U.S. Preservation Requirements and EU Data Protection: Headed for Collision

Tania Abbas

Follow this and additional works at: https://repository.uchastings.edu/hastings_international_comparative_law_review

Part of the Comparative and Foreign Law Commons, and the International Law Commons

Recommended Citation
Available at: https://repository.uchastings.edu/hastings_international_comparative_law_review/vol36/iss1/4

This Note is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings International and Comparative Law Review by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.
U.S. Preservation Requirements and EU Data Protection: Headed For Collision?

By TANIA ABBAS*

Table of Contents

I. Introduction .......................................................... 258
II. The Origins of the Conflict ........................................ 258
   A. The Duty to Preserve and the Over-Preservation Phenomenon ...................... 261
   B. The Alleged Lack of Clear Guidance to Litigants Concerning Preservation Duties ........................................ 262
   C. The Over-Preservation Practices of Multinational Corporations ..................... 263
III. European Privacy Laws and Their Enforcement ............... 266
   A. The European Privacy Framework ........................................ 266
   B. The Potentially Broad Applicability of European Union Data Protection Laws ..................................... 270
   C. The Trend Towards Increased Enforcement of European Union Data Protection Laws ..................................... 274
   D. The Proposed Data Privacy Regulation ....................................... 276
IV. The American Attitude: Treatment of Non-U.S. Data Privacy Laws in U.S. Courts ........................................ 277
   A. The Case Law Governing the Applicability of Foreign Privacy Laws in U.S. Courts ........................................ 279
   B. European Regulators Call for Dialogue ....................................... 284
V. Conclusion .................................................................. 286

* J.D. Candidate, 2013, University of California, Hastings College of the Law; B.A., University of California, Berkeley. I would like to thank Professor Richard Marcus for his ongoing guidance on the topic discussed in this Note.
I. Introduction

When companies operate across multiple jurisdictions, they may find themselves subject to conflicting laws that are difficult, if not impossible, to reconcile. The intersection of European privacy laws and broad discovery requirements for U.S. litigation creates now well-known conflicting legal duties that require companies to expunge information in Europe that they are required to preserve in the United States. However, researchers, scholars and practitioners have given limited attention to the ways in which information preserved for discovery could violate European data protection laws because the more visible problem is violations that occur when information is actually produced in Europe and transferred to the United States for use in a lawsuit. However, the time is ripe for European regulators to grasp on to these potential preservation violations for two reasons. First, large corporations are explicit about how much data they are over-preserving and have brought the issue into the limelight in an attempt to effect changes to the Federal Rules of Civil Procedure. Secondly, because EU regulators are increasingly enforcing data privacy laws more vigorously and are poised to begin demanding compliance to a much greater degree. It is possible that the vast quantities of data on hold for potential litigation in the United States inherently violate the European data protection laws to such an extent that emboldened EU regulatory authorities could sanction multinationals in Europe for privacy transgressions in the United States.

II. The Origins of the Conflict

Views concerning the concept of the “right to privacy” diverge remarkably between citizens of the United States and the European Union - a difference that is reflected in our respective legal cultures. Observers have identified the fundamental contrast as between “privacy as an aspect of dignity and privacy as an aspect of liberty.” The foundational European privacy rights are the former and protect “one’s image, name, and reputation,” ensuring “a right to respect and personal dignity.” American privacy rights, on the


2. Whitman, supra note 1, at 1161.
other hand, are liberty-oriented and protect "the right to freedom from intrusions by the state, especially in one's own home."³

Some commentators claim that the contemporary European view emerged largely as a reaction to fascism and transgressions against personal integrity by authoritarian states during World War II.⁴ Others propose the European concept of the right to privacy is an extension to the general public of a right to respect that existed in the monarchical tradition on the continent for centuries, but that was previously reserved only for those of high social status.⁵ Whatever its origins, the privilege to keep personal information private is enshrined in the Charter of Fundamental Rights of the European Union as "the right to the protection of personal data" and is "secured by statute in each Member State."⁶

For Americans, the concept of privacy is more elusive. While it is not a right explicitly protected by the founding documents, the Supreme Court has declared it is in the "penumbra" of other guarantees enumerated in the Bill of Rights.⁷ Unlike the comprehensive framework governing the protection of personal data in the EU, American privacy laws have been called a "patchwork quilt" of industry specific regulations.⁸ To onlookers from the continent, Americans seem to routinely compromise privacy protections in favor of other fundamental rights such as freedom of expression. By European standards, one distinct area where the right to privacy is egregiously compromised is in the discovery phase of civil litigation in U.S. courts.

3. Id.


5. Whitman, supra note 1, at 1166.


In the United States over the last century, the right to "discover" relevant information from an adverse party in civil litigation has become increasingly broad. In 1947, the U.S. Supreme Court declared, "[m]utual knowledge of all the relevant facts gathered by both parties is essential to proper litigation."9 In the 1960s and 1970s, the discovery right expanded to its peak, in part as a tool to aid private litigants defending enforcement of legislation designed to benefit the public, such as civil rights and antitrust laws.10 As Professor Geoffrey Hazard points out in an article published in 1998 – the same year the most comprehensive data protection regime in the world was to be implemented throughout the European Union – broad discovery "has become, at least for our era, a procedural institution perhaps of virtually constitutional foundation .... [W]hen litigation eventuates, no secrets shall be hid."11

According to the preeminent American research institute on the subject, the Sedona Conference, the law concerning cross-border discovery and data privacy is "an area often thought of as so complex and confounding that it has been largely ignored."12 But, addressing the underlying conflict of laws is only becoming more important because more companies are operating across borders, and more individuals conduct their activities on a global scale, whether in person or over the Internet. Because of new laws in Europe designed to address this, even data held in the United States may be subject to European data privacy rules.

To advocates of strict, dignity-based privacy rights, liberal disclosure at the American level is particularly ominous in the digital age because more data is generated, circulated, preserved,

---

and ultimately, produced. Under the European framework, this data is subject to strict privacy protocols that may be breached when litigants attempt to produce information for American discovery. Companies that can expect to be sued in the United States have begun preserving mass quantities of data to comply with what they believe U.S. law requires from an entity that may become involved in litigation. This practice of data hoarding creates the potential for conflict with European data privacy laws because multinational corporations keep information that pertains to people in the European Union or that otherwise falls within the scope of EU regulations.

A. The Duty to Preserve and the Over-Preservation Phenomenon

The duty to preserve relevant information for ongoing or future litigation is a well-established aspect of American discovery procedures rooted in the common law. The duty can arise, even before a party comes in contact with the court, whenever litigation is reasonably anticipated, threatened, or pending. The preservation requirement is intended to prevent spoliation of discoverable evidence that could be germane to a lawsuit and the obligation attaches to potential plaintiffs and defendants alike. Although the general obligation to identify, locate, and maintain relevant information has not changed substantively with the proliferation of electronically stored information (ESI), the medium presents unique challenges.

