BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Document Retention

EU Data Protection

Between a Rock and a Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements

FRED H. CATE AND MARGARET P. EISENHAUER

Fred H. Cate is a Distinguished Professor of Law, Adjunct Professor of Informatics, and Director of the Center for Applied Cybersecurity Research at Indiana University, and Senior Policy Advisor in the Center for Information Policy Leadership at Hunton & Williams LLP.

Margaret P. Eisenhauer is the founder of Privacy & Information Management Services-Margaret P. Eisenhauer, P.C. law firm, a Fellow of the Ponemon Institute, a Certified Information Privacy Professional (CIPP) and a member of the International Association of Privacy Professionals CIPP Advisory Board.

These materials have been prepared for informational purposes only and are not legal advice. Additionally, the views expressed herein are those of the authors personally, and do not necessarily reflect the views of their clients, employers or associates.

Companies in the United States are routinely required to retain and disclose internal records in the course of civil litigation. Among the most familiar of these requirements are the obligations to protect evidence relevant to pending or reasonably foreseeable litigation and to produce documents sought under a subpoena or court order.

For documents stored outside the United States, retention and production requirements often conflict directly with international data protection laws. As multinational companies link their affiliates on global networks and leverage consolidated data processing hubs, corporate documents are increasingly located in other countries. The implications for companies facing complex discovery in connection with U.S.-based litigation can be profound.

U.S. Document Production Requirements

Rule 34 of the U.S. Federal Rules of Civil Procedure governs the production of documents in civil litigation before the federal courts. Under Rule 34, companies have a legal duty to retain *all documents* that may be relevant to pending and reasonably foreseeable litiga-

 ISSN 1538-3423

tion. During the discovery process, companies are obligated to search and produce all relevant records.

The failure to preserve documents for the other party's use as evidence is spoliation. The corporate scandals involving Enron and Arthur Andersen both involved charges of spoliation. The consequences for spoliation may include adverse rulings in the litigation as well as criminal sanctions and independent tort claims.

Under Rule 34, the duty to preserve documents applies irrespective of the format in which they are maintained. The Rule was amended in 2006 expressly to state that the term ''documents'' includes all types of electronically stored information.[1] The amendment confirmed that ''discovery of electronically stored information stands on equal footing with discovery of paper documents'' and clarified that ''a Rule 34 request for production of 'documents' should be understood to encompass, and the response should include, electronically stored information.''[2]

Given the consequences of spoliation, U.S. companies are wisely focused on records management and preservation. Many companies have implemented systems that automatically scan all electronic records (including e-mails) and copy those records that may be relevant to possible future litigation. These systems are generally invisible to users, who may not realize that their documents are being scanned and copied for future document production purposes. Multinational companies using these systems must also consider the conflicts that exist between the Rules of Civil Procedure and international data protection laws.

European Data Protection Laws

European data protection laws codify the concept of privacy as a fundamental human right. In accordance with the European Union Data Protection Directive,[3] each member state has enacted a national data protection law governing the ''processing of personal data.''

The scope of the European data protection laws cannot be understated. ''Processing'' is broadly defined as ''any operation or set of operations,'' whether or not automated, including but not limited to ''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.''[4] ''Personal data'' are defined equally broadly as ''any information relating to an identified or identifiable natural person.''[5]

The general rule in Europe is that companies must collect only the personal data they need to fulfill a specific legitimate purpose, then use, disclose and retain the data only as needed for that purpose. The use of business records that reveal personal data (such as e-mails) in the course of litigation is a secondary use, which requires (at minimum) the consent of the data subject. But the mere retention of the records containing personal data in anticipation of a discovery request would itself violate this general rule.

European data protection laws guarantee individuals access to and the opportunity to correct and request deletion of information held about them. Data subjects are also entitled to object to the processing of their personal data, and they must be offered the opportunity to have their personal data erased before they are disclosed to third parties or used for secondary purposes. To enable individuals to understand how their data is used and exercise their rights, the laws require companies to provide detailed privacy notices.

European data protection laws also generally prohibit the transfer of personal data to countries outside of Europe that do not provide an adequate level of protection. As discussed below, the data transfer prohibition is subject to some exceptions. Unfortunately, these exceptions are interpreted very narrowly by the European regulatory community.

