Can Europe learn from US E-discovery?

Intellectual Property Forum: journal of the Intellectual and Industrial Property Society of Australia and New Zealand
Issue 96 (Mar 2014)

Pailli, Giacomo[1]

Abstract: There may be several reasons that explain why a European scholar should approach the topic of discovery in general, beginning from a sense of fascination toward one of the features of the so-called American Exceptionalism. Without having the possibility of dealing here with all of them and to explore every facet of discovery, I would like to underline one practical and one theoretical consideration that suggest the opportunity to shed light on electronic discovery.

Personal Author:	**Pailli, Giacomo**;
Source:	Intellectual Property Forum: journal of the Intellectual and Industrial Property Society of Australia and New Zealand, No. 96, Mar 2014: 44-54
Document Type:	Journal Article
ISSN:	0815-2098
Subject:	**International economic relations**; **Electronic discovery (Law)**; **Civil procedure**;
Peer Reviewed:	Yes
Affiliation:	(1) University of Florence

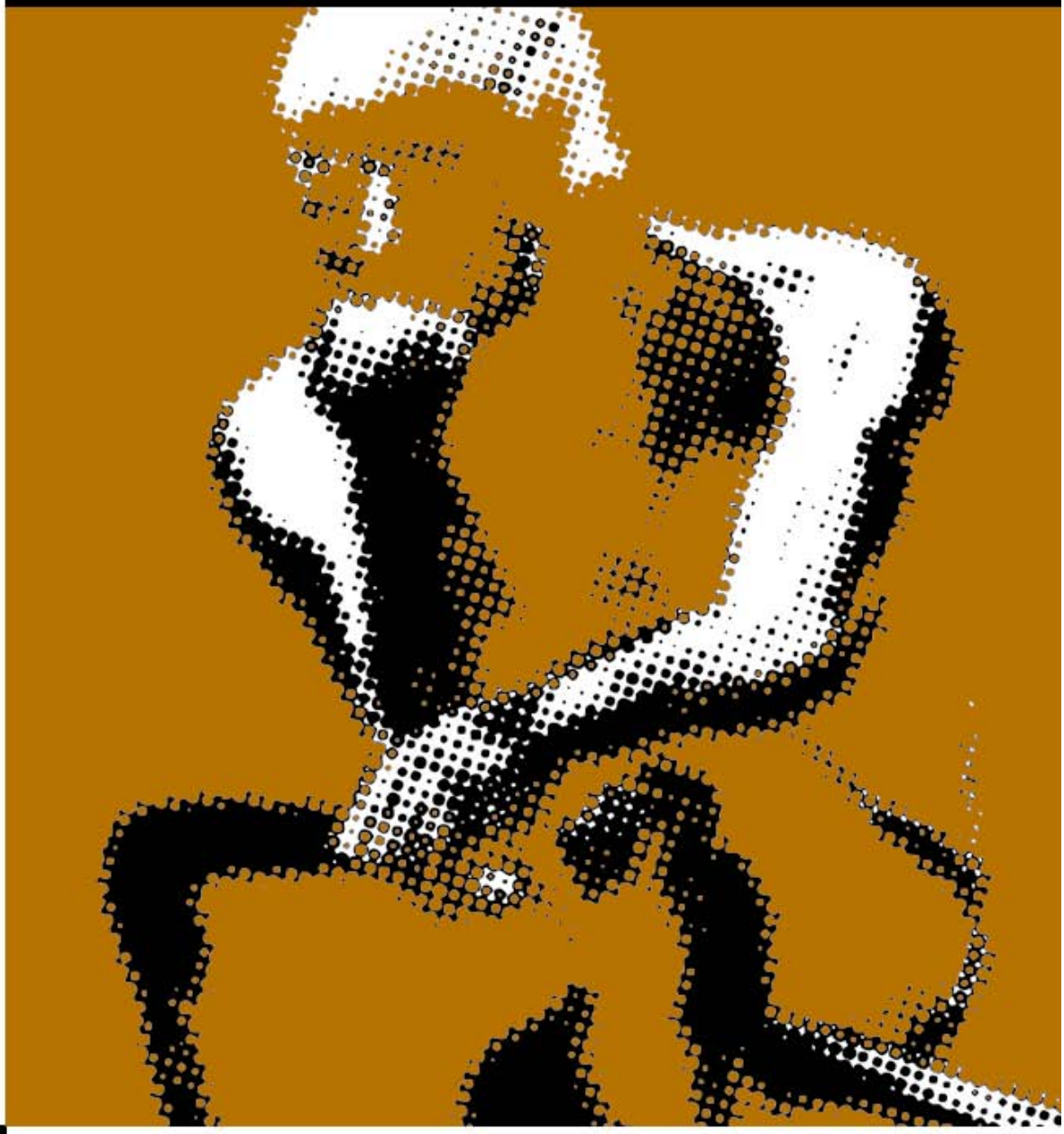
Database: **HUMANITIES & SOCIAL SCIENCES COLLECTION**

Journal of The
Intellectual Property
Society of Australia
and New Zealand Inc.

March 2014

Editor
Christopher Sexton

Intellectual Property Forum



Issue 96 Contents

Can Europe Learn from US E-discovery?

Dr Giacomo Pailli*
University of Florence

Introduction

There may be several reasons that explain why a European scholar should approach the topic of discovery in general,[1] beginning from a sense of fascination toward one of the features of the so-called *American Exceptionalism*.[2] Without having the possibility of dealing here with all of them and to explore every facet of discovery, I would like to underline one practical and one theoretical consideration that suggest the opportunity to shed light on electronic discovery.

From a concrete point of view, suffice to say that transnational commerce increasingly exposes European entities to contacts with the American market. While most of the time everything goes well, there are instances in which litigation, or threats of litigation, might come up. In all these cases, European companies should be ready to take into account the various duties related to US discovery or face the risk of serious sanctions. As some notable cases show,[3] US judges may be not very lenient toward foreign parties, usually defendants, who do not or cannot produce what is being requested by the other party.[4] While this also happened well before computers made their appearance on the scene, the new digital era poses brand new challenges both in terms of quantity and quality of discovery.[5]

At the theoretical level, instead, the procedural philosophy that has long informed the rules of civil procedure in Europe, which in the field of evidence is well summarised by the principle *nemo tenetur edere contra se*, seems no longer capable of meeting all the needs of a modern culture of litigation.[6] Rules that were built upon the paradigm of the bourgeois citizen owner of land, with a "one rule fits all" approach, strive to adapt to today's relations. Disputes more often arise between small and isolated consumers or employees on one side and complex transnational corporations on the other, hardly comparable one to the other. No doubt that one party cannot match the resources and power of the other, which sometimes outweighs even national public authorities entrusted with supervisory and regulatory functions.

In such a scenario, some of the instruments that America's civil procedure has crafted are of the utmost interest in view of levelling the playing field to achieve equality and, in the end, a better justice. These devices range from *class actions* allowing isolated damaged individuals to get together against a giant,[7] through *treble damages*, channelling egoistic instincts toward public welfare,[8] to, finally, *discovery*, sometimes the only way to find evidence jealously kept by the wrong-doer and to bring a meritorious claim.[9] No doubt these means can be, and maybe too often are, abused by unprincipled plaintiffs and greedy lawyers blackmailing corporate defendants to obtain favourable settlements.[10] Nor they should be simply transplanted in the European legal environment. Nonetheless, each represents an attempt to answer today's emerging issues, and each should be seriously taken into account either as a paradigm or as a benchmark for European experiments in this direction.

With specific reference to discovery, both the "Enforcement" directive on the protection of intellectual property[11] and the English[12] and French[13] experience tell us that European law-makers are realising that certain interests can only be protected through a partial retreat of the *nemo tenetur* principle and on means of compelling corporations to produce their documents, rightly considered their "DNA".[14]

Without resisting the temptation to throw such a large stone in the pond, I am now forced to narrow such a broad topic down and focus on the novelty that the digital revolution has brought to discovery. The article begins by considering whether e-discovery is in fact a real revolution or simply an evolution of traditional discovery. The next section will describe the case of *Zubulake*, an instructive and clear example of the issues and risks surrounding e-discovery. I then deal with some of the most interesting aspects and questions raised by the interaction between computers and discovery, beginning first with a seemingly easy task such as the definition of "document". Next, I consider a point of clash between US and Europe philosophies when US e-discovery is directed toward European personal data, a mismatch that might expose European companies to conflicting duties and difficult decisions. The last two sections address the duties to preserve and protect and the costs related to US e-discovery, as well as some of the solutions that US judges and rule-makers have developed.