When the Federal Rules of Civil Procedure (FRCP) were amended in 2006 to better accommodate the discovery of electronically stored information, the changes did not include affirmative provisions concerning preservation. Instead, the FRCP regulate the preservation of ESI through sanctions. Allowing a system to continue its normal operation, with knowledge that information relevant to litigation will be lost, is an omission sanctionable under the Federal Rules. Rule 37(e), however,
provides a "safe harbor" for parties who have lost evidence through "the routine, good-faith operation of an electronic information system." As the committee notes point out, this means that when the duty to preserve is triggered, a litigant may be required to institute a "litigation hold" which involves intervening in the routine operation of an electronic system to ensure that relevant information is not destroyed.

B. The Alleged Lack of Clear Guidance to Litigants Concerning Preservation Duties

Large, multinational corporations, often parties to discovery-intensive litigation, claim that ambiguity in the law forces them to over-preserve as the only risk-free way to navigate divergent standards among the circuit courts concerning what triggers the duty to preserve, the scope of the preservation requirement, and the level of culpability required to warrant sanctions for the spoliation of ESI.

Microsoft, for example, alleges that plaintiffs abuse the inherent uncertainty in the fact-specific, "ever-shifting case law" because "[t]he threat of a spoliation claim - or even the threat of extremely broad discovery or discovery-on-discovery in an attempt to manufacture a spoliation claim - tends to drive up the value of an otherwise weak case." Thus, because even negligent conduct can lead to sanctions in some circuits, Microsoft maintains, "over-preservation is the only rational response to a system that imposes such high costs for such a low level of culpability." The issue has led to a raging debate over whether the FRCP should be further amended to level the playing field. Large companies assert that "conflicting and ambiguous case law on the duty to preserve" requiring companies to retain massive amounts of information to avoid spoliation sanctions in U.S. courts has created a crisis in civil litigation that should be resolved through amendments to the

17. FED. R. CIV. P. 37(e).
18. FED. R. CIV. P., supra note 16.
20. Id. at 6.
21. Id. at 3.
Federal Rules. Whether or not changes to the rules are actually warranted has become the subject of conferences and scholarly debate, elicited prolific comment from practitioners, and attracted the attention of Congress. Whatever the merit of those pleas, the discussion has thrown light on the extent to which companies are amassing and storing nonessential data.

C. The Over-Preservation Practices of Multinational Corporations

In an open letter to the Chair of the Advisory Committee on Civil Rules in preparation for the Mini-Conference on Preservation and Sanctions in September 2011, Microsoft described in detail its “over-inclusive” preservation practices. The company uses a “custodian-based approach” to litigation and discovery, which means they preserve all relevant documents associated with a specific person. Ultimately, however, only a very small percentage of the massive volume of data originally collected is deemed relevant and discoverable at trial.

Microsoft reports that about 12.5% of the company’s domestic employees are currently under legal holds for pending or ongoing litigation, but only about one-third of those cases concern active litigation. “That means Microsoft preserves the vast majority of material based on some trigger event other than the filing of an


26. Microsoft Letter, supra note 19, at 3. This is a total of 14,805 separate custodian legal holds, but only 6,732 unique custodians because some of the company’s senior managers and executives are under legal holds for multiple issues.
actual lawsuit."  

If a matter reaches litigation, most of the custodians who were placed under a legal hold in connection with the matter contribute nothing to the information actually produced because most of the data collected is irrelevant or otherwise unusable. In its submission to the conference, Microsoft cites a recent survey conducted by the Searle Center on Law, Regulation, and Economic Growth at Northwestern University, for the proposition that "only 1 in 1000 pages produced in discovery is ever actually used as evidence to resolve the merits of a case." As Microsoft outlines in the letter, "the remaining 999 pages are produced at enormous cost – because they are the tip of a very large ice-berg." For every 2.3 MB of data that are actually used in litigation, Microsoft preserves 787.5 GB of data – a ratio of 340,000 to 1. Microsoft claims this disparity "stems from the conservative approach [it] takes at the earliest stages of a matter in order to avoid backward-looking scrutiny regarding the scope of preservation." Judge Rosenthal explicitly acknowledged this problem in Rimkus Consulting Group, Inc. v. Cammarata, noting that "[t]he frequency of spoliation allegations may lead to decisions about preservation based more on fear of potential future sanctions than on reasonable need for information."

Thomas Hill, Associate General Counsel for General Electric (GE) echoed Microsoft’s concerns in his written testimony for the December 2011 Congressional hearing on The Costs and Burdens of Civil Discovery. He asserted that "GE must guess whether a case will ever be filed, guess as to what claims may ever be brought, and then do its best to preserve an unspecified amount of information

27. Id.
28. Ultimately, Microsoft collects data from only 12 custodians rather than the 45 whose data was preserved under the original hold. Even information from the twelve custodians who ultimately contribute to a case is “further reduced through filtering based on date ranges, search terms, de-duplication, and other data minimization processes.” Through the use of third party vendors, Microsoft eliminates, on average, nearly 95% of the data originally under litigation hold for a case. Then, the company’s attorneys review and reduce that information resulting in only about 22% of the previously filtered set being produced. Id. at 4.
29. Id.
30. Id.
31. Id.
32. Id.
for an indefinite period of time.” 34 By way of example, Hill offered that if management makes a decision that could conceivably lead to a shareholder derivative suit against GE, current law requires the company to begin preserving potentially relevant information if they believe litigation could be “reasonably anticipated.” However, without knowing which claims may be asserted, and without any plaintiff, judge, or opposing counsel with whom to negotiate the relevance of ESI, the company must over-preserve to avoid the risk of sanctions in a case that may never be filed. 35 He then described a specific matter, limited to GE’s U.S. operations, in which the company had been preserving information for years even though no litigation is pending. 36 “In a company the size of GE,” posits Hill, “it would not be out of the ordinary for hundreds or even thousands of individuals to be involved in a subject matter that becomes the subject of litigation that lasts for many years.” 37

Although neither Microsoft nor GE specifically mentions any legal problems this mass preservation creates for them abroad, the practice undoubtedly runs afoul of non-U.S. privacy laws, especially those of the European Union. Under the arguably far-reaching EU rules, information need not be located in an EU Member State or even refer to someone living there to be subject to the strictures of EU data protection. This means that large multinationals, which operate globally and that have mobile employees working and interacting across multiple jurisdictions, create and collect data that is subject to EU regulation. Under those laws, the indiscriminate accumulation of this data in the United States, as described above, could be a sanctionable violation. The next section provides an overview of the European Privacy Framework in an attempt to outline the ways in which a wide range of potential evidence can fall within its ambit to inform a discussion on the conflicting legal duties created by the European data protection laws and American discovery procedures.