Finally, the data protection laws establish independent data protection authorities to supervise compliance efforts and hear data subject complaints. These authorities have the power to investigate data processing activities and to order the cessation of processing and the erasure of personal data. The authorities meet collectively as a group created by Article 29 of the Directive to issue guidance on the application of the Directive.[6]

Across Europe, the data protection authorities take their oversight roles very seriously. They routinely conduct investigations, bring enforcement actions, levy fines, and, in some cases, even seek criminal penalties for non-compliance with the data protection laws. Additionally, while the threat of large fines is daunting, companies also risk burdensome investigations and the possibility that their data transfers may be disrupted. This latter risk is very real; transfers of even innocuous employee data from Europe have been blocked as a result of legal violations. [7]

Processing of Personal Information for U.S. Litigation

While the restrictions on transborder data flows are the focal point of many U.S. company concerns about data protection law compliance, it is important to remember that these restrictions only come into play if the personal data have otherwise been lawfully processed within Europe. However, the mere retention and searching of records containing personal data of EU nationals (such as e-mails) for Rule 34 compliance purposes will likely violate EU data protection laws, even if the data never leave Europe.

Of all of the privacy interests implicated by the Rule 34 production requirements, perhaps the most complex are those of the employees, whose documents and e-mails are subject to retention and disclosure. As a preliminary matter, the data protection authorities regard virtually all data about employees as personal data, subject to the data protection laws.[8] Almost all business

[1] *Report of the Judicial Conference Committee on the Rules of Practice and Procedure* 71-72 (Sept. 2005)

[2] Id. at 72

[3] *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281)

[4] Id. art. 2(b)

[5] Id. art 2(a)

[6] This group is referred to as the Article 29 Working Party.

[7] See, *e.g.*, Jennifer L. Kraus, On the Regulation of Personal Data Flows in Europe and the United States, 1993 *Colum. Bus. L. Rev*. 59, 71 (1993)

[8] Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context*, Sept. 13, 2001 (5062/01/EN/Final WP 48)

  PVLR ISSN 1538-3423

records contain some personal information, such as the name of the individual that created the document or the e-mail addresses of the sender and recipients.

The Article 29 Working Party has developed an extensive body of interpretation concerning the protection of employees' personal data. Although the analysis focuses on employee data, it should be remembered that the same legal requirements will apply to the data of other individuals contained in the company's records.

European regulators have repeatedly stressed that employers can only process personal data ''lawfully,'' in accordance with established data protection principles, including:

- Finality: personal data may be processed only for specific, stated purposes and may not be processed for any other incompatible purpose.
- Legitimacy: personal data may only be processed for ''legitimate'' purposes as set forth in the Data Protection Directive.
- Proportionality: processing of personal data may not be excessive in relation to the purposes for which it was collected.
- Transparency: employers must notify employees of the data it is collecting about them, must give employees access to such data, and state the purposes for which the data are processed.[9]

Compliance with these principles trumps any employer interest or claim of necessity:

> The legitimate interests of the employer justify certain limitations to the privacy of individuals at the workplace. Sometimes it is the law or the interests of others which impose these limitations. However, no business interest may ever prevail on the principles of transparency, lawful processing, legitimisation, proportionality, necessity and others contained in Directive 95/46/EC. *Workers can always object to the processing when it is susceptible of unjustifiably overriding his/her fundamental rights and freedoms*.[10]

Using the principles as a starting point, employers may process data concerning their employees for lawful and legitimate purposes with ''unambiguous consent'' or if the processing is ''necessary.'' [11] Consent and necessity provide the only legitimate basis for data processing. Unfortunately, neither consent nor necessity support the kinds of processing required for Rule 34 compliance, and the data protection authorities generally believe that any inspection of employee communications, such as e-mail, violates the principles stated above.

Consent is problematic as a basis for processing for document production. To be valid, consent must be both freely given and capable of being revoked. The Working Party makes this point repeatedly: ''If it is not possible for the worker to refuse it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice.''[12]

From a Rule 34-standpoint, however, companies cannot permit employees to opt-out of having their documents examined in connection with document production requests. Companies cannot rely on consent as the basis for its discovery and production requirements.

Employers must therefore rely on the ''necessity'' of the processing for document production efforts. This approach is problematic as well, however, because the Article 29 Working Party has concluded that there are only three types of really ''necessary'' processing:

- Processing required for the employer to perform its contractual obligations vis-a-vis an employee (*e.g.*, processing an employee's salary data for payroll);
- Processing required for the employer to protect an employee's vital interests (*e.g.*, to protect the employee against particular hazards at the workplace); and
- Processing required for an employer to comply with its domestic legal obligations in Europe (*e.g.*, processing an employer's data for the purpose of calculating the withholding tax).[13]

The Working Party does not agree that compliance with extra-territorial legal requirements is ''necessary'' to justify processing of employee data in Europe. This conclusion was forcefully demonstrated in the data protection authority response to U.S. company establishment of whistleblower hotlines in Europe as required by Section 301 of the Sarbanes-Oxley Act.[14]

Moreover, analysis of employee e-mails—an essential part of the discovery process—is viewed with exceptional hostility. Where employers examine employee e-mails in connection with specific employee wrongdoing, they have often faced legal sanction. This is most vividly demonstrated in *Societe Nikon France v. M. Onof*.[15] There the French high court held that an employer had no legal right to intercept and read employees' e-mails and other documents, even if the employer supplied the computer and expressly provided that employees were not to use their computers for personal uses. The court stated that monitoring personal messages violates this fundamental freedom even if the employer prohibits the usage of the computer for nonprofessional purposes.[16]

