US civil discovery.⁵ Particularly in an environment in which the United States is perceived to be a more eager participant in resurgent internationalism, these guidelines may point the way to a true détente by embracing the longstanding principle of international comity—mutual respect for the laws of other countries—and by creating pragmatic legal solutions that implement those principles.

Understanding the sister problem: US discovery and EU privacy

Several commentators have documented the conflicts that arise when a multinational corporation operating

in the European Union engages in pre-trial civil discovery in the United States.⁶ According to the Federal Rules of Civil Procedure, companies have an affirmative obligation to collect, preserve and/or produce all relevant records within the company’s possession, custody or control in the course of pending or reasonably anticipated litigation.⁷ Recent amendments to the Federal Rules have made clear what sophisticated litigators have realised for years: electronically stored information is rapidly becoming the most important source of discoverable material. The broad scope of these discovery rules sweeps into their purview documents that frequently contain employees’ personal information. The incentive to collect, review and sometimes produce records containing personal information is strong: failure to comply with the discovery requirements of the Federal Rules could lead to severe sanctions, including fines, prosecution for obstruction of justice, contempt proceedings and dismissal of claims.

Whereas the United States has focused on broad discovery obligations, the European Union has mandated protection of data subjects’ personal information. In 1995, the European Council of Ministers and the European Parliament approved Directive 95/46/EC, which establishes uniform provisions for the processing of personal information in the European Union (the EU Directive).⁸ Member States must implement the principles of the Directive via national legislation, although they are free to impose even more onerous substantive and administrative requirements, such as registration and permitting regimes. According to the EU Directive, processing is legitimate if necessary for compliance with a “legal obligation” or if in line with the data controller’s “legitimate interests”. Because the European Union has not generally regarded US discovery as either a sufficient “legal obligation” or a “legitimate interest” for EU data protection purposes, the EU Directive limits collection, processing and transfer of personal information of EU data subjects to satisfy US litigation requirements.

More focused “blocking” statutes have, of course, existed for years in a variety of contexts. Furthermore,

4 See Cate and Eisenhauer, “Between a Rock and a Hard Place” (2007) 7 *BNA Privacy & Security Law Report* 229 (February 5); see also Ian L. Schaffer, “An International Train Wreck Caused in Part by a Defective Whistle: When the Extraterritorial Application of SOX Conflicts with Foreign Laws” [2006] *Fordham Law Review* 1829, 1865.

5 Art.29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, 00339/09/EN, WP 158 (February 11, 2009), available at http://ec.europa.eu/justice_home/fsj/privacy/docswpdocs/2009/wp158_en.pdf [Accessed June 24, 2009].

6 See Reyes, “The U.S. Discovery” (2009) 19 *Duke Journal of Comparative & International Law* 357; Stanley W. Crosley, Alan Charles Raul, Edward McNicholas and Julie Dwyer, “A Path to Resolving European Data Protection Concerns with U.S. Discovery” (2007) 6 *BNA Privacy & Security Law Report* 41 (October 15); and Cate and Eisenhauer, “Between a Rock and a Hard Place” (2007) 7 *BNA Privacy & Security Law Report* 229 (February 5).

7 See Fed. R. Civ. P. 26, 34.

8 EU Directive [1995] OJ L281/31.

US courts have frequently not given them full respect.⁹ Such statutes, however, were traditionally limited to particular areas of life, such as banking, or smaller particular jurisdictions, and so the effect of these statutes has not proved overly problematic.¹⁰ The EU Directive, in contrast, covers all personal data in one of the world's largest markets.