34. Discovery Hearing, supra note 25 (testimony of Thomas H. Hill, Associate General Counsel for General Electric).
35. Id.
36. Id.
37. Id.
III. European Privacy Laws and Their Enforcement

A. The European Privacy Framework

In 1995, the European Parliament passed Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the Directive or the Privacy Directive).\(^{38}\) It is the centerpiece of a framework of data protection laws in the European Union and the European Economic Area (EEA) that have been called the "most ambitious, comprehensive and complex in the field."\(^{39}\) These laws are based on principles of respect and dignity and they protect the rights of individuals to control information pertaining to them.\(^{40}\) The 1995 Directive treats the protection of personal data as a fundamental human right, thereby embodying "a profoundly European vision of what protection of privacy and personal data should involve."\(^{41}\)

The Directive is a model for legislation, which was enacted into law at the national level in each Member State.\(^{42}\) It is a distinct type of legislation from an EU-wide "regulation,"\(^{43}\) which would create a uniform law across the European Union. As a result, while data protection laws across the European Union are based on the same principles and are therefore similar, they are not the same, and entities operating in different states are expected to comply with the rules of each state to which their data processing activities are subject.\(^{44}\)

---

40. Whitman, supra note 1, at 1161.
41. Bygrave, supra note 6, at 33. This creates a sometimes-awkward balance between the European Union's goals of economic harmony and its strict notions of privacy. The Directive seeks to facilitate economic growth through the free flow of goods, persons, services, capital, and personal data by making privacy laws compatible across the EU Member States. At the same time, however, the Directive seeks to protect the right to personal privacy that is inherently jeopardized by this level of data circulation. Id. at 32.
42. Directive 95/46, supra note 6, at preamble recital 9; Bygrave, supra note 6, at 22.
43. Not to be confused with the word "regulation" in general.
44. The Directive, therefore, is a "lowest common denominator" establishing minimum requirements on which Member States must fashion their data protection laws. In fact, Member States have sometimes passed laws that are inconsistent with the Directive, specifically those pertaining to the transfer of data outside the European Union. Bygrave, supra note 6, at 32; See also ANDREW SERWIN,
The Directive applies to "personal data," which is defined broadly as any information that can directly or indirectly identify a person. The Directive applies to "personal data," which is defined broadly as any information that can directly or indirectly identify a person. This can include "anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer’s IP address." The person to whom the data refers is the "data subject" and the data belongs to that individual, not the entity that holds it. Use of the information is "data processing," defined as "[a]ny 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." Under these broad definitions, an email from Europe or an attached document may contain "personal data," and could potentially be evidence that might be preserved for an unspecified period of time in the event of a litigation hold.

The Directive states that data must be processed "fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Furthermore, the personal data is restricted to that which is "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed." Nor can personal data be kept in a form that identifies the data subject for "longer than is necessary for the purposes for which the data were collected."

In terms of U.S.-based litigation, data that has been preserved

---

47. SERWIN, supra note 44, at 4.
48. Directive 95/46, supra note 6, art. 2(b).
49. Id. art. 6(a)–(b).
50. Id. art. 6(c).
51. Id. art. 6(e).
may be "adequate and relevant" to a particular legal proceeding, but it is unlikely that that information is ever originally collected for use in a lawsuit. When a company retains data for litigation, EU law requires that the data subject explicitly consent to that use because this type of preservation is deemed "further processing" that is conducted for a purpose unrelated to the reasons the data were originally collected.52

The concept of a "data controller" is also central to the Directive's framework. This is the person or entity that "determines the purposes and means of the processing of personal data."53 The "data processor" processes the data on behalf of the controller and could be a third party such as a cloud service provider.

Additionally, the Directive mandates that each Member State establish an independent Data Protection Supervisory Authority (DPA) endowed with investigative powers and the ability to bring legal proceedings.54 Delegates from each country's DPA, together with representatives of the European Commission and the European Data Protection Supervisor make up the "Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data" (Article 29 Working Party or Working Party).55 The Working Party has a profound influence on implementation of the Directive through its recommendations, opinions, and working documents throughout the European Union.

The Article 29 Working Party has recognized that the concept of processing contained in the Directive directly implicates the preservation practices of U.S. discovery requirements. Retention of data is processing under EU law and "[c]ontrollers in the European Union have no legal ground to store personal data at random for an unlimited period of time because of the possibility of litigation in the United States however remote this may be."56 In American

52. This is in addition to the "unambiguous consent" the data subject must give, even for an initial act of processing. Id. art. 7(a); Legitimate Reasons for Processing of Personal Data, EUROPEAN DATA PROTECTION SUPERVISOR - THE EUROPEAN GUARDIAN OF PERSONAL DATA PROTECTION, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/QA6 (last visited Nov. 6, 2012).
53. Directive 95/46, supra note 6, art. 2(d).
54. Id. art. 28(1)-(3); they can also typically impose fines, although some DPAs cannot. See SERWIN, supra note 44, at 79.
55. AMERICAN BAR ASSOCIATION, supra note 45, at 79.
courts, however, the expectation is that a company that chooses to do business in the United States will abide by the Federal Rules of Civil Procedure, which mandate data preservation in some circumstances. But, as the Working Party points out, this is problematic because employees and customers of such a company are "data subjects" and not parties to any decision to do business in the United States that could expose their data to U.S. disclosure rules. Under the current EU regime, even an order from a U.S. judge directing a party to preserve data would not automatically create the legal grounds for doing so.

The Directive also closely regulates the transfer of information from one country to another — often a necessary step in producing evidence for U.S.-based litigation. Article 25 of the Directive prohibits the transfer of data to "third countries" — meaning countries outside the European Economic Area — that do not provide an "adequate level of data protection." The standard used to determine which countries' data protection regimes are "adequate" is stringent, and like most non-EEA countries, U.S. privacy laws do not qualify. Lawmakers have tried to alleviate difficulties created by the incompatibility between European data protection laws and U.S. discovery practices by approving regimes that allow multinational corporations to move data across borders if they adhere to certain standards endorsed by European data protection authorities. If data is preserved and transferred


57. Id. at 8.
58. Id.
59. Directive 95/46, supra note 6, art. 25.
60. Id. art. 25(1).
61. Bygrave, supra note 6, at 39.
62. Businesses can institute protocols that will bring them in line with the European framework. For example, a multinational corporation or group of companies can write its own privacy regulations, known as Binding Corporate Rules (BCRs), under which intracompany transfers of personal data across borders will not be held to violate EU data protection laws. AMERICAN BAR ASSOCIATION, supra note 45, at 81; See Overview on Binding Corporate Rules, EUROPEAN COMMISSION - JUSTICE, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm (last updated Apr. 23, 2012). The Directive itself also provides some exceptions to the strict regulation of data transfers. For example, data can be transferred if the data subject gives "unambiguous consent." Directive 95/46, supra note 6, art. 26(1)(A). Another important exception is the United States' Safe Harbor Scheme, which allows an
pursuant to these schemes, it is less likely to attract regulatory attention. However, because these arrangements are focused on the legality of data transfers, evidence that is already stored within the United States may fall outside their purview.