Similarly, in May 2006, the French high court ruled that, absent exceptional circumstances, an employer has no right to invade the personal privacy of employees in their workplace computers.[17] In this case, a company found ''erotic photos'' on a worker's desk; as a result, the company searched the employee's work-issued computer, discovered that he had downloaded pornographic images and fired him. Although lower French courts upheld the search and firing, the high court disagreed, noting that the presence of pornography on the

[9] Id. at 3
[10] Id. at 28 (emphasis added)
[11] Id. at 15-16
[12] Id. at 23
[13] Id. at 15
[14] See Article 29 Data Protection Working Party, *Opinion 1/2006 on the Application of E.U. Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime*, Feb. 1, 2006 (00195/06EN WP117)
[15] Cass. soc., Oct. 2, 2001, Bull Civ. V, No. 291.
[16] See Yohei Suda, ''Monitoring E-Mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States,'' 4 *Wash. U. Global Stud. L. Rev*. 209 (2005), 253-256.
[17] *Philippe K. v Cathnet-Science,* Cour de Cassation, Chambre Sociale, Arret No. 1089 FS-P+B+R+1, Pourvoi No. J-03-40.017, 5/17/05. Reported in the BNA *Privacy Law Watch* (June 6, 2005).

computer did not present the type of risk that could justify an unauthorized search of the computer.[18]

The French position is not unique. The Greek data protection authority held in 2004 that even a technological ''intervention'' (such as automated scanning) by an employer of employee e-mails is illegal unless the employee is informed of the intervention and given a ''technical means of using special software to protect the secrecy of his own communication.''[19] In Italy, employers are also prohibited from monitoring e-mails; the Italian Supreme Court has held that ''an employer can only carry out such monitoring if it is aimed at ascertaining unlawful behavior on the part of the employee and provided it has reached an agreement with the local union or has authorization from the local labor office.''[20]

Given the state of the law around employee e-mails, it is difficult to imagine how a company could justify examining e-mails or computer files merely in anticipation of U.S. litigation—even if Rule 34 requires precisely that.

Indeed, in the one case that has considered the conflict between EU privacy laws and U.S. production requirements, the privacy right, as expected, triumphed. In 1995, the German government intervened in a U.S. state court civil case to object to the production of Volkswagen's printed corporate telephone directory. Based on that intervention and expert testimony about the scope and burden of German privacy laws, the Texas Supreme Court concluded that the ''corporate phone book should not be produced in contravention of German law.''[21]

International Transfers of Personal Information

Even if personal data are lawfully obtained and processed, they may not be transferred outside of the EU unless the recipient country offers adequate protection or an exception to the transborder transfer restriction applies. Since the United States has not been declared adequate, data transfers from the EU to the United States can only occur if:

- The recipient is in the U.S. Safe Harbor;[22]
- The transfer is authorized using an approved model contract; [23] or
- Another exception to the data transfer restrictions applies.[24]

Unfortunately, none of these mechanisms provide cover for U.S. companies that need to process and transfer business records containing personal information (especially employee information) to the U.S. for document production purposes.

Under the Safe Harbor agreement, U.S. entities self-certify that they are abiding by the Safe Harbor Principles. These companies may believe that the Safe Harbor provides a mechanism for processing and transferring personal data in the context of U.S.-based document production efforts because the Principles state:

> [a]dherence to these Principles may be limited: . . . by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization. . . .[25]

This interpretation is extremely risky, however, for two reasons.

First, the Safe Harbor provides a legal basis only for exporting personal data from the EU—it does not authorize any additional processing within Europe, nor does it broaden the ability of the organization to further process the data once in the United States. EU and U.S. negotiators explicitly agreed that ''where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes,'' the ''U.S. organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes.''[26]

Second, despite the general principle that Safe Harbor enforcement is the responsibility of U.S. regulators, the European data protection authorities retained jurisdiction to handle data protection violations concerning employee data.[27] Accordingly, the strict EU interpretations of the exceptions will prevail.

The model contracts are no better than Safe Harbor. Under the model contracts, the data exporter and the data importer agree to comply with applicable EU laws or similar data protection principles, thus limiting the U.S. company's ability to include the EU data in U.S. discovery and production initiatives. And, again, the data protection authorities have jurisdiction to address any perceived violations.

Neither the Safe Harbor nor the model contracts provide any resolution of the conflicts created by the EU data protection laws when employee data or other personal information is processed in the context of U.S.-based document production efforts. Conversely, companies using these data transfer constructs may have even greater risk. By bringing personal data to the U.S. pursuant to Safe Harbor or a model contract, they are in the precarious position of having data in the U.S. that is clearly subject to the Rule 34 requirements but without the authority to process the data as needed to meet those requirements.