Revolution or Evolution?

A first question that may be asked with regard to e-discovery is whether the "e" represents a revolution or an evolution of traditional paper discovery. In the first case, a whole new body of rules would be needed, while in the latter Rule 26 of the Federal Rules of Civil Procedure (FRCP) could still provide, with some adjustment, a suitable bedrock for e-discovery procedures.[15] Scholars tend to agree that e-discovery is surely a major development of traditional discovery, but falls short of a revolution; it is an evolution, no more than what happened when, in the 1950s photocopying machines made their appearance, dramatically altering the way discovery was being made.[16]

This is one of the reasons that allows us to deal only with the peculiar features of e-discovery, without entering into the complexities of the whole phenomenon.[17] A real revolution, on the other side, took place (and is still taking place) inside law offices. The technological aspects of e-discovery, in fact, have caused new professionals and service providers to appear on the market, as well as brand new departments of lawyers being constituted to face the hurdles of digital world.[18]

Regardless of its non-revolutionary nature, e-discovery has still rendered amending the FRCP necessary. The Supreme Court did so in December 2006, modifying Rules 26 and 34, answering some of the doubts that had been expressed by the Bar[19] and adopting some of the recommendations that came from frontline judges.[20] The most significant amendments related to the definition of the term *electronically stored information* (ESI),[21] the forms of e-data production[22], the possibility of avoiding discovery of electronic material when too costly or time-consuming,[23] provision to allowing the parties to dispute before the court the format of electronic document production[24] and, finally, a "safe harbour" against sanctions for data spoliation caused by the routine operating of a business.[25]

The Case of *Zubulake*

In order to understand how e-discovery works in practice, as well as to present some of the issues that arise in this field, it may prove useful to describe the seminal and multimillion dollars litigation between Laura Zubulake and UBS Warburg[26] before the US District Court for the Southern District of New York. This most-cited case gave the chance to Judge Shira Scheindlin, a renowned judge in this field, to deal with and solve many issues.[27]

By way of background, UBS hired Laura Zubulake in 1999 as one of the directors of the US Asian Equities Sales Desk, with a salary of approximately $500.000 and the promise to be considered as head of the desk in the short term. When, in December 2000, the place became vacant, however, the company preferred another employee to fill the position, Matthew Chapin, who immediately started discriminating against Laura Zubulake. After a few months of this treatment, in August 2001, Zubulake filed a complaint with the Equal Employment Opportunity Commission (EEOC). No more than two months later, UBS fired Zubulake with two weeks' notice. She responded by suing UBS in the US District Court for the Southern District of New York, claiming $13 million in compensatory damages, as well as punitive damages[28] for discriminatory treatment and retaliatory termination.

During the long phase of pre-trial discovery, the parties agreed to limit the number of emails to be produced. More specifically, Zubulake gave up her previous request for "[a]*ll documents concerning any communication by or between UBS employees concerning Plaintiff*"[29] *"includ*[ing]*, without limitation, electronic or computerized data compilations*",[30] agreeing to narrow it down to the accounts of five individuals. In turn, UBS agreed "*unconditionally to produce responsive e-mails from the accounts of* [these] *five individuals*".[31]

In honouring this agreement, however, UBS produced only 100 pages of emails, while Zubulake produced approximately 450 pages: this difference strongly suggested that it was at least likely that UBS had not produced a substantial part of the requested material.[32] It turned out that what was missing were emails sent and received by the five accounts, which had been deleted from the personal computers and were stored only in the backup tapes that UBS kept as a sound business practice.[33] It was likely that those emails contained information potentially relevant to Zubulake's case, since a sort of smoking gun had already been found: one of UBS managers suggested in an email to fire Zubulake immediately ("Exit her ASAP") after she had complained to the EEOC, adding that this could have the positive effect of also depriving her of the annual bonus.[34] UBS, however, answered that recovering the files from the backup tapes would be too expensive, and requested the Judge to shift the relative costs on the demanding plaintiff.[35]

Judge Scheindlin, after developing a new test to determine when cost should be shifted on the demanding party,[36] devised a reasoned solution

that took into account the conflicting needs of the parties.[37] The Judge, in fact, ordered UBS to recover, at its own expense, the emails stored on a sample of five out of 94 pertinent tapes, reporting in detail the time and cost of the operation.[38] On the basis of the sample, the Court would then decide on the cost shifting issue.

UBS, thus, performed the task and reported that recovering the emails from the first five tapes cost around $19,000,[39] while the total costs for all tapes was counted as amounting to more than $ 270,000,[40] including, both times, the fees for UBS's lawyers' review. Judge Scheindlin, applying her own test as developed in *Zubulake I*, shifted to the plaintiff 25% of the expenses for recovering the emails, excluding, however, any lawyers' fees, which were to be borne entirely on UBS.[41]

The dispute is further complicated when the recovery process made it clear that some of the backup tapes were no longer usable.[42] Contrary to the (oral) directives given by its attorneys and to the general duty to preserve evidence when litigation is reasonably foreseeable,[43] UBS recycled some of the backup tapes, destroying the data previously stored. Some emails were forever lost, and this meant "data spoliation".[44] Zubulake reacted by moving to have UBS's behaviour sanctioned in three ways: setting aside the cost shifting order; instructing the jury to draw an "adverse inference" from UBS's failure to comply with its duties; and ordering UBS to bear all expenses related to the re-deposition of the witnesses whose emails were destroyed. Judge Scheindlin, in her *Zubulake IV* decision, granted only the last measure, considering the request for an "adverse inference" an *extrema ratio* to punish only the most serious violations.

The procedural epilogue is reached in the last decision, *Zubulake V*. Following the depositions ordered in *Zubulake IV* and additional emails produced by UBS, it was clear that both UBS and its lawyers seriously breached their duties to preserve and produce evidence.[45] Zubulake was able to prove that, in addition to the violations already sanctioned in *Zubulake IV,* other emails, potentially relevant to the case, had been destroyed, that some emails were produced only after more than two years from the beginning of the pre-trial discovery phase, that UBS failed to preserve the evidence and that, in general, UBS employees intentionally erased several emails after Zubulake had already formally lodged her lawsuit before the Court. The picture was so serious, and the violations were so many, that Judge Scheindlin eventually instructed the jury on the possibility to draw an adverse inference from UBS's behaviour. The verdict was heavy: the jury awarded to Zubulake $9.1 million in compensatory damages and $20.1 million in punitive damages,[46] following which the parties reached an undisclosed settlement.

Notwithstanding the difficulty of reducing such a complex dispute in few paragraphs, *Zubulake* suggests several points of analysis on e-discovery, highlighting issues such as the costs associated to e-discovery, the objective and subjective scope of the duties to preserve and produce evidence for future litigation and the possible sanctions for failing to comply with such duties. Additional issues that are worth exploring are the definition of "document" and the interaction between e-discovery and the protection of privacy rights. In the next sections I shall try to address some of the most significant aspects of US e-discovery, showing how American law developed and adapted to the challenges brought by technological changes.

Definition of "Document"

Notwithstanding that *Zubulake* does not focus directly on this issue, the first challenge that technological progress offers is represented by the definition of "document". Where in traditional paper discovery a document is essentially a sheet of paper, the digital revolution blurs the picture. Only a portion of electronic documents is the digital counterpart of traditional paper documents, simply stored on a different medium (such as text documents or emails). Many other present peculiar features.[47] Some electronic "documents" are the result of operations (such as queries) performed on dynamic databases, so that they cannot be said to be really "existing" outside such operation.[48] In general, an electronic document may include the positioning of a mobile phone, the access log of a building security system,[49] the log of an electronic toll collection device,[50] the GPS positioning of a vehicle, data on access and activities performed on a computer system, audio or video files, photographs,[51] and much more. What all these elements have in common is not being "documents", but rather being "*electronically stored information*".