B. The Potentially Broad Applicability of European Union Data Protection Laws

While the Directive was pioneering in many ways, its drafters were particularly bold in tackling the thorny issue of which country’s laws apply to an act of data processing. Addressing applicable law issues for multinationals operating across countries within the European Union certainly involves complex considerations, but applying EU law to data that lies beyond the Member States is even more unwieldy. In some cases, the Directive’s terminology arguably provides for universal application of European data protection laws.

If a data controller has an “establishment” in a Member State, EU law will apply if an act of processing is performed “in the context of activities” of its establishment there. “The notion of

American company to self-certify that it complies with a set of privacy principles approved by EU authorities. A company that ascribes to the Safe Harbor Scheme can receive data from an entity within the EU. AMERICAN BAR ASSOCIATION, supra note 45, at 81; See Safe Harbor, EXPORT.GOV HELPING U.S. COMPANIES EXPORT, http://export.gov/safeharbor/ (last updated Apr. 11, 2012, 2:45 PM).


65. “The place at which a controller is established, implies the effective and real exercise of activity through stable arrangements and has to be determined in conformity with the case law of the Court of Justice of the European Communities.” Id. at 8. An establishment could be a “local office, a subsidiary with legal personality or a third party agency.” Article 29 Data Prot. Working Party, Opinion 1/2008 on Data Protection Issues Related to Search Engines at 10, No. 00737/EN, WP 48 (Apr. 4, 2008).

66. The key to determining whether EU law applies is the concept of the “context of activities” introduced in Article 4(1)(a). “The notion of ‘context of activities’ – and not the location of data – is a determining factor in identifying the scope of the applicable law.” Article 29 Data Prot. Working Party, Opinion 8/2010 on Applicable Law at 29, No. 0836-02/10/EN, WP 179, 2010) [hereinafter WP 179].
'context of activities' implies that the applicable law is not the law of the Member State where the controller is established, but where an establishment of the controller is involved in activities implying the processing of personal data." 67

For data controllers located outside the European Union, the Directive may apply if personal data is processed on "equipment" located inside the European Union, even if the controller has no physical "establishment" in any Member State. 68 The law that applies is the law of the Member State where the equipment used for data processing is located. 69 In this context, ownership of the equipment is not required and control over it need not be complete as long as the relevant data is processed on the controller’s behalf. 70 The Working Party interprets the word "equipment" broadly in part because it is translated in other European languages as "means." 71 Thus, "equipment" can refer to a process that is manual or automated, including "human and/or technical intermediaries, such as in surveys or inquiries." 72

It is the site of the equipment processing the data that determines jurisdiction, not characteristics of the data subject. A person need not reside in, or have citizenship of, any Member State for the protocols of the Directive to apply to their personal data as long as it is processed on equipment located in the European Union. 73 Accordingly, as with outsourcing or cloud computing, 74 a

The Working Party has clarified that the Directive "should apply in those cases where there is no establishment in the EU/EEA which would trigger the application of Article 4(1)(a) or where the processing is not carried out in the context of such an establishment." Id. at 20 (emphasis omitted).

67. WP 179, supra note 66, at 29.
68. WP 56, supra note 64, at 5. Article 4(1)(c) of the Directive states that its provisions shall apply when "the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community." Directive 95/46, supra note 6, art. 4(1)(c). According to the Working Party, the data controller must engage in some kind of activity which utilizes the equipment and have the intention to process personal data. WP 56, supra note 64, at 9.
69. WP 179, supra note 66, at 20.
70. WP 56, supra note 64, at 9.
71. WP 179, supra note 66, at 20.
72. Id.
73. Id. at 20-21.
74. Id. at 2 (Executive Summary); Recital 20 of the Directive also employs the
non-EU-based data controller could use equipment located in an EU Member State to process data that has no real connection with the EU/EEA, but to which the Directive still applies.\textsuperscript{75}

To illustrate these concepts, the Working Party offers the example of an online agenda service where the data controller will sometimes be the service provider and sometimes the user. In the former instance, the data subject, a user who may have no relationship with the European Union, uploads personal information to an online program, which the service provider organizes and synchronizes. "If the cloud service provider uses means in the EU, it will be subject to EU data protection law . . . . \textsc{[T]he application of the Directive would not be triggered by means used for transit purposes only, but it would be triggered by more specific equipment e.g. if the service uses calculating facilities, runs java scripts or installs cookies with the purpose of storing and retrieving personal data of users."}\textsuperscript{76} In the latter case, where the user is the data controller, a company may be using an online agenda service that itself has no connection to the European Union to schedule meetings with clients. "If the company uses the service in the context of the activities of its establishment in the European Union, EU law will be applicable to this processing of data via the agenda on-line . . . ."\textsuperscript{77}

Now that essentially all business is conducted and stored electronically, and given the Directive's potentially broad reach, it is not difficult to imagine myriad examples, such as those noted above, of practices that produce data that implicate privacy laws in several jurisdictions. In fact, for some businesses, such as social networking sites and internet companies, it may be harder to imagine ways in which the data they generate and collect might not be subject to the laws of more than one country. Data created by a multinational company and stored in the United States could implicate the Directive if it originated in the European Union, if it were processed in the context of activities of the enterprise's establishment in the European Union, or if it were otherwise processed using equipment located in a Member State. For the purposes of discovery, the fact that the data is retrieved from servers on U.S. soil does not

\textsuperscript{75.} WP 56, supra note 64, at 7.
\textsuperscript{76.} WP 179, supra note 66, at 22.
\textsuperscript{77.} Id.
necessarily exempt it from European privacy regulations.\textsuperscript{78}

Web 2.0 and networking sites further complicate the issue because users located in several different countries may contribute to a project on such sites. Preserving data created in this way, even on a server located in the United States, could implicate the rights of contributing EU data subjects.\textsuperscript{79} The ways in which individuals and corporations use these services is expanding, which means that information produced through these collaborative processes will become increasingly relevant to all types of litigation.\textsuperscript{80}

Furthermore, a laptop or a smartphone can be "equipment" for purposes of the Directive. When a website places a cookie on the computer of a data subject located in a Member State, the information communicated back to the web site controller, no matter where that controller is located, is subject to the protocols of the Directive.\textsuperscript{81} The same applies to programs like Java Scripts that allow remote servers to introduce information onto an individual's computer.\textsuperscript{82} In the words of the Article 29 Working Party: "The controller decided to use this equipment for the purpose of processing personal data and... several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory."\textsuperscript{83} Thus, EU law applies.