Article 26 of the EU Data Protection Directive contains exceptions to the general prohibition on transborder data flows. Under Article 26(1)(c), personal data may be transferred as ''for the establishment, exercise

---

[18] Id .

[19] *Eighth Annual Report of the Article 29 Working Party on Data Protection* (2005) at 44 (citing Decision 61/2004)

[20] ''Monitoring Employees E-Mail and Internet Usage in Europe,'' *Internet Law-Business-e-Commerce*, May 1, 2005.

[21] *Volkswagen, A.G. v. Valdez*, 909 S.W.2d 900 (Tex. 1995)

[22] Commission Decision 2000/520/EC of 26.7.2000 - O. J. L 215/7 of 25.8.2000

[23] Commission Decision 2001/497/EC and Commission Decision C(2004)5271

[24] *E.g.*, a derogation under Article 26(1) of the E.U. Data Protection Directive. Companies can also seek specific permission from the applicable data protection authorities for the transfer, but the operational difficulties of obtaining such permission (and the low likelihood that it would be granted) render this approach of almost non-existent practical value.

[25] U.S. Department Of Commerce, Safe Harbor Privacy Principles (July 21, 2000), available at <http://op.bna.com/pl.nsf/r?Open=byul-6y2qtw>.

[26] Safe Harbor, FAQ 9 (Human Resources)

[27] Id.

  PVLR ISSN 1538-3423

or defence of legal claims.'' While this derogation seems to provide exactly what U.S. companies need, it cannot be used to support the document discovery processes necessary to comply with Rule 34 either.

All of the Article 26(1) derogations are interpreted very narrowly by the European regulatory community, and 26(1)(c) is no exception. [28.] According to a Working Party example, ''the parent company of a multinational group, established in a third country,'' that was being sued by one of its own European employees could transfer ''certain data'' relating to that employee from its European subsidiary if those data were necessary for its defense. But ''this exception cannot be used to justify the transfer of all the employee files to the group's parent company on the grounds of the possibility that such legal proceedings might be brought one day.''[29]

Moreover, the Working Party has limited the application of this exception to those cases in which ''the provisions of the Hague Conventions of 18 March 1970 (''Taking of Evidence'' Convention) and of 25 October 1980 (''Access to Justice'' Convention)'' have been complied with.[30] The U.S. is not a signatory to the Access to Justice Convention and U.S. law does not require courts to follow the procedures of the Hague Convention on the Taking of Evidence. As a result, the Article 26(1)(c) exception appears inapplicable to U.S. document production requests.

Additionally, even if the derogation did apply, it would not exempt the company from otherwise complying with all of the provisions of the data protection laws (such as limits on e-mail scanning), and it can be trumped if the transfer, in the eyes of the relevant authority, would violate the fundamental rights of the data subject. The Working Party's language is stark:

> It should also be noted, however, that the provisions of the Directive relating to transfers of personal data to third countries cannot be applied separately from other provisions of the Directive. As explicitly mentioned in Article 25(1), these provisions apply ''without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive''. This means that regardless of the provisions relied upon for the purpose of data transfer to a third country, other relevant provisions of the Directive need to be respected.[31]

Conclusion

The Rule 34 requirements pose almost insurmountable risks for companies with operations in Europe or other countries with EU-style data protection laws. These laws require both government permission and compelling justification before even the most innocuous personal data can be collected, retained, exported from the jurisdiction, or disclosed to a third party.

The conflicts between U.S. discovery requirements and international data protection laws will only become more pronounced, given the increasing use of consolidated data systems and the expanding reach of U.S. document production orders. Unfortunately, these conflicts likely cannot be resolved by companies due to the vast number of data protection authorities and lack of support for U.S.-government mandated processing generally.

Given the current attitudes of EU data protection authorities around employee-data processing generally (and employee monitoring in particular), it is unlikely that support for the types of vast data-mining and analysis required by U.S. discovery orders will be found. This likelihood is reduced even further by the current controversies between Europe and the United States over the transfer of air passenger name records or the SWIFT international financial data.

Europe is not alone. To date, EU-style laws have been enacted in many other countries, including Argentina, Australia, Canada, Hong Kong, Japan, New Zealand, and Russia. To be certain, not all of these laws are as complex or as zealously enforced as their EU models, but many of the substantive requirements are similar if not identical.

Ultimately, an accommodation, if not a solution, will have to be found. Judging from the experience with the Safe Harbor and passenger information agreements, that accommodation will result not by pressuring companies caught between two sets of conflicting legal requirements, but through long, careful, detailed negotiations between governments.

[28.] *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*

[29] Id. at 15

[30] Id. at 15

[31] Id. at 8