The conflict between US and EU law that arises during US internal investigations of multinational companies is equally problematic. The EU Directive simply does not expressly contemplate internal investigations. As experienced commentators have observed, the EU Directive was enacted to “operate[] at a more general level” than to “specifically legislate the collection and handling of personal data in the investigative context”.¹¹

Whereas US litigants can look to a federal district court for guidance in resolving the conflict between the breadth of US discovery¹² and the prescriptions in the EU Data Privacy Directive, a corporation conducting an internal investigation operates without a comparable referee, unless the corporation is willing to present its nascent internal investigation to a European Data Protection Authority. Furthermore, the corporation is acting unilaterally in responding to or anticipating requests from public authorities: the lack of bilateral conventions for exchange of information increases pressure on the corporation to locate *all* relevant materials, no matter their location in the European Union or the sensitive personal information they contain. The result is a legal and public relations imbroglio. Non-disclosure in the name of privacy may appear to US public authorities and the press as a

pretext for concealing the smoking gun, while disclosure looks to EU authorities like an irresponsible or smug company's disrespect not only for EU authority, but also for a fundamental human right.¹³

Recognising common goals: identifying the groundwork for embracing principles of international comity

Despite this conflict, the concerns animating the relevant US and EU laws are not incompatible. The first step to laying the groundwork for embracing principles of international comity is to recognise the extent to which the United States and European Union have common interests regarding privacy and the need for corporate oversight.

The EU will countenance limits on privacy to identify or prevent wrongdoing

Even though the US and EU conceptions of privacy diverge, the regimes share common truth-seeking features: both have legitimate goals in seeking to identify and eradicate corporate fraud and other crime.¹⁴ As in the United States, EU public authorities require companies to gather significant information during internal investigations.

In the United States, a company may conduct an internal investigation to comply with a number of regulations, including, for example, the Securities and Exchange Commission's enforcement of the Sarbanes-Oxley Act or the Department of Justice's enforcement of the Foreign Corrupt Practices Act. In the European Union, the European Anti-Fraud Office (OLAF) 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

9 See *Société Internationale Pour Participations Industrielles et Commerciales, SA v Rogers*, 357 U.S. 197, 204–206 (1958); *Madden v Wyeth*, 2006 U.S. Dist. LEXIS 880 (N.D. Tex. January 12, 2006) (ordering documents from French corporate affiliates despite a French blocking statute).

10 See, e.g. Swiss Penal Code art.273 (protecting “business secrets” from production); French Penal Code Law No.80-538 (requiring use of the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, March 18, 1970, 23 U.S.T. 2555, T.I.A.S. No.7444, codified at 28 USC s.1781, to take evidence in France); Panamanian Commercial Code arts 89 and 93 (prohibiting disclosure of certain corporate records or their removal outside of Panama, which functions in addition to practices such as not listing beneficial owners in many contexts).

11 Dan Cooper, “Corporate Investigations and EU Data Privacy Laws: What Every In-House Counsel Should Know” (2008) 8(12) *BNA World Data Protection Report* 21.

12 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. See Fed. R. Civ. P. 26, 34.

13 See Fred H. Cate, “The Conflict Between European Data Protection Laws and U.S. Civil Discovery Rules” (2008) 1 *IAPP Privacy Tracker* 7.

14 See, e.g. *Sweden v Council of the European Union* (C-39/05 P) [2008] 3 C.M.L.R. 17 (allowing public access to lobbying registration information).

15 See Regulation (EC) 1073/1999 of the European Parliament and of the Council of May 25, 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF) [1999] OJ L136, art.4(2). While this regulation is in the process of being amended, no changes have been proposed to art.4(2).

OLAF requires companies to preserve and produce business records, a feature of the EU system very similar to US discovery and to investigations conducted at the behest of US regulatory authorities. The European Data Protection Supervisor himself has expressly found that OLAF's preservation and production requirements are not contrary to the EU Data Privacy Directive's protection of personal data, so long as the investigating agency takes precautions to ensure respect for personal information during the course of the investigation.¹⁶

Nor is OLAF's requirement of collection of business records that may contain personal data unique. The European Commission similarly has extensive powers to compel private companies to produce evidence for the purpose of competition enforcement. The Commission requires companies to "provide all necessary information" to the Commission, including copies of business records contained in any medium.¹⁷ Like its US regulatory counterparts, the Commission has authority to impose penalties for incomplete productions of records.¹⁸