It is also worth noting that even those documents that are more akin to a paper sheet, in fact hide in the lines of their digital code a series of additional and valuable information. A sheet of paper contains no more than what is written on its surface. It is hard to determine its real author, as well as the phases and moment of its creation. On the contrary, an electronic document is accompanied by additional information, called *embedded* and *meta data*,[52] in which one can read about

the document's author(s), the dates of creation and modification, possibly the various stages of evolution of the document and the identity of who made those changes. It is clear that these data, if played in the right way, can win or lose a game, for instance uncovering the lies of who says that they did not author a document or showing that, following certain events, a memorandum was altered and how.

Furthermore, anything that is stored on a digital medium enjoys the additional feature of not being easily erasable. The *delete* key does not actually remove the electronic document from the realm of being, but simply marks the corresponding physical space on disk as available for writing.[53] It can take days, months or even years before the system, in fact, writes on these sectors. During this whole period, and sometimes even after, the electronic document remains there, ready to be recovered by specific software.[54] Moreover, *Zubulake docet*, it is a good commercial practice to keep back-up copies of the entire content of the company's computers, so as to avoid the consequences of a computer disaster. Such copies, however, are a true mine to find the "smoking gun" when litigation arises.

Both the definition of electronic document and the importance of metadata have been accounted for in the amendments to Rule 34 of the FRCP. The Rule now includes in the broad definition of *electronically stored information* any "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations",[55] whatever the medium used to store it. With reference to the forms of production of electronic material, the Rule now states "[i]f a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms". This ensures that the information given by one party to the other has not been rendered useless in practice[56] or that, translated in a different format, has lost the valuable additional information hidden in its metadata.

Communications and Privacy

The digital revolution and the inexorable invasion of personal computers deeply affected the way social relations are lived, moving a large part of interpersonal communication from oral to written. Not only thousands of emails are sent every day,[57] but the dialogue continues on blogs, chats, Facebook, Twitter and many other forms of written communication. Each of these communications leaves a distinctive footprint in the digital air describing its date, hour, sender and recipient. Quite often, the very content of the communication is also recorded, regardless of whether the author is aware of it or not.

The consequence of this sociological change is that a large number of conversations that previously were left to the phone or to informal water-cooler chat (*verba volant*) are now stored on digital devices, hard to erase and soon copied in back-up tapes (*scripta manent*).[58] Once again this mass of information is an invaluable resource for someone looking for the decisive piece of evidence that will bring to a rich settlement or a favourable jury verdict.[59] A clear example is the mail in which one of Zubulake's bosses, after filing her complaint with the EEOC, suggested to "fire her ASAP".[60] This is a typical conversation that both its authors and the company would have never wanted to see engraved in the digital memory of the employees' computers and copied in durable backup tapes.

Companies, thus, clearly wish to limit the chances that employees use their emails in an improper manner. One soft way of achieving this goal has been through a number of codes of conduct instructing employees on internet and company mail etiquette. A more subtle measure, and one that has been quite widely adopted in the US, is the use of "spy" software that monitors how emails and computers are used by the employees, and even records their content.[61] While some American scholars have already questioned this measure,[62] European companies would likely encounter obstacles when trying to use these systems in countries that traditionally give much more protection to employees' rights, including to the protection of their privacy.[63]

The real point of friction between e-discovery and privacy, however, relates more broadly to the duty to preserve and produce evidence because of different conceptions between Europe and America on the protection of personal data.[64] Across the ocean, the protection of personal data is mostly sector-based[65] and each company is generally considered the owner of the data it possesses.[66] Usually there are no specific rules on data processing and no judicial protection for the subject to which data refers.

The same does not hold true within the European Union where the protection is *omnibus* and personal data is usually owned by the person to which it refers, whose consent is required for data processing and who also has the right to request the correction or elimination of such data and is afforded judicial and regulatory protection.[67] It is not by chance that Article 1 of the Directive 46/95/

EC on the protection of personal data states that "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data",[68] echoed by the Charter of Fundamental Rights of the European Union that raises the protection of personal data to the status of a fundamental right.[69]

The Directive further states in its LVII *considerando* that "the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited". This is further specified in Article 25 of the Directive instructing Member States to take measures "necessary to prevent any transfer of data of the same type to the third country in question", although the following Article provides for a derogation when "the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims".

In order to determine which countries offer an adequate level of protection of personal data, meaning that data can flow from the EU to that State without any problem or additional requirement, the Directive set up a certification mechanism that ends with a Commission decision qualifying the foreign State as "adequate". So far only few States have applied and acquired such statute: Argentina, Australia, Canada, Israel, New Zealand, Switzerland and Uruguay.[70] The United States is not accorded such status, with the notable exceptions of the US Department of Commerce's Safe Harbour Privacy Principles[71] developed in collaboration with the Commission to ensure protection and a correct transfer of personal data in commerce-related matters, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection.[72]

Thus, apart from these two areas, European regulators and judges do not seem ready to give up the protection of personal data in name of US e-discovery. At the same time, it is unlikely that such a framework could provide a sufficient justification for a European company to refuse complying with a request of production in a US courtroom or with the duty to preserve personal data relating to a particular dispute,[73] especially when the litigation involves an important American interest.[74] The clash between e-discovery and EU privacy exposes EU companies to conflicting obligations, thus representing a sort of legal mismatch.

Duty to Preserve and Produce

The heart of *Zubulake*, at least in its more dramatic aspects, turns around the duties of the litigants to preserve documents relating to a pending dispute and to produce them when requested by the other party. The case shows that breaching those duties may lead to serious procedural and economic sanctions. The matter is far too varied and complex for a complete analysis here and I shall only give some brief impression.

The first aspect is establishing the moment in which a duty to preserve arises. As it has been noted, this is when "the party has notice that the evidence is relevant to the litigation or when a party should have known that the evidence may be relevant to future litigation".[75] The interpretation of the duty given by American judges is therefore quite broad and characterised by partially subjective elements. For instance, in *Zubulake* Judge Scheindlin held that UBS reasonably foresaw a dispute because its employees started to exchange emails having UBS attorney-client privilege, notwithstanding that no lawyer was taking part in the conversation.[76] In any case, this duty comes out quite early in time.

The objective scope of this duty,[77] on the other hand, cannot be too broad either in general or in view of a specific litigation. Not only an order to "freeze" the state of the information as it is in a certain moment could prejudice and even stop the ordinary business of a company,[78] but the modification and elimination of digital data may sometimes be involuntary.[79] At the same time, when a dispute has arisen or is arising, the company has a duty to place a *litigation hold* on all relevant material and the normal data elimination and backup tapes' recycling operations should be suspended to avoid spoliation.[80] Both the subjective and objective scope of the duty to preserve, which no doubt are traditional issues, should be read against the background of the digital structure of companies, which should be aptly adapted in order to enable the company to easily comply without bringing the business to an halt.

The peculiarity of the duty to produce as applied to electronically stored information relates, instead, to the difficulty of recovering data that has been eliminated but is still recoverable or is contained in back-up tapes or in obsolete digital systems.81 Judge Scheindlin settled this issue in *Zubulake* by distinguishing two categories: accessible and inaccessible data. In the former, the Judge included *active/online data, near-line data* and *offline storage/ archives*,[82] namely data that is immediately or easily available and that, without any doubt, is supposed to be produced in every ordinary e-discovery.

Inaccessible data is, instead, that contained in *backup tapes*[83] or *erased, fragmented or damaged data*.[84] In relation to the latter category, the duty to produce, or at least the duty to bear the costs, is attenuated. Such distinction is also evoked by Rule 26(b)(2)(B) of the FRCP, in the 2006 amended version, which provides a twofold test:[85] the burdened party may avoid discovery showing that the requested information is not "reasonably accessible because of undue burden or cost".[86] On the other hand, the demanding party may still compel discovery of such information showing a good cause as the probable importance of the material to the case.