\textsuperscript{78} Theoretically, a company which has no establishment in any Member State, such as the online agenda service provider, but that targets customers in the European Union, has an obligation to comply with the data protection laws of every Member State to which it directs activities. If this company preserves data for litigation in the United States, it may be penalized in multiple EU countries.

\textsuperscript{79} Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking 6-7 (No. 01189/09/EN, WP 163, 2009) [hereinafter WP 163]. Although the considerations can become quite complex, in general, users of sites such as Facebook and Google Plus are classified as "data subjects" who are exempt from the Directive's restrictions because they are processing data "in the course of a purely personal or household activity." Directive 95/46, supra note 6, arts. 2(a) and 3(2). This is known as the "household exemption." Operators of those sites, however, are considered "data controllers" and are fully subject to the Directive. WP 163, supra at 5.

\textsuperscript{80} Although social networking discovery is currently used most frequently in individual-oriented litigation, such as personal injury suits, rather than in complex corporate disputes, its overall use is rising. Stephen W. Green, Social Media and E-Discovery: Impact and Influence, 2 BLOOMBERG LAW REPORTS - CORPORATE COUNSEL, 1 (2011).

\textsuperscript{81} WP 56, supra note 64, at 10-11.

\textsuperscript{82} Id. at 11-12.

\textsuperscript{83} Id. at 11.
In a likely scenario, a U.S.-based executive may travel throughout Europe sending and receiving information on his personal devices that could eventually be subject to a litigation hold in the United States. Because those devices are classified as "equipment" under the Directive, and may, at some point, be located within EU territory when data is processed, much of that information could be subject to Directive protocols.\footnote{In fact, just taking that data out of Europe to the United States could violate data transfer rules, unless the company at issue adheres to the Safe Harbor Scheme or has approved Binding Corporate Rules.}

In short, even if multinational companies, after instituting a litigation hold, only preserve evidence on servers in the United States, and continue to allow data kept in foreign offices to be expunged, information held in the United States may still fall within the ambit of European Union data protection laws. Currently, the likelihood that European regulators would prosecute such a violation seems remote, especially since they have historically focused on violations resulting from data transfers and production of information for discovery. However, data protection authorities realize that effective protection of the privacy of data subjects within the European Union requires a globalized approach and regulators are preparing to take a tougher stance against transgressors.

\textbf{C. The Trend Towards Increased Enforcement of European Union Data Protection Laws}

The extent to which data protection laws are enforced varies across the European Union, but recent trends indicate that lenient, localized enforcement is giving way to stricter sanctions and cross-border cooperation among regulators. Although adequate funding for DPAs across the European Union has been and may continue to be a problem, governments are reinvigorating these bodies with greater enforcement responsibilities. Additionally, consumers, themselves, are more aware of their privacy rights, and now report transgressions to the appropriate authorities, or use social media to focus attention on privacy breaches, which allows regulators to enforce with confidence.\footnote{Privacy at the Crossroads: Current Trends in Global Privacy Enforcement, HUNTON & WILLIAMS LLP (Jan. 12, 2012) [hereinafter Privacy Webinar], http://www.hunton.com/media/20120112_privacywebinar/player.html (last visited Nov. 6, 2012).}

Perhaps one of the most significant developments is the ever-
increasing amount of monetary sanctions. Previously, fines levied against companies for violating data protection laws, if assessed at all, had been low in all but a few cases. A turning point occurred in March 2011 when the French DPA, the CNIL, fined Google a record €100,000 for unlawfully gathering Street View data. The move indicated the CNIL’s serious stance towards enforcement, and is representative of a newfound willingness on the part of European regulators to take on large corporations like Google and Facebook. In the UK, the Information Commissioner’s Office (ICO), issued its first fine of £100,000 in November 2010 and has threatened sanctions of up to £375,000 since then.

Several EU Member States have also begun aggressively using privacy audits as an enforcement tool. In France alone, the number of audits rose from 100 to 300 between 2005 and 2010 and the CNIL plans to significantly increase that number even further. Both the

---


87. Commission nationale de l’informatique et des libertés.

88. Privacy Webinar, supra note 85.


90. Privacy Webinar, supra note 85; Google Bosses Convicted in Italy, BBC.COM (February 24, 2010, 12:38 GMT), http://news.bbc.co.uk/2/hi/8533695.stm (last visited Nov. 3, 2012) (Reporting that in 2010, Google Global Privacy Counsel Peter Fleischer and two other executives were convicted of violating the Italian privacy code for transmission of an offensive video). On February 2, 2012, the Article 29 Working Party announced that it had designated CNIL, the French data protection authority to complete an analysis of Google’s new privacy policies and asked the company to “pause” changes to the procedures. Letter from Article 29 Working Party to Google Inc. (Feb. 2. 2012).

91. The UK Information Commissioner’s Office (ICO) was authorized to impose fines under the Data Protection Act of 1998 in November of 2010. UK INFORMATION COMMISSIONER WEOLS FIRST FINES FOR VIOLATIONS OF DATA PROTECTION ACT, supra note 86.


93. Privacy Webinar, supra note 85; Sylvie Rousseau et al., France - An Update on the CNIL and Data Protection Enforcement, LINKLATERS (Sept. 20, 2011), http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-
ICO in the UK and the Irish DPA have augmented their use of audits as well.\(^4\) Still, European regulators and DPAs are calling for even broader power to regulate, enforce, and fine.\(^5\)

Amidst this climate of intensified monitoring and enforcement within Europe, regulators have also begun approaching their duties from a stance of longer arm jurisdiction. DPAs are being imbued with extended power to regulate and impose fines\(^6\) and have begun collaborating across jurisdictions in an unprecedented way – a manifestation of the cross-border nature of data processing today.\(^7\)

**D. The Proposed Data Privacy Regulation**

The most significant harbinger of what is to come, however, is the European Commission's announcement on January 25, 2012 of comprehensive reforms to the 1995 Directive that would update and modernize the law.\(^8\) The legislation is still in its preliminary stages, and subject to change, but the European Commission has highlighted certain key modifications to the existing framework that the reforms will include. Broadly defined, the proposed law creates affirmative obligations and increased accountability for organizations operating in and serving the European Union while augmenting protection for the rights of individuals. A major goal of the new legislation is to strengthen the role of DPAs, especially in the area of enforcement, to facilitate more effective compliance with data protection initiatives within the European Union. Unlike the

\(^{94}\) Privacy Webinar, supra note 85.

\(^{95}\) Both Peter Hustinx, the European Data Protection Supervisor, and Jacob Kohnstamm, the Chair of the Article 29 Working Party have been vocal about the need for increased accountability for data controllers and greater enforcement powers for DPAs. \textit{Id.}; European Data Protection Supervisor, Press Release, Reform of EU Data Protection Law: EDPS Calls on the European Commission to Be Ambitious in Its Approach (Apr. 29, 2010), http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/10/8.