Willingness to curb privacy considerations to ensure the efficacy of truth-seeking mechanisms is not unique to the fraud or competition contexts. Member countries of the European Union have been willing to countenance the considerable collection of personal information so long as the purpose for such collection outweighed the privacy interests at stake. For example, France, a stalwart defender of privacy rights, has authorised data retention and disclosure rules that require internet and telecommunications service providers to make user communication data available to law enforcement. The *Conseil d'Etat*, the nation's highest administrative court, upheld the rules when the data is used for counter-terrorism purposes. The *Conseil d'Etat* was cognizant of the privacy implications of collecting such personal communications, but the Court found that the impact on individuals' privacy rights was not disproportionate in light of the gravity of the

public security interests at stake in counter-terrorism measures.¹⁹

US protection of privacy does not fundamentally conflict with EU protections

Not only do the US and EU systems share legitimate goals in seeking to eliminate corporate fraud and combat terrorism, but they also share many of the same privacy concerns.

In general, the information relevant in US internal investigations parallels the information relevant in US discovery (i.e., all information reasonably likely to lead to the admissible evidence). Equating US internal investigations with unreasonable encroachments on privacy is as question-begging—and as incorrect—as it is to equate US discovery with an excessive invasion of privacy. While the breadth of the US inquiry could, particularly in poorly-managed litigation, be at odds with EU privacy protections, the divergence, in practice, is not nearly so extreme.

While the Federal Rules of Civil Procedure authorise broad discovery, the Federal Rules contain protections for significant areas of privacy, particularly sensitive areas such as financial, medical and home-life matters. US federal courts have repeatedly shown sensitivity to privacy concerns through the use of protective orders, sealed proceedings and other judicial management or intervention. Moreover, US courts increasingly recognise that employees may need to consent to searches of private areas.²⁰ Because US internal investigations are often the precursor to, or a surrogate for, civil litigation, the information sought will parallel that available in civil discovery. Court-imposed protection of personal information not only sets a precedent for discovery, but also for internal investigations.

Secondly, unlike litigation, an internal investigation is self-limiting. Particularly in the context of consumer class actions, opposing litigants are often able to engage in asymmetrical assertions of the importance of electronic discovery because their clients have few—if any—records, while defendant corporations have extensive databases. This asymmetry yields the

16 See Opinion on a notification for prior checking received from the Data Protection Officer of the OLAF on OLAF internal investigations, Case 2005-418 (June 23, 2006), available at <http://ec.europa.eu/dgs/olaf/data/doc/interninvestig.pdf> [Accessed June 24, 2009].

17 See Council Regulation 1/2003 of December 16, 2002 on the implementation of the rules on competition laid down in arts 81 and 82 of the Treaty [2003] OJ L1/1, arts 18–20.

18 See Regulation 1/2003, art.23(1)(b) and (c).

19 *Association des Fournisseurs d'Accès et de Services Internet (AFA) v Ministère de l'Intérieur (Conseil d'Etat)*, August 7, 2007.

20 See, e.g. *Wal-Mart Stores, Inc v Lee*, 74 S.W.3d 634 (Ark. 2002) (vitiating employee consent to home search by employer investigating allegations of theft and allowing action for invasion of privacy).

classic fishing expedition in which litigants with weak cases troll for any possible hook or use corporate reticence to engage in extensive electronic discovery as a means of bolstering a weak case. No such incentive exists in an internal investigation. Investigating counsel usually know the organisation well and are charged with rooting out improper conduct without otherwise disturbing corporate operations.

Lastly, companies conducting internal investigations in the United States have incentives to protect employee privacy. While the company's first priority is to isolate and eradicate fraud, sophisticated entities (as large companies tend to be) will be cognizant of the consequences of their investigation on their workforce: the company will not want to alienate employees by delving unnecessarily into materials containing personal information. Moreover, as installing a privacy officer to oversee corporate compliance with international privacy law becomes the norm, clumsy collection, processing and transfer of business records without consideration for privacy will become increasingly less common. The fewer overreaching investigations, the less the European Union will consider such investigations to be tantamount to wholesale disregard of employee privacy.

Vehicles for implementing common goals: embracing international comity

The groundwork for relying on principles of international comity already exists, not only in the shared goals of truth-seeking and privacy, but also in the language of the EU Directive itself. The EU Directive permits data processing that is necessary to comply with a "legal obligation".²¹ The EU Directive further states that a transfer of data is acceptable where "necessary . . . for the establishment, exercise or defense of legal claims".²² While the term is outwardly broad, its meaning has thus far been narrowly circumscribed, such that foreign law is rarely deemed a "legal obligation", as the Data Protection Authorities have acknowledged.