The array of sanctions that a US judge may inflict in case of violation of the duty to preserve and produce is particularly interesting. [87] The most serious breaches may be sanctioned with a default judgment or a dismissal of the action. This is the case, for instance, when the party acted with intent to eliminate key evidence.[88] In other cases, as in *Zubulake*, the sanction is instructing the jury on the possibility to draw an adverse or negative inference from the party's failure to preserve or produce digital information.[89] Finally, some judges simply punish the defaulting party by monetising their breach or ordering to pay the other party's legal fees.[90] Given the serious consequences of these sanctions, the Rules now provide a safe harbour that protects a party when data spoliation is due to the "routine, good-faith operation of an electronic information system".[91]

Costs

The last aspect of e-discovery to analyse relates to costs. The digital revolution not only increased the quantity of written communications to a level that was not even conceivable before, but also rendered it extremely cheap to store documents and other information in an electronic format. As a consequence, pre-trial discovery today can involve millions of pages and an enormous amount of data[92] that needs to be reviewed by expensive lawyers. Once again, this does not represent a revolution as scholars and practitioners already focused on time and cost factors of traditional discovery, for instance in relation to so-called *dump truck* techniques, when a party answers to the requests of the other literally burying her under boxes and boxes of non-relevant documents with the sole purpose of obstructing discovery.[93] The broader storing capacity offered by digital media simply emphasises this profile and takes it to a new level.

At the same time, digital files can be indexed, searched, manipulated and elaborated with data mining software,[94] allowing the receiving party to perform a first screening of the billion files produced by the other, in order to narrow down the number of potentially relevant documents and files to be reviewed by attorneys or paralegals,[95] thereby reducing overall costs.

The real digital innovation relates, instead, to the cost of recovering inaccessible data.[96] As *Zubulake* shows, recovering data from backup tapes may be expensive.[97] Even higher may be the cost of retrieving erased files. In order to limit costs, American judges, and Judge Scheindlin in particular, have developed two techniques. The first is ordering a sample of inaccessible data to evaluate the probable relevance of the recovered data to the litigation and to assess the cost of recovery.[98] The second involves shifting some or all of the costs associated with retrieving the data to the party requesting its production.[99] In this respect, *Zubulake* teaches that the cost of legal review of recovered data by the party's lawyers should not be shifted and that a cost shifting decision is not neutral, having the potential collateral effect of "chill[ing] the rights of litigants to pursue meritorious claims".[100]

Conclusion

In this article, I have attempted to sketch out some of the complexities and issues that the digital revolution has brought to the production of documents, and more specifically to US e-discovery. In some cases, as in defining "electronic document" or recovering inaccessible data, the problems presented and the solutions proposed are common to any document production technique, being it a *discovery*, *disclosure* or another instrument typical of European countries.

In others, instead, there is a clear conflict between the two shores of the Atlantic Ocean, especially in the European adherence to the principle of *nemo tenetur* and in the clash between the duties to preserve and produce and the protection of personal data. This is the background on which we should read the, surely imperfect, attempts of the European Union and the United States to find an arrangement in the matter of privacy and e-commerce,[101] or the novelty represented by the European "enforcement" directive on the protection of intellectual property rights.[102]

The differences, sometimes quite deep, that exist in the very procedural and substantive legal philosophies in Europe and in America should not prevent scholars and practitioners to look at the US experience as a valuable touchstone to find a European way to e-discovery.[103]

* Ph.D. University of Florence; LL.M. New York University; J.D. University of Florence. This article is based on a paper presented for the first time at a Seminar on E-Justice in the European Union held at the Universidad Complutense de Madrid on 11November 2011 within the project on "European Civil Procedure and e-Justice implementation within the European Union: a planning for its study and diffusion among legal practitioners", Action Grant JLS/2008/JCIV/AG/1008-30-CE-0306633/00-00, European Commission, 2010/2012 directed by Professor Andrés de la Oliva Santos. A revised and modified version was recently presented at the 2013 Society of Legal Scholars conference held in Edinburgh on 3-6 September 2013 and, later, at the "Law in a Changing Transnational World" Workshop held at the University of Tel-Aviv on 30-31 October 2013. I thank all participants to these encounters, and particularly Professor Michael Birnhack, for their useful comments, critiques and suggestions. Finally, I deeply thank Professor Vincenzo Varano for encouraging me toward e-discovery and Professor Nicolò Trocker for his mentoring. All errors and omissions are of course mine. Comments are most welcome at giacomo.pailli@unifi.it

1 With discovery we mean mainly pre-trial discovery of Rule 26(b) of the FRCP, according to which not only the amount of discoverable material is very large, but also material that is not admissible as evidence may be discovered if it could reasonably lead to find admissible evidence. See N Trocker, "Transnational Litigation, Access to Evidence and U.S. Discovery: Learning from American 'Exceptionalism'?" in R Stürner and M Kawano (eds.), Current Topics of International Litigation (2009), p.145.

2 See O Chase, "American 'Exceptionalism' and Comparative Procedure, (2002) 50 Am. J. Comp. L., 277, esp. 292-296 on discovery. According to G Hazard, "Discovery and the Role of the Judge in Civil Law Jurisdictions" (1997-1998) 73 Notre Dame L. Rev., 1017, 1018: "[t]his system of pre-trial discovery is unique to the United States. Other common law countries have nothing like it". See, also id., "From Whom No Secrets Are Hid" 76 *Texas L. Rev*. 1665, 675-82.

3 Starting from *Societé Nationale Industrielle Aérospatiale v. U.S. Dist. Court*, 482 U.S. 522 (1987) to *Columbia Pictures, Inc. v. Bunnell*, 245 F.D.R. 443 (C.D. Cal 2007), via *Strauss v. Credit Lyonnais*, S.A., 242 F.R.D. 199 (E.D.N.Y. 2007). On Aerospatiale and the Hague Convention, see N. Trocker, *Transnational Litigation, Access to Evidence and U.S. Discovery*, cit. *supra* note 1, 164-172. In general on the deep differences between the United States and civil law country in relation to discovery and the role of legal actors (both attorneys and judges), see G. Hazard, *Discovery and the Role of the Judge in Civil Law Jurisdictions*, cit. *supra* note 2, *passim*. *Blocking statute* may not be enough to excuse the foreign party, as witnessed by *In re Global Power Equipment Group, Inc.*, No. 06-11045, 2009 WL 3464212 (Bankr. D. Del. Oct. 28, 2009), where the Judge ordered discovery even after the French *Cour de Cassation* made its first use of a criminal blocking statute, fining a lawyer who participated to a U.S. discovery on the French soil, *In re Advocat Christopher* X, Cour de Cassation, Chambre Criminelle, Paris, Dec. 12, 2007, No. 07-83228.

4 R Marcus, "E-discovery Beyond the Federal Rules" (2008) 37 *Baltimore L. Rev*. 321, 339-40; S Berman, "Cross-border Challenges for e-Discovery" (May 2010) 11 *Business Law Int'l* 123, 128-29.

5 Another reason of practical interest may be the rule codified at 28 U.S.C. § 1782 that allow parties to seek US discovery "in assistance to foreign and international tribunals and to litigants before such tribunals". See N Trocker, "Transnational Litigation, Access to Evidence and U.S. Discovery", cit. *supra* n1, 182-185, and Id., "U.S.-Style Discovery for Non-U.S. Proceedings: Judicial Assistance or Judicial Interference?" (2011)1 *Int'l J. Proc. L*. 299.

6 N Trocker and V Varano, "Concluding Remarks" in N Trocker and V Varano (eds.), The Reform of *Civil Procedure in Comparative Perspective* (2005), 255-58.

7 See H Muir Watt, "Brussels I and Aggregate Litigation or the Case for Redesigning the Common Judicial Area in Order to Respond to Changing Dynamics, Functions and Structures in Contemporary Adjudication and Litigation" (2010) *IPRax*, 11; R Nagareda,, "Aggregate Litigation Across the Atlantic and the Future of American Exceptionalism" (2009) 62 *Vand. L. Rev.*, 1.

8 In the field of competition law, see S Burbank, S Farhang and H. Kritzer, "*Private Enforcement of Statutory and Administrative Law in the United States*" (2011) Int'l Lis, 3-4, 153 ss. See, also, H Buxham, "The Private Attorney General in a Global Age: Public Interest in Private International Antitrust Litigation" (2001) 26 Y. L. J., 222-ss and critics in W Wills, "Should Private Antitrust Enforcement Be Encouraged in Europe?" (2003)26(3) *World Competition* 473, 9-14. On punitive damages in general, D Makel, "How Should Punitive Damages Work?" (2009) 157 *U. Pa. L. Rev*. 1383.