\(^{96}\) The UK Information Commissioner's Office (ICO) was authorized to impose fines under the Data Protection Act of 1998 in November of 2010. UK INFORMATION COMMISSIONER WIELDS FIRST FINES FOR VIOLATIONS OF DATA PROTECTION ACT, \textit{supra} note 86.

\(^{97}\) Privacy Webinar, supra note 85.

\(^{98}\) The proposed new regime would be set forth in a regulation, which would have binding legal force across the Member States. This would be a significant step towards harmonizing the EU data protection rules and provide much sought after relief for companies who now navigate the differing privacy laws of each country in the European Economic Area. COMMISSION PRESS RELEASE, \textit{supra} note 46.
current regime where some DPAs can only issue recommendations, all DPAs under the regulation would have the power to impose fines for violations, which could reach one million Euros, or up to 2% of a company’s global annual turnover. 99

Additionally, in a deliberate step to clarify the European Union’s power to sanction privacy transgressions beyond its borders, the regulation would stipulate: “EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.” 100 Thus, lawmakers plan to explicitly empower data protection authorities to regulate information held by companies outside the European Union. In combination with additional tools to enforce compliance, and a general intent to aggressively pursue infringers, the proposed legislation would pave the way for DPAs to depart from the current practice of localized enforcement. 101

The massive volumes of data being preserved for litigation by multinationals operating in Europe fall squarely within the ambit of the proposed new law, and regulators stand poised to chastise offenders with a heavy hand. 102 Unfortunately for companies operating in the European Union or just storing data to which the Directive may apply, the threat of prosecution in Europe does not absolve them of the obligation to fulfill their duty to issue litigation holds and preserve relevant data for reasonably foreseeable litigation in U.S. courts.

IV. The American Attitude: Treatment of Non-U.S. Data
Privacy Laws in U.S. Courts

In American jurisprudence, it is well established that non-U.S. privacy laws do not preempt the power of an American court to order production of evidence for discovery purposes. This remains

99. Id.
100. Id.
102. Id. As Google Global Privacy Counsel Peter Fleischer put it bluntly in his blog post of JANUARY 2, 2012, “there’s going to be a lot more privacy enforcement actions. By a lot of different government authorities, not just DPAs. And the sanctions/damages are going to go through the roof.” Peter Fleischer, Peter Fleischer: Privacy...?: Harsher Data Protection Sanctions Are Coming, PETER FLEISCHER: PRIVACY...? (Jan. 2, 2012, 4:08 PM), http://peterfleischer.blogspot.com/2012/01/harsher-data-protection-sanctions-are.html (last visited Nov. 3, 2012).
true even if a litigant would be subject to civil or criminal penalties under foreign law for producing the information. Data protection laws, such as European Data Protection Directive 95/46 and its predecessors, are not the only type of legislation that can hinder the success of international discovery. Several European nations have enacted blocking statutes, which are designed for the express purpose of thwarting discovery for U.S.-based litigation. Although both privacy laws and blocking statutes prevent the transfer of certain kinds of documents to the United States for use in a legal proceeding, blocking statutes arose from contempt for American-style discovery rather than the desire to protect substantive privacy rights.

In addition, the United States is a signatory to the Hague Convention on Taking of Evidence Abroad (the Hague Evidence Convention or the Convention), which “prescribes certain procedures by which a judicial authority in one contracting state may request evidence located in another contracting state.” Blocking statutes, data protection laws, and the Hague Evidence Convention, if invoked, can all thwart a litigant’s ability to fulfill an international discovery obligation. At the same time, litigants who fail to comply with discovery orders may be subject to sanctions in U.S. courts. As noted above, difficulties in resolving this conflict usually arise in the context of orders to produce information for discovery and often involve data that must be collected overseas and transferred to the United States. Nonetheless, the principles developed to address the laws concerning production of ESI may become increasingly important at the preservation stage of the discovery process because of the intensified enforcement efforts from Europe, even where data transfers are not at issue.


106. Aérospatiale, 482 U.S. at 524.
A. The Case Law Governing the Applicability of Foreign Privacy Laws in U.S. Courts

In the foundational case, Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa, the Supreme Court established the bases for two important precedents regarding document production from foreign jurisdictions. First, the Hague Evidence Convention is not the exclusive means for obtaining evidence located abroad, nor must litigants resort first to Convention procedures whenever discovery is sought extraterritorially. Second, the Court approved a balancing test set forth in the Restatement (Third) of Foreign Relations Law of the United States to guide judges in determining whether to order litigants to produce information despite claims that they could suffer penalties under foreign law for doing so. This analysis, which embodies principles of international comity, fairness to litigants, evidentiary necessity and procedural fairness, applies broadly to blocking statutes and data protection laws alike. Since the Aérospatiale decision, use of the test has frequently resulted in pro-forum results, in part because American courts are generally hostile towards blocking statutes. However, judges in the United States are increasingly adept at accommodating non-U.S. substantive data protection laws.

Nevertheless, while U.S. courts may be more deferential to European privacy laws than blocking statutes, they are “often so

107. Id. at 529, 542.
108. Id. at 556.
109. See In re Global Power Equip. Group Inc., 418 B.R. 833, 850 (Bankr. D. Del. 2009); but see Linde v. Arab Bank, PLC, 262 F.R.D. 136, 152 (E.D.N.Y. 2009) (“[T]he above factors weigh in favor of denying Arab Bank’s discovery of the Protected Materials.”); see also Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1478 (9th Cir. 1992) (“We therefore conclude that the order compelling discovery should be upheld in spite of the PRC secrecy statute.”).
110. The Court in Aérospatiale noted, “The American Law Institute has summarized this interplay of blocking statutes and discovery orders: ‘[W]hen a state has jurisdiction to prescribe and its courts have jurisdiction to adjudicate, adjudication should (subject to generally applicable rules of evidence) take place on the basis of the best information available...[Blocking] statutes that frustrate this goal need not be given the same deference by courts of the United States as substantive rules of law at variance with the law of the United States.’ See Restatement, § 437, Reporter’s Note 5, pp. 41, 42.” Aérospatiale, 482 U.S. at 544 n.29.
111. Even the Article 29 Working Party has recognized that U.S. courts have become more sensitive to the reality of enforced compliance with data protection laws in Europe since Aérospatiale. WP 158, supra note 56, at 6.
tied to the liberal domestic discovery practice that they fail to fully appreciate the scope of data privacy laws worldwide, especially in the EU.”¹¹² In *Strauss v. Crédit Lyonnais, S.A.*, the district court determined it was proper to compel production of documents located abroad after conducting a systematic analysis of the factors articulated in the *Aérospatiale* balancing test. Specifically, the court considered:

(1) the importance to the . . . litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine the important interests of the state where the information is located.¹¹³

The fifth factor, the comity factor, which entails assessment of the competing interests of the United States and the nation from which discovery is sought, was “of the greatest importance in determining whether to defer to the foreign jurisdiction.”¹¹⁴ Applying the *Aérospatiale* factors to the specific facts of the *Strauss* case, the court concluded that the U.S. interest in “fully and fairly adjudicating matters before its courts,”¹¹⁵ outweighed the French interest in having its privacy laws enforced.¹¹⁶

In terms of synchronicity with the European Data Protection Directive, it is noteworthy that the *Aérospatiale* factors contemplate whether the relevant information originated in the United States, rather than where the data is or has been located or processed. In *Strauss*, the plaintiffs obtained bank documents from France without

---


¹¹⁴ *Id.* at 213.