Currently, conducting an internal investigation pursuant to a US law or at the behest of a US regulatory authority is not reliably considered a legal obligation under the EU Directive. Under principles of international comity, however, an investigation conducted pursuant to a legitimate US law would be a "legal obligation".

²¹ EU Directive, art.7(c).

²² EU Directive, art.26(1)(d).

International comity is a principle of mutual respect, recognised abroad and by the US Supreme Court since the nation's inception. A law:

" . . . ought never to be construed to violate the law of nations if any other possible construction remains, and consequently can never be construed to violate neutral rights, or to affect neutral commerce, further than is warranted by the law of nations as understood in this country."²³

This longstanding principle of respect for the laws of other nations has become increasingly important as legal disputes frequently take on an international flavour. Indeed, US federal courts continue to invoke the principles of international comity when resolving transnational discovery suits. US federal courts hold that they 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

US courts are not alone in recognising the need for flexibility in resolving such disputes. As the art.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 Respect and flexibility are bedrock principles of both legal regimes.

Pragmatic resolution drawing on the EU Directive's flexibility and on principles of international comity is thus not only possible, but also readily achievable. The best evidence of that possibility is not an argument from first principles, but from recent experience. The United States and European Union have already begun the work of relying on principles of international comity to reconcile truth-seeking with privacy concerns—even if neither country has identified the incremental reconciliation as the result of embracing principles of international comity.

²³ *Murray v The Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804).

²⁴ *Société Nationale Industrielle Aérospatiale v U.S. Dist. Ct.*, 482 U.S. 522, 546 (1987).

²⁵ Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN, WP 136, p.4, available at http://ec.europa.eu/justice_home/ffsj/privacy/docswpdocs/2007/wp136_en.pdf [Accessed June 24, 2009].

The High-Level Contact Group

The European Union and United States have begun discussions to address these issues in the context of law enforcement. The EU Commission, the EU Council Presidency, the US Department of Justice, the US Department of Homeland Security and the US Department of State have created the High-Level Contact Group:

“... to start discussions on privacy and personal data protection in the context of the exchange of information for law enforcement purposes as part of a wider reflection between the EU and the U.S. on how best to prevent and fight terrorism and serious transnational crime.”²⁶

The High-Level Contact Group has issued 12 principles for conducting effective criminal investigations without trampling individuals' privacy interests.²⁷ A cornerstone of the principles is proportionality. In this balancing test, privacy is important, but even an important interest can be outweighed by an interest of greater gravity.

The High-Level Contact Group has by no means harmonised US and EU law. Indeed, the Group is still debating five additional principles. Nevertheless, its work demonstrates that upon recognising the importance of a common endeavour—fighting terrorism and serious crime—and upon recognising that this global endeavour will only be successful with mutual co-operation, the nations can reconcile ostensibly diametrically opposed privacy regimes.

Anti-Bribery Convention

Nor is the High-Level Contact Group the first effort at international co-operation regarding investigation and privacy. As part of the Organisation for Economic Co-operation and Development (OECD) Anti-Bribery Convention, each country party to the convention must adopt national legislation to criminalise the bribery of foreign public officials. The OECD Working Group on Bribery conducts monitoring and surveillance. Among the 37 countries that have ratified the convention are privacy stalwarts like France and the United States,

26 “Final Report by the EU-U.S. High Level Contact Group on Information Sharing and Privacy and Personal Data Protections”, 9831/08 (May 28, 2008), available at http://ec.europa.eu/justice-home/fsj/privacy/news/docs/report_02_07_08_en.pdf [Accessed June 24, 2009].