9 See G Hazard, "From Whom No Secrets Are Hid", cit. supra n2, pp.1671-72. Another feature of this non-exclusive list is *contingency fee agreement* that facilitates plaintiffs in bringing their claims.

10 See for example, F. Easterbrook, "Discovery as Abuse" (1989) 69 B.U. L. Rev. 635; E. Dudley, "Discovery Abuse Revisited: Some Specific Proposals to Amend the Federal Rules of Civil Procedure" (1991-1992) 26 *U.S.F. L. Rev*. 189; C. Yablon, "Stupid Lawyer Tricks: An Essay on Discovery Abuse" (1996) 96 *Col. L. Rev*. 1618 Contra, L. Mullenix, "Discovery in Disarray: The Pervasive Myth of Pervasive Discovery Abuse and the Consequences for Unfounded Rulemaking" (1993-1994) 46 *Stan. L. Rev*. 1393.

11 Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights (OJEU L. 157 of 30 April 2004).

12 CPR 31 *Disclosure and Inspection of Documents* e CPR 25(1)(h) allowing the judge to issue a search order (formerly *Anton Piller* order). On the deep difference between U.S. *discovery* and English *disclosure*, see G. Hazard, "From Whom No Secrets Are Hid", cit. *supra* n2, pp. 1677-82.

13 Art. 10 of the French Civil Code. In Germany and Italy there are some provisions allowing the judge to order production of documents by the parties or third parties, but usually with no meaningful sanction. See § 142 ZPO or art. 210 Italian *Codice di procedura civile*. See B. Ficcarelli, *Esibizione de Documenti E Discovery*, (Torino, 2004), 253 ss.

14 R. Marcus, "E-discovery & Beyond: Toward Brave New World" (1984) 25 *Rev. Litigation*, 644. For a comparative analysis, see O. Chase and H. Hershkoff (eds.), *Civil Litigation in Comparative Context*, (2007), 207-240.

15 J. Carroll, "Developments in the Law of Electronic Discovery" (2003) 27 Am. J. Trial Advoc., 359-60; see, also, B. Shariati, "*Zubulake v UBS Warburg*: Evidence that the Federal Rules of Civil Procedure Provide the Means for Determining Cost Allocation in Electronic Discovery Disputes? (2004) 49 *Villanova L. Rev*. 392, 397-407 for some elements differentiating paper and electronic discovery.

16 R. Marcus, "E-discovery & Beyond", cit. *supra* n14, pp. 634-35 and 660-61, states: "[a]lthough the possibilities of [e-discovery] might seem … momentous, the outcome of a fairly comprehensive effort to grapple with its problems is hardly revolutionary. … Although [the impact of digital technology on litigation] could be very dramatic, to date it has not and there are reasons to think that in the future it will not. To the contrary, at least with regards to our method of trying cases, there seem to be important reasons for being skeptical about the ways in which digital technology could transform litigation". See, also, ID., "Only Yesterday: Reflections on Rulemaking Responses to E-discovery" (2004) 73 *Fordham L. Rev*. 1, pp. 1-9, presenting the steps of historical evolution of discovery rules and practice under the pressure of technological developments, from the invention of the photocopying machine to the digitalization of all communications. See also J. Carroll, "Developments in the Law of Electronic Discovery", cit. *supra* n15, pp. 360-366: see, also, J. Baron, "Law in the Age of Exabytes: Some Further Thoughts on 'Information Inflation' and Current Issues in E-Discovery Search" (2011) 17 *Rich. J. L. & Tech*. 9, 13. Other scholars disagree, stressing the uniqueness of e-discovery, M. Redish, "Electronic Discovery and the Litigation Matrix" (2001) 51 *Duke L. J*. 561, pp. 583-591; M. Yager, "E-Discovery as Quantum Law: Clash of Cultures—What the Future Portends", (2013) 19 *Rich. J. L. & Tech*. 10 comparing, and perhaps exaggerating a little bit, the change that e-discovery brought to civil procedure to quantum physics, based on the steeply increasing number of e-discovery sanction cases.

17 See S. Subrin, "Fishing Expeditions Allowed: The Historical Background of the 1938 Federal Discovery Rules" (1998) 39 B.C.L. Rev. 691.

18 Revenues of this industry are growing at a very fast rate from $40 million in 1999 to $2,8 billion in 2007 and roughly $4 billion in 2009. R. Marcus, "E-discovery & Beyond", cit. supra n14, p.645; Id., "E-discovery Beyond the Federal Rules" 37 *Baltimore L. Rev*. 621, 326-28. An interesting view on the emergence of new professions in the field of e-discovery can be read in J. Markoff, "Smarter than You Think: Armies of Expensive Lawyers, Replaced by Cheaper Software", *The New York Times, 4 March 2011*. Available

at http://www.nytimes.com/2011/03/05/science/05legal.html (last visited August 8, 2013). In a certain way, the relationship between the attorney and the IT professional changes too, as the former, too often not very well-equipped in terms of technical knowledge, tends to depend on the latter.

19 See R. Marcus, "E-discovery & Beyond", cit. *supra* n14, pp. 647-59; B. Tennis, "Cost Shifting in Electronic Discovery" (2010) 119 *Yale L. J.*,1115-16.

20 A clear example is the *Zubulake* case, on which see *infra* para. 3. See, also, B. Tennis, "Cost Shifting in Electronic Discovery", cit. *supra* n19, pp. 1116-18. R. Marcus, "E-discovery & Beyond", cit. *supra* no14, pp. 641-42 reports that Texas legislation dealt with e-discovery already in 1996, with a provision that has in part inspired the 2006 amendments to Rule 26.

21 Rule 34(a).

22 Rule 34(2).

23 Rule 26(b)(2)(B).

24 Rule 26(f)(3).

25 Rule 37(e).

26 The *Zubulake* litigation is composed of five decision, four of which are relevant to our analysis: *Zubulake I*, 217 F.R.D. 309 (S.D.N.Y. May 13, 2003) (where the Judge develops a new test on cost shifting), *Zubulake III*, 216 F.R.D. 280 (S.D.N.Y. Jul 24, 2003) (shifting a portion of recovery costs from UBS to Zubulake); *Zubulake IV*, 220 F.R.D. 212 (S.D.N.Y. 2003) (sanctioning UBS partial violation of its duties to preserve and produce the information stored on backup tapes) and *Zubulake V*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (sanctioning the serious violation of UBS and instructing the jury on the possibility to draw an adverse inference from UBS behaviour). See J. Evangelista, "Polishing the 'Gold Standard' on the E-discovery Cost-Shifting Analysis: *Zubulake v. UBS Warburg, LLC*", (2004) 9 *J. of Techn. & Pol.*, 5-6 e 12-14. Laura Zubulake even wrote a book on her history, titled *Zubulake's e-Discovery: The Untold Story of my Quest for Justice*.

27 As Judge Scheindlin states: "[t]his case provides a textbook example of the difficulty of balancing the competing needs of broad discovery and manageable costs". *Zubulake I*, 217 F.D.R. p. 311.

28 *Zubulake I,* 217 F.R.D. p. 312fn9.

29 *Zubulake I*, 217 F.D.R. p. 312.

30 Ibid.

31 *Zubulake I*, 217 F.D.R. p. 313.

32 As a confirmation of this suspicion, in the 450 pages that Zubulake had produced there were several emails sent from the five accounts that were not included in UBS document production. *Zubulake I*, 217 F.D.R. p. 313.

33 As Judge Scheindlin describes in *Zubulake I*, 217 F.D.R., pp. 313-315, there were two backup systems for emails: one on tapes and the other on optical disks. The first performed three types of backups (daily, weekly and monthly) on all UBS employees. These backups were kept for different periods, daily backups for twenty days, weekly backups for a year and the monthly backup for three years. After the period expired the tapes were recycled. The second system based on optical disks was reserved to "registered traders" only, to which four out of the five accounts indicated by Zubulake belonged. According to this system, all emails received and sent by these accounts were immediately recorded on optical disks, without any expiration date of the disks that were never recycled.