¹¹⁵ *Id.* at 214 (quoting Minpeco, S.A. v. Conticommodity Services, Inc., 116 F.R.D. 517, 523-24 (S.D.N.Y. 1987)).

¹¹⁶ *Id.* at 222 ("Crédit Lyonnais's purported obligations to preserve bank customer secrecy (Article L 511-33), and comply with French anti-money laundering and anti-terrorism laws (Articles L 561-1 to L 563-5), judicial secrecy laws (Articles 11 and 434-7-2) and the French blocking statute (French Law No. 68-678), do not preclude the bank from responding to plaintiffs' discovery demands . . .").
the consent of the bank or its customer and argued they were discoverable because they were located in the United States where the French privacy law did not apply. The court rejected this argument stating it was "unaware of any precedent which ignores the bank-customer relationship simply because the documents at issue are currently located in the United States." The court pointed out that the Restatement factors address where the documents "originated," not where they are "located." The Strauss decision shows some respect for the French privacy statutes, but it also underscores the ad hoc, case law-oriented analytical framework American courts use to determine the applicability of non-U.S. data protection laws. How would the Restatement factors resolve the issue of whose law applies to an email sent from Europe to the United States? Or even more perplexing, where do Web 2.0 documents, such as the hypothetical online agenda discussed, supra, originate?

Since Aérospatiale, numerous cases have addressed the incongruity between the privacy interests protected by European legislation and the needs of parties to U.S. litigation to obtain discovery. The outcomes are dependent on the unique facts of a particular case, and the court's consideration of each factor in the balancing test. Still, themes are emerging in the case law that are relevant to application of non-U.S. data protection laws at the preservation stage.

For example, litigants may need to prove that authorities in the foreign jurisdiction will enforce the non-U.S. privacy law against them for producing information in violation of a foreign law. The Strauss court found it persuasive that there was no "indication that civil or criminal prosecutions by the French government or civil suits by [bank customers were] likely, rather than mere possibilities." In United States v. First National City Bank, the court heard extensive testimony from German law experts before concluding that the party resisting production of bank documents "would not be subject to criminal sanctions or their equivalent under German law." The judge found "that there was only a 'remote and speculative' possibility that [the party] would not have

117. *Id.* at 209.
118. *Id.*
119. *Id.* at 224.
120. United States v. First Nat'l City Bank, 396 F.2d 897, 900 (2d Cir. 1968).
a valid defense if it were sued for civil damages” in Germany.\textsuperscript{121}

These cases represent a trend in U.S. litigation: lack of prior prosecutions under the statute alleged to be violated by compliance with the discovery request weighs in favor of ordering production.\textsuperscript{122} However, even a showing that there have been prosecutions for violations of the non-U.S. law may leave an American judge undeterred.

In 2007, for the first time, the French Supreme Court sustained criminal penalties and fines against a French lawyer who violated a blocking statute when he tried to obtain evidence in France for U.S.-based litigation.\textsuperscript{123} But, since that conviction, U.S. courts have continued to order discovery from France.\textsuperscript{124} For example, in a 2009 case, In re Global Power, the court concluded that, despite evidence of enforcement, the chance of prosecution remained “minimal,” especially in light of the fact that the party opposing discovery “identified only one case where the French Blocking Statute ha[d] been used to prosecute a French national for engaging in discovery without going through the Hague [Evidence Convention] Procedures.”\textsuperscript{125} The court quoted precedent decided prior to the French lawyer’s conviction in 2007 for the proposition that “the French Blocking Statute does not subject defendants to a realistic risk of prosecution.”\textsuperscript{126} EU regulators have not yet held companies liable for their mass preservation of evidence in the United States, so demonstrating there is a possibility of prosecution for this practice, even in the face of increased enforcement in Europe, could prove difficult.

In Columbia Pictures v. Bunnell, the court noted “[a] party relying on foreign law has the burden of showing that such law bars the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{121} Id.
\item \textsuperscript{122} See United States v. Vetco Inc., 691 F.2d 1281, 1289 (9th Cir. 1981) (“No case has been cited in which a person has been prosecuted for complying with a court order enforcing an IRS summons.”).
\item \textsuperscript{124} Id. at 1; See also In re Air Cargo Shipping Services Antitrust Litig., 278 F.R.D. 51, 54-55 (E.D.N.Y. 2010) (ordering production of documents despite violation of the French blocking statute).
\item \textsuperscript{125} Id. at 849.
\item \textsuperscript{126} Id. at 850.
\end{itemize}
\end{footnotesize}
discovery in issue," and Defendants in the action had not met this burden. In that case, the defendants used a third-party web hosting service to store data in the Netherlands. The court ordered them to preserve and produce information held there by a Dutch company despite Defendants' claim that the Netherlands Personal Data Protection Act barred them from producing the relevant information. The magistrate judge found that the IP addresses, at issue in the case, identified computers, not individuals, and so did not fall within the ambit of "identifying information," which was the type of data to which the Dutch statute applied.

The judge's final order, however, still reserved the right to require production, if necessary, in a form that did not mask the IP address holders' identities. Thus, while deferring at first to European privacy principles, the judge's main concerns lay with American values of broad discovery.

Similarly, it is significant that the magistrate judge in Bunnell seemed to consider preservation a lesser evil than production. In her emphasis on the rule from Aérospatiale she adds a telling parenthetical: "[F]oreign blocking statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce (let alone preserve) evidence even though the act of production may violate that statute." Under the European Data Protection Directive, however, preservation is "data processing" and information stored in this way is subject to legal limitations.

The Bunnell opinion also highlights the reality that litigants claiming non-U.S. law bars discovery face an even higher burden than they would arguing for application of other areas of non-U.S. law. The court may conduct its own research to determine the

---

128. Id at 452.
130. Id.
131. Id. at *14 ("[D]efendant [sic] are not, at least at this juncture, ordered to produce such IP addresses in an unmasked/unencrypted form.").
132. Id. at *12 (emphasis added).
133. PROSKAUER ROSE LLP, supra note 104, at ch. 8, § 3; see also Strauss v. Crédit Lyonnais, S.A., 242 F.R.D. 199, 207 (E.D.N.Y. 2007) (The party resisting discovery must show that "such law actually bars the production or testimony at issue ..."
relevance of foreign law, but it is under no obligation to do so. A court is also free to give little or no weight to a party’s submissions on the applicability of foreign law. With such amorphous guidelines, the extent to which European data protection laws will be interpreted in accordance with their legislative intent as understood by the Member States to which they apply is variable. Indeed, a good example of a misinterpretation is the magistrate judge’s assumption in Bunnell that requiring preservation of data located in the Netherlands was legally less onerous than ordering production of that information.