27 Lisa N. Venbrux, “EU and U.S. Officials Agree on 12 Principles for Sharing Data in Law Enforcement Context” (2008) 7 *Privacy & Security Law Report* 27.

which amended the Foreign Corrupt Practices Act in accordance with the Convention.²⁸

Article 29 Data Protection Working Party

The most salient example of relying on principles of international comity is the pragmatic solution recently developed to address the conflict between US discovery and the EU Directive. In a working document adopted on February 11, 2009, on “pre-trial discovery for cross border civil litigation” (the Guidelines), the Article 29 Data Protection Working Party (“Working Party”) offers advice to companies regarding compliance with EU privacy law while conducting civil discovery for US litigation.²⁹ The Working Party acknowledges the “tension between the disclosure obligations under US litigation or regulatory rules and the application of the data protection requirements of the EU”.³⁰ In drafting the Guidelines, the Working Party recognised that:

“... the parties involved in litigation have a legitimate interest in accessing information that is necessary to make or defend a claim, but this must be balanced with the rights of the individual whose personal data is being sought.”³¹

The Working Party recommended compromise. For example, the Guidelines highlight the fact that the EU Directive does not prohibit data transfers to the United States for litigation. Reasonable litigation holds, or the pre-emptive storage of personal data for anticipated

28 Another example of international co-operation to provide a uniform solution to a global problem is the Convention on Cybercrime. Forty-three nations have signed this international treaty, which seeks to address cybercrime and other internet crimes by harmonising national laws, improving investigative techniques and increasing co-operation among nations. In the context of this Convention, the expansionist notions of the freedom and protection of speech in the United States serve as the stumbling block for the investigative concerns of the European Union. Article 9(2)(c) of the Convention of Cybercrime flatly bans “realistic images representing a minor engaged in sexually explicit conduct”. While internationally differing conceptions of protected speech do prevent absolute uniformity in compliance with the Convention, the theoretical difference has not prevented international compliance with the vast majority of the Convention's provisions. While compliance for the United States may be a theoretically fraught position, the theoretical wrangle has not, as a practical matter, prevented the United States largely from complying with its obligations to the international community.

29 Guidelines, fn.5.

30 Guidelines, p.2.

31 Guidelines, p.2.

litigation, are permissible under the EU Directive in certain circumstances.³²

Based on the Guidelines, multinational companies can take certain steps to reduce the likelihood of conflict between US and EU law. For example, multinationals can revise their privacy policies to provide data subjects with notice of the possibility of litigation in the United States, which would require collection, retention, processing and transfer of business records containing personal data.³³ In addition, companies can reduce the burden on privacy rights by advising data subjects on how to involve the Data Protection Authority.³⁴

The Working Party embraced principles of international comity in allowing that:

“... [the] interests of justice would be served by not unnecessarily limiting the ability of an organisation to act to promote or defend a legal right.”³⁵

While the Guidelines are non-binding, they demonstrate that pragmatic solutions, based on principles from both legal systems, are possible to resolve a seemingly intractable conflict.

Conclusion

In each of these examples, resolution was not easy or theoretically tidy. Nevertheless, once interested nations focused less on theoretical purity and more on pragmatic possibility, the nations achieved reconciliation.

The European Union and United States should agree that as long as a company's litigation and associated internal investigation are conducted in accordance with a legitimate truth-seeking function, the company is acting to comply with a “legal obligation” within the meaning of the EU Directive. Such pragmatic resolution is consonant with the EU Directive's “flexibility” and with the fundamental principle of EU privacy law: proportionality. In this way, principles of international comity will vindicate both the truth-seeking goals of litigation and the privacy-protection goals of the international community.

32 Guidelines, pp.7–9.

33 See Crosley et al, “A Path to Resolving European Data Protection Concerns with U.S. Discovery” (2007) 6 *BNA Privacy & Security Law Report* 41 (October 15), p.5.

34 Crosley et al, “A Path to Resolving European Data Protection Concerns with U.S. Discovery” (2007) 6 *BNA Privacy & Security Law Report* 41 (October 15), p.5.

35 Guidelines, pp.7–13; see also Alan Charles Raul et al., “Assessing the EU Working Party's Guidance on Harmonizing U.S. Discovery and EU Data Protection Requirements”, 8 *Privacy and Security Law Report (BNA)* 10, pp.2–3 (March 9, 2009) (arguing that the Guidelines' recognition that US discovery is a “legitimate interest” within the meaning of the EU Directive signifies “a significant advance in the international comity dialogue”).