34 *Zubulake I*, 217 F.D.R. p.312fn8.

35 It should be noted that cost shifting is not purely an economical exercise, especially when the dispute sees individual against large corporations: imposing costs on the plaintiff during discovery may make it impossible for her to proceed with the request and translate in an obstacle to the protection of her rights. See Judge Scheindlin in *Zubulake I*, 217 F.R.D. p. 317: "Courts must remember that cost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations. As large companies increasingly move to entirely paper-free environments, the frequent use of cost-shifting will have the effect of crippling discovery in discrimination and retaliation cases. This will both undermine the strong public policy favouring resolving disputes on their merits, and may ultimately deter the filing of potentially meritorious claims" (citations omitted). According to F. EASTERBROOK, *Discovery as Abuse, cit. supra* note 10, p. 646, however: "Those of modest means rarely participate in the kind of cases in which there is voluminous discovery", nor could Laura Zubulake be pictured as destitute.

36 The test is partially modelled on a line of decisions represented by *Rowe Entertainment, Inc v. William Morris Agency,* 205 F.R.D. 421 (S.D.N.Y. 2002). See also J. Evangelista, "Polishing the "Gold Standard", cit. *supra* n26, pp. 3-5.

37 *Id est*, allowing the discovery requested by the plaintiff without imposing on the other party unreasonable costs that, according to U.S. procedural principles, stay with the party that bore them including in case it wins the case. J. Maxeiner, "The American 'Rule': Assuring the Lion His Share" in Reimann (ed.), Cost and Fee Allocation in Civil Procedure: A Comparative Study, (Springer Publisher: Ius Gentium Series, 2011), available on http://ssrn.com/abstract=1806042 (last visited 14 August 2013), p. 6, notes that this rule, another element of the *American exceptionalism,* is more a custom than a legal rule.

38 In addition to all accessible material, such as the emails stored on the optical disks mentioned *supra* note 33. See also *infra* para. 6.

39 *Zubulake III*, 216 F.D.R. p. 283.

40 Ibid.

41 *Zubulake III*, 216 F.D.R. pp. 289-91.

42 And that some relevant emails sent after Zubulake filed her lawsuit had been erased from UBS employees' computers and are now stored only in the backup tapes, rendering their production much more complex and expensive.

43 See, e.g., *Silvestri v. GMC*, 271 F.3d 583, 591 (4th Cir. 2001) "The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation".

44 *Zubulake IV*, 220 F.D.R. p. 215. This, moreover, violated the company policy of maintaining monthly backup tapes for three years.

45 The role and importance of lawyers, and of in-house counsels in particular, in the field of e-discovery should not be underestimated. These are, indeed, characters that should develop suited plans for preserving documents as well as place "litigation hold" to avoid spoliation and loss of data and consequent sanctions. See J. Evangelista, "Polishing the "Gold Standard", cit. *supra* n26, pp. 2-3.

46 E. Porter, "UBS Ordered to Pay $ 29 Million in Sex Bias Lawsuit", *The New York Times*, 7 April 2005. Available at http://www.nytimes.com/2005/04/07/business/07bias.html (last visited 15 August 2013). It is not entirely clear whether the instruction given by Judge Scheindlin to the jury were decisive in the outcome of the case, although UBS overall behaviour probably acquired relevance at least in the determination of punitive damages. See S. Nelson, "Exit Her ASAP!" Dinner with Laura Zubulake". Available at http://ridethelightning.senseient.com/2008/08/exit-her-asap-d.html (last visited 15 August 2013).

47 For a series of definitions see S. Scheidlin and J. Rabkin, "Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up To the Task?", (1999-2000) 41 B.C. L. Rev. 327, pp.331-41.

48 R. Marcus, "E-Discovery & Beyond", cit. supra n14, 649; R. Marcus, "Only Yesterday", cit. *supra* n16, pp.12-13.

49 R. Marcus, "Only Yesterday", cit. *supra* n16, p.11, footnote.

50 R. Marcus, "E-discovery Beyond the Federal Rules", cit. *supra* n4, p.333: "Thus one can prove that the wandering husband was actually in Marin County with his squeeze rather than being (as he claimed to his wife) hard at work at the office in the city".

51 In a workplace harassment case, *Smith v. Café Asia,* 246 F.D.R. 19 (D.D.C. 2007), the Judge, upon request by the defendant, ordered the plaintiff to produce certain pictures stored on her mobile phone.

52 For an in-depth analysis of metadata, see S. Bennet and J. Cloud, "Coping with Metadata: Ten Key Steps" (2010) 61 *Mercer L. R.* 471; P. Favro, "A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata" (2007) 13 B.U. J. Sci. & Tech. L. 1. As R. Marcus, "E-Discovery & Beyond", cit. *supra* n14, pp.650-51, specifies, in the case of e-discovery the form of production of digital data may be of the utmost importance, to avoid losing valuable information. Metadata also guides data mining software in performing its activity of retrieving electronically stored information

which is relevant to the litigation, giving it information on the context rather than on the content of data itself.

53 Bennet, "Two Views from the Data Mountain", (2003) 36 *Creighton L. Rev.* 607, 612-15.

54 As Judge Rosenthal puts it, however, "Electronic information is simultaneously permanent (deletion does not mean delete, although it is progressively more and more difficult to get to) and fragile, because if steps are not taken to freeze information it will change. The information on your computer changes every time you turn it on". L. Rosenthal, District Court Judge, United States District Court for the Southern District of Texas, Remarks at the Philip D. Reed Lecture Series, 76 *Fordham L. Rev.* 1, 5 (Oct. 2007), cited by R. Alexander, "E-discovery Practice, Theory, and Precedent: Finding the Right Pond, Lure, and Lines Without Going on a Fishing Expedition" (2011) 56 S.D. L. Rev. 25, 35.

55 See R. Marcus, "E-Discovery & Beyond", cit. *supra* n14, p.649.

56 For instance removing databases indexing and, thus, producing a bulk of row and hard to read data.

57 As example, *Zubulake I* reports that each seller of UBS Asian Desk received an average of 200 emails every day. *Zubulake I*, 217 F.D.R. at p. 314.

58 J. Evangelista, "Polishing the "Gold Standard", cit. *supra* n26, p.2: "As you probably also know, e-mail has nearly replaced the casual phone call and individuals frequently put in writing what should never be spoken. Chances are that such comments and other potentially useful evidence exist on a back-up tape in the defendant's e-mail archive, *even if all other copies have been "deleted" by the author and recipients"* (emphasis in the original). See also R. Marcus, "Only Yesterday", cit. *supra* n16, p.15.

59 A famous case in which emails played an important part is the antitrust litigation between the U.S. Government against Microsoft in 1998, where the statement of Bill Gates, founder and then-CEO of Microsoft, of not being aware of certain facts was contested word-by-word by the superstar lawyer David Boies by producing Gates' own emails. L. Orland, "Teaching Antitrust During Microsoft" (1998-99) 31 Conn. L. Rev. 1375, 1376-77. Another famous case is the sanction against Arthur Andersen for obstruction to justice based on one email sent by Nancy Temple, Arthur Andersen in-house counsel, suggesting to destroy legal documents relating to the Enron affaire. While such sanction was later set aside by the Supreme Court, this did not save the company that already ceased to exist. E. Ainslie, "Indicting Corporations Revisited: Lessons of the Arthur Andersen Prosecution" (2006) 43 Am. Crim. L. Rev. 107, 107ff. See R. Marcus, "E-discovery & Beyond", cit. supra n14, p.646: "[n]owadays one follows the e-mails, not the money". The same R. Marcus in "E-discovery Beyond the Federal Rules" (2008) 37 Baltimore L. Rev. 321, 323-26 describes all changes that "Corporate America" tried to put in play in the emails area to reply to the risks related to e-discovery, and the effects that this has on the law firms that assist and defend such corporations. See also Redish, "Electronic Discovery and the Litigation Matrix", cit. supra n16, pp. 587-88.

60 *Supra* n33.