A lack of expertise in the applicable foreign law on the part of American judges may mean that even their good-faith attempts to try to accommodate the needs of litigants facing a conflict of laws due to discovery requests could be misguided. And while European regulators have not vigorously enforced violations of the Directive resulting from judicial misapplication of and disregard for EU privacy laws in American courts, they have begun devoting more attention to the issue.

B. European Regulators Call for Dialogue

On February 11, 2009, through publication of Working Party Paper 158 on Pre-Trial Discovery for Cross-Border Civil Litigation (WP 158), EU authorities officially addressed the growing tension and “describe, inter alia, the provisions of the foreign law, the basis for its relevance, and the application of the foreign law to the facts of the case.”) (internal quotations omitted) (emphasis omitted); see also Weiss v. Nat’l Westminster Bank, PLC, 242 F.R.D. 33, 40 (E.D.N.Y. 2007) (“[T]he party resisting discovery must provide the Court with information of sufficient particularity and specificity to allow the Court to determine whether the discovery sought is indeed prohibited by foreign law.”) (internal quotations omitted).

134. Bel-Ray Comp., Inc. v. Chemrite (PTY) Ltd., 181 F.3d 435, 440 (3d Cir. 1999) ("This rule provides courts with broad authority to conduct their own independent research to determine foreign law but imposes no duty upon them to do so.").

135. Euromepa, S.A. v. R. Esmerian, Inc., 154 F.3d 24, 28 n.2 (2d Cir. 1998) (noting federal courts “are not required to take all allegations of [foreign] law proffered by [a party] to be true”).

136. For example, in some situations similar data is held both in Europe and in the United States. In such scenarios, when a production order could expose a litigant to liability for violating a foreign data protection law, the court may order production of the data that is held in the United States rather than the same type of data held in Europe. However, as shown, if the data falls within the jurisdiction of the Directive, the fact that it is located in the United States is irrelevant. The longer arm of jurisdiction now reaching across the Atlantic could render concessions such as this from U.S. judges moot.
between the European interest in strong data protection laws and the needs of litigants in U.S. courts to provide for broad disclosure.\textsuperscript{137} The paper is not, and does not claim to be, a comprehensive set of guidelines to govern cross-border discovery disputes; rather it enumerates certain discussion points in a call to dialogue about the issue. Predictably, the document specifically identifies preservation of information in anticipation of litigation as "processing" subject to Directive protocols.\textsuperscript{138} Although processing for "compliance with a legal obligation to which the controller is subject" is one of the criteria that can make data processing legitimate under the Data Protection Directive,\textsuperscript{139} the Working Party states that "[a]n 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."\textsuperscript{140} The paper highlights the ways in which data can be lawfully disclosed under the Directive and encourages U.S. lawyers to cooperate with European data supervisory authorities.\textsuperscript{141}

WP 158 references the Sedona Conference Framework for Cross-Border Discovery (Cross-Border Discovery Framework) for some of its conclusions about American jurisprudence regarding conflicts between the European Union and United States over data protection in discovery. The Cross-Border Discovery Framework is a product of the Conference's Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6) which specifically addresses issues relevant to multinational companies that may be subject to conflicting laws. The Cross-Border Discovery Framework engages the kinds of problems that the Working Party discusses, but from the perspective of U.S. courts.\textsuperscript{142} The WG6 responded to WP 158 with a letter accepting the


\textsuperscript{138} WP 158, \textit{supra} note 56, at 8.

\textsuperscript{139} Directive 95/46, \textit{supra} note 6, art. 7(c).

\textsuperscript{140} WP 158, \textit{supra} note 56, at 9.

\textsuperscript{141} \textit{Id.} at 10.

invitation to dialogue.\textsuperscript{143}

The WG6’s letter directly addresses preservation issues that the Working Party raises in WP 158. In an attempt to assuage some of the Working Party’s concerns, the WG6 highlights the fact that “a party need only preserve relevant information” and discovery requests are “subject to limitations of proportionality and concerns for privacy and confidentiality.”\textsuperscript{144} While this response is consistent with the Sedona Conference’s framework for analysis and best practices principles,\textsuperscript{145} it largely ignores the reality that many multinationals are data hoarders and over-preservers.\textsuperscript{146}

The goal of this transnational dialogue between the Working Party and the WG6 appears to be a “win-win” situation where data minimization practices that bring companies into compliance with EU laws in turn result in lower discovery costs for American litigants.\textsuperscript{147} While that is certainly a rosy possibility, developed extensively in conference papers and working documents it seems an unlikely reality in the near future. The competing values — broad discovery as the foundation of our adversarial system, and privacy as a fundamental human right — are proving difficult to reconcile. While cooperation can certainly achieve some level of comity, the fact that U.S. preservation practices have attracted the interest of European regulators may be more likely to lead to penalties rather than compliance.

\section*{V. Conclusion}

Faced with spoliation sanctions in the U.S. or preservation sanctions in Europe, multinationals face a Hobson’s choice. However, until vigorous enforcement of preservation practices eventuates, corporations are likely to maintain their current policies because they ensure compliance with U.S. law under which

\begin{itemize}
\item \textsuperscript{144} \textit{Id.} at 7.
\item \textsuperscript{145} \textit{See Sedona Best Practices, supra} note 12 at 11.
\item \textsuperscript{146} The Sedona Conference recognizes that multinationals are data hoarders in its Recommendations for Best Practices, but suggests this is a result of bad records management strategies and is not necessary. \textit{Id.} at 21.
\item \textsuperscript{147} Joshua Kubicki, \textit{Yes, There Is Such a Thing as EU Data Privacy}, \textit{Legal Transformation: The Legal Profession} (Feb. 25, 2010), http://www.legaltransformationblog.com/2010/02/yes-us-there-is-such-thing-as-eu-data.html.
\end{itemize}
spoliation sanctions appear much more real. Unlike the laxity that has characterized European data protection enforcement, U.S. courts remain undeterred by the possibility that their discovery orders will obligate litigants to violate foreign laws. Times are changing, though, and European data protection authorities are entering a new era of increased enforcement. Soon to be armed with a new EU-wide regulation and with the public already on their side, regulators could begin sanctioning violations with a vengeance. Whether they will single out multinational data hoarders in the context of U.S. litigation remains to be seen, but those companies should be wary. With both sides taking a strong stance, clashes are inevitable.