61 As R. Marcus, 'E-discovery & Beyond", cit. *supra* n14, pp. 643-44, reports in the United States several courts have declared that employers' spying systems monitoring employees' email accounts do not violate employees' privacy rights. *Fraser v. Nationwide Mut. Ins.* Co., 352 F.3d 107, 114 (3d Cir. 2003). According to studies cited by Marcus, 74% of U.S. companies monitor employees Internet use and 72% spy their emails. K. Livingstone, "Battle over Big Brother", *S.F. Recorder*, 30 August 2001, p.1.

62 For instance E. Kim, "The New Electronic Discovery Rules" (2011) 115 *Yale L. J.* 1481,p. 1485-86, who, however, notes that the Electronic Communications Privacy Act and several State laws allow an employer to monitor employees digital activities when they use company's properties and there is a plausible economic justification for doing so, such as increasing productivity. R. Marcus, "Confronting the Future: Coping with Discovery of Electronic Material" (2001) 64 *Law and Contemporary Problems* 253, 262, reports the opposition of the National Labor Relations Board about spying the emails of unionised employees.

63 S. Berman, "Cross-border Challenges for e-Discovery", cit. *supra* note 4, p. 128. In Italy such practice would be prohibited under art. 4 of the law of 27 May 1970, no. 300 (the Workers' Statute). A recent decision by the French *Cour de Cassation* however, while confirming the principle of secrecy of employees personal mail and documents, apparently limited its scope. The court, in fact, stated that all documents created by an employee using company devices are presumed to be of professional nature and are, therefore, always accessible by the employer, including when the employee is absent. Only when the employee marks its personal nature, the principle of privacy comes into play. Cour de Cassation, Chambre Social, ârret du 15 Dec. 2009, No. 07-44264, *Bruno B. vs. Giraud et Migot*.

64 According to the Directive, personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". Art. 2(a), Directive 95/46/EC. Sensitive data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" are further protected by art. 8 of the Directive. This data cannot be processed unless a derogation applies such as consent, vital interests data subject or another person, data manifestly made public or legal claims.

65 G. Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards" (2000) 25 *Y. Int'l L. J.*,1, pp. 24-28.

66 G. Shaffer, Id., p. 2, states "[m]uch of the compilation and transfer of personal information that is a daily occurrence in the United States is illegal in Europe". In general an American company can make use of the personal data it acquires without requiring the consent of the subject to which it refers to, sell this data to third parties and is not under an obligation of correcting or deleting the data upon request by the interested party. Ivi, p. 26.

67 S. Berman, "Cross-border Challenges for e-Discovery", cit. *supra* n4, p.125. The Tribunale di Roma, in a decision dated 17 March 2008, in *Guida al diritto* 2008, 41, 67 with reference to the "enforcement" directive stated that: "the discovery order, even if allowed by the Legislative Decree 140/2006 implementing the Enforcement Directive, cannot be issued when there is a reasonable risk of violating the privacy right of Internet users".

68 Directive 95/46/EC of 24 October 1995 (OJEC, 23/11/1995, L 281, p. 31). See also Directive 2002/58/EC of 12 July 2002 (OJEC, 31/07/02, L 201, p. 37) and the remarks in S. Berman, "Cross-border Challenges for e-Discovery", cit. *supra* n4, pp. 125-27. The Directive has been variously implemented at the national level. For instance in Italy with Legislative Decree of 30 June 2003, no. 196.

69 Art. 8: "Protection of personal data. 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority". See also art. 7 and of the Charter and art. 8 of the European Convention on Human Rights, signed in Rome on 4 November 1950. G. Shaffer, "Globalization and Social Protection", cit. *supra* n65, pp.10-11, citing the *considerando* to the Directive 95/46/EC, connects the importance that the European legislator gives to the protection of personal data to the correct and fair functioning of the internal market.

70 The list also includes Andorra, Faeroe Islands, Guernsey, Isle of Man, Jersey.

71 2000/520/EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

72 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) signed in Brussels, 23 July 2007 and in Washington, 26 July 2007. The agreement is strongly grounded in the need to share PNR data to "prevent and combat terrorism and transnational crime effectively as a means of protecting their respective democratic societies and common values". See, on the same line, Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (2010/412/EU).

73 R. Marcus, "E-discovery Beyond the Federal Rules", cit. *supra* n4, p.340 reports at least one case in which the Court refused to justify a party from its failure to produce based on the need to comply with European laws. *Columbia Pictures, Inc. v. Bunnell*, 245 F.D.R. 443 (C.D. Cal 2007). In a more recent case, the Judge ordered production of documents notwithstanding the Malaysian bank secrecy laws, see *Gucci America, Inc. v. Curveal Fashion*, 2010 WL 808639 (S.D.N.Y. Mar. 8, 2010). See, also, *Gucci Am., Inc. v. Weixing Li*, 2011 U.S. Dist. LEXIS 97814 (S.D.N.Y. Aug. 23, 2011) (bank secrecy laws are entitled to less deference when their protections amount to simply a privilege that can be waived by the customer). In *In re Vitamins Antitrust Litigation*, No. 99-197, 2001 U.S. Dist. LEXIS 8904 (D.D.C. June 20, 2001) the Judge held that when the requested information is "so relevant and necessary to the plaintiffs' case", discovery requests can overcome foreign legal barriers but the court must "seriously consider the sovereign interests implicated". See also *supra* n3 for the relative inefficiency of European blocking statutes. See, also, *Liberty Media Corp. v. Vivendi Universal S.A.* (In re Vivendi Universal, S.A.), 618 F. Supp. 2d 335 (S.D.N.Y. 2009) ("there is little doubt that the United States has a strong interest in enforcing its securities laws and ensuring the compliance of its citizens with the Federal Rules of Civil Procedure").

74 Such as the enforcement of tax or antitrust laws. It is the fifth factor of § 437 of he Restatement of Foreign Relations Law of the United States (Third) of 1987 also cited (in its previous version) in *Aérospatiale,* 482 U.S. 522, *supra* n3. See, e.g., *United States v. Vetco, Inc.*, 691 F.2d 1281, 1287 (9th Cir. 1981); *United States v. Field*, 532 F.2d 404, 407 (5th Cir. 1976); *United States v. First Nat'l City Bank*, 396 F.2d 897, 903 (2d Cir. 1968); *Alfadda v. Fenn*, 149 F.R.D. 28, 33 (S.D.N.Y. 1993); *SEC v. Banca Della Svizzera Italiana*, 92 F.R.D. 111, 119 (S.D.N.Y. 1981).

75 *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 175 (S.D.N.Y. 2004); see also *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001), and *supra,* note 43. This is a definition that pertains to discovery in general. V. J. Carroll, "Developments in the Law of Electronic Discovery", cit. *supra* n15, pp. 369-375.

76 *Zubulake IV*, 220 F.D.R. pp. 216-17.

77 T. Allman, "The Case for a Preservation Safe Harbor in Requests for E-Discovery" (2003) 70 *Def. Counsel. J.* 417, p. 419, notes that even after *Zubulake* there are still doubts on the objective scope of the duty to preserve.

78 R. Marcus, "Only Yesterday", cit. *supra* n16, p.13 e *Zubulake IV*, 220 F.D.R. p.217.

79 R. Marcus, "E-Discovery & Beyond", cit. *supra* n14, p.656, reports *Gates Rubber Co. v. Bando Chem. Indus.*, 167 F.D.R. 90, 111-12 (D. Colo. 1996) in which the computer expert of the party that had requested discovery permanently erased certain data loading his own software on the other party's computers, involuntarily overwriting certain files. See also R. Marcus, "Only Yesterday", cit. *supra* n16, p. 13, warning that even turning on the computer or opening a document may alter valuable information.

80 *Zubulake IV*, 220 F.D.R. p. 217. Similarly, from a subjective point of view, a litigation hold should include all documents and correspondence of all subjects that are in some way related to the dispute. Ibid. A.R. Miller and C. E. Tucker, "Electronic Discovery and the Adoption of Information Technology" (2012) *Journal of Law, Economics, and Organization* (2012), available on SSRN http://ssrn.com/abstract=1421244 (last visited 28 August 2013) made a statistical study on the use of electronic medical records (EMR) by hospitals, finding evidence that hospitals are one-third less likely to adopt EMRs if there are state rules that facilitate the use of electronic records in court.

81 R. Marcus, "Confronting the Future", cit. *supra* n62, pp.265-66.

82 The first type is represented by data stored on computer or active server (hard drives), the second by data stored in automated digital libraries and the third by optical or magnetic disks that were filed and that require manual retrieval. *Zubulake I*, 217 F.D.R. p.319.

83 As Judge Facciolla states, "The one judicial rationale that has emerged is that producing backup tapes is a cost of doing business in the computer age. But that assumes an alternative. It is impossible to walk ten feet into the office of a private business or government agency without seeing a network computer, which is on a server, which, in turn, is being backed up on tape (or some other media) on a daily, weekly, or monthly basis. What alternative is there? Quill pens?", in *Mc Peek v. Ashcroft*, 202 F.r.D. 31, 33 (D.D.C. 2001) (citation omitted), reported in R. Marcus, "Only Yesterday", cit. *supra* n16, p. 11.

84 *Zubulake I*, 217 F.D.R. p. 319. The difference between accessible and inaccessible data is not only in the time and cost required for accessing it, but more specifically in the need, in the latter, to recover and retrieve the data before being able to using it.

85 T. Allman, "The "Two-Tiered" Approach to E- Discovery: Has Rule 26(b)(2)(B) Fulfilled Its Promise?" (2008) 14 *Rich J.L. & Tech.* 7, 14-16.

86 Rule 26(b)(2)(B). Judge Scheindlin noted: "[i]n fact, whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format". *Zubulake I*, 217 F.R.D. p. 318.

87 Rule 37(e) FRCP. For an overview on the type and number of sanctions inflicted by American courts for failing to comply with the duties to preserve and produce, see S. Scheindlin and K. Wangkeo, "Electronic Discovery Sanction in the Twenty-First Century" (2004-2005) 11 *Mich. Telecomm. & Tech. L. Rev.* 71, pp.74-80; see also D. Willoughby et al., "Sanctions for E-Discovery Violations: By the Number" (2010) 60 *Duke L. J.* 789, reporting an increase in the number of sanctions, partially linked to the increased use of e-discovery, and a predominance of violations relating to the duty to preserve. Sanctions may hit plaintiffs too, see *Pension Committeee of the Univeristy of Montreal v. Banc of America Securities*, 210 U.S. Dist. LEXIS 4546 (S.D.N.Y., 15 January 2010).

88 D. Willoughby et al., "Sanctions for E-Discovery Violations", cit. *supra* n87, pp.805-11.

89 Id., pp. 811-14. Another example of serious sanctions, beyond *Zubulake, is Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005), where the judge punished Morgan Stanley and its lawyers' behaviour and failure to produce certain emails, instructing the jury on the possibility to draw an adverse inference and subsequent verdict of about $1.5 billion against Morgan Stanley. The decision was later overturned on appeal on other grounds, but the case is still a clear example of the risks of non complying with e-discovery related duties. *Morgan Stanley & Co., Inc. v. Coleman (Parent) Holdings, Inc.*, No. 4D05-2606 (Fla. Dist. Ct. App. Mar. 21, 2007). S. Berman, "Cross-border Challenges for e-Discovery", cit. *supra* n4, p.124, notes: "[l]uckily for Morgan Stanley, the judgment was ultimately overturned for other reasons, but the lesson is still very clear: a party that fails in its preservation and disclosure obligation does so at its peril". Other Morgan Stanley misfortunes with emails are told in REUTERS, "Wall St. Firm Settles Case on Handling of E-Mail", *The New York Times*, 28 September 2007, available at http://www.nytimes.com/2007/09/28/business/28morgan.html (last visited 15 August 2013).

90 D. Willoughby et al., "Sanctions for E-Discovery Violations", cit. *supra* n87, pp.814-15. The AA. further report an increase of sanctions for lawyers. Id., pp. 815-823.

91 Rule 37(e) FRCP. See S. Scheindlin and K. Wangkeo, "Electronic Discovery Sanction in the Twenty-First Century", cit. *supra* n87, pp.94-95; T. Allman, "The Case for a Preservation Safe Harbor", cit. *supra n77, passim*.

92 R. Marcus, "Only Yesterday", cit. *supra* n16, p. 12, reports figures that allow one to understand the scope of the digital revolution. On one side it is estimated that a dispute presenting a certain degree of complexity between two corporations may involve production of more than a hundred million of pages, equal to about thirty man-years of review for each side. On the other it is reported the equivalence between digital devices and written documents, according to which a 1.44 MB floppy disk is equivalent to 720 typed pages, a 650 MB CD to 325.000 pages and a Terabyte (one trillion Bytes) to approximately 500 billion typed pages. It is the Terabyte that represents the appropriate measurement unit to calculate the backup volume produced by modern corporations. See, also, the interesting figures and cases cited in J. Baron, "Law in the Age of Exabytes", cit. *supra* n16, pp. 19 ff.

93 F. Hare and J. Gilbert, "Discovery in Product Liability Cases: The Plaintiff's Plea for Judicial Understanding" (1988-89) 12 *Am. J. Trial Advoc.* 413, pp.425-26. See also R. Marcus, "Retooling American Discovery for the Twenty-First Century: Toward a New World Order" (1999) 7 *Tul. J. Int'l & Comp. L.* 168, pp. 166 e 177.

94 From the easy and freely downloadable "Google Desktop" to more sector-specific software.

95 On this point see The New York Times article, J. Markoff, "Smarter than You Think", cit. *supra* n16.

96 J. Evangelista, "Polishing the "Gold Standard"", cit. *supra* n26, pp. 8-9. In addition to the issue of forms of production mentioned *supra* n52.

97 It should also be noted, however, that the total cost of recovering all backup tapes ($165,000) represented only a minimal ratio, about 0.5%, of the sum awarded by the jury to Laura Zubulake ($29 million). *Zubulake III*, 216 F.R.D. p. 283; E. Porter, "UBS Ordered to Pay $ 29 Million in Sex Bias Lawsuit", cit. *supra* n46.

98 T. Allman, "The Case for Preservation Safe Harbor", cit. *supra* n77, p.418, cites as a pioneer decision in the choice of sampling documents to evaluate the opportunity for discovery *McPeek v. Ashcroft*, 202 F.D.R. 31, 34-35 (D.D.C. 2001)

99 B. Tennis, "Cost Shifting in Electronic Discovery", cit. supra n19, pp.1013-1121.

100 *Zubulake III* 216 F.R.D. p. 289. T. Allman, "The "Two-Tiered" Approach to E- Discovery", cit. *supra* n85, pp. 26-28. The State of Texas follows a different approach, characterized by an increased automaticity. See Rule 196.4 of Texas Rules of Civil Procedure: "Electronic or Magnetic Data. To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot - through reasonable efforts - retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information". See the critique in T. Allman, "The Case for a Preservation Safe Harbor", cit. *supra* n77, p. 417.

101 See the complex negotiation of the Safe Harbor Arrangement between USA and UE for the protection of personal data in e-commerce, described by H. Farrel, "Constructing the International Foundations of E-Commerce – The EU-U.S. Safe Harbor Arrangement" (2003) 57 *International Organization* 277. See in general G. Shaffer, "Globalization and Social Protection", cit. *supra* n65, *passim*.

102 On the relationship between the new Enforcement Directive 2004/48/EC, and the protection of personal data, see the decision of the ECJ (Grand Chamber) in the case C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, of 13 June 2006 where the court stated that the Enforcement Directive: "do[es] not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings".

103 For further thoughts on e-discovery see, i.a., S. Scheindlin and J. Redgrave, "Special Masters and E-Discovery: The Intersection of Two Recent Revisions to the Federal Rules of Civil Procedure" (2008-200930 *Cardozo L. Rev. 347*, in which the AA. discuss the possibility of entrust the management of e-discovery to special master pursuant to Rule 53 FRCP in order to render the entire phase more efficient and to assist the judge who may lack specific knowledge in the field. An attempt to limit e-discovery in patent disputes is reported in S. Qualters, "Federal Circuit Chief Judge Announces Model Order to Limit e-discovery" *Nat'l L.J.*, 27 September 2011. See also the important work performed by the *Sedona Conference*, www.thesedonaconference.org.