

# The Information May Be Virtual, but the Borders are Real: The Challenges of International E-Discovery

Kenneth N. Rashbaum, Esq.  
Sedgwick, Detert, Moran & Arnold LLP



Email and electronic documents are fast becoming the most sought-after evidence in civil litigation. “Electronic data,” wrote Judge Elizabeth T. Maass in the case of *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, “are the modern-day equivalent of the paper trail.”<sup>1</sup> The amendments to the Federal Rules of Civil Procedure on electronic discovery take effect on December 1, 2006, but inconsistency in judicial decisions regarding discovery of electronic evidence can cause severe headaches to counsel attempting to define parameters of discoverable email.

Adding to the level of complexity is the challenge of obtaining electronic evidence from Europe, Asia, and, increasingly, Latin America. As more U.S. companies expand global reach by establishing facilities and by outsourcing services offshore, an increasing amount of data will be found outside the United States. These data cannot be obtained by the expedient of a discovery demand or even, in many countries, by an American court order. How, then, does one fulfill one’s obligation to obtain electronic evidence from outside the U.S.? Alternatively, how can counsel representing a global company comply with the discovery requirements to produce electronic evidence located overseas, while at the same time complying with regional and local regulations that restrict data transfer?

The threshold question is whether data are protected from transfer by statute or regulation. In most EU member states, the term “personal data” is liberally construed to include any information relating to an identified person. In Europe, personal data are protected from disclosure outside the European Union. Without the consent of the data subject (the author, usually, in the case of emails), European Union Directives<sup>2</sup> and enabling legislation of EU member states prohibit transfer of such data outside the European Economic Area (the member states plus Iceland, Norway, and Liechtenstein) to any area in which the data protection laws are not commensurate with the level of protection within the EU. The only countries the European Commission considers to have commensurate protection are Canada and Argentina, plus the territories of the Isle of Guernsey and the Isle of Man.

It would be safe, then, to assume that emails, which routinely list the position and location of the sender, may be construed as protected data in many, if not most, EU states.<sup>3</sup>

In the absence of consent of the data subject or an order of a court in the country in which the data resides, a data protection agreement is required to transfer data to the United States for production of email evidence sought in discovery. Such an agreement can take one of the following forms: a data transfer agreement utilizing model contract clauses approved by the European Commission<sup>4</sup>; a Safe Harbor agreement<sup>5</sup> filed with the U.S. Department of Commerce, or a set of binding corporate rules.<sup>6</sup> Each format

requires that the company seeking to transfer data to the U.S. certify that it has policies and practices that protect personal data to the same extent as in Europe. As preparation of such agreements and of the required certifications regarding the existence of privacy practices takes a fair amount of time, corporations with facilities in Europe would be well advised to have such agreements in place now rather than await judicial directives to produce emails that, in the absence of data-protection agreements or orders of a foreign court, would place the producing party in violation of law.

The litigator faced with demands or court orders for e-discovery from a global corporation faces yet another hurdle: Where are the data? This is not as simple as it sounds; data created, for example, in Tokyo may reside on a server in Singapore. The law that applies to the data transmission is the law of the data’s location, but, again, there is a caveat. Certain countries, such as Canada<sup>7</sup>, France<sup>8</sup>, and the United Kingdom<sup>9</sup> consider data created in those countries to be under the protection of their laws, as U.K. Deputy Information Commissioner David Smith confirmed when he recently stated that an unauthorized transfer of U.K. data from an offshore outsourcer could be prosecuted by his office “[even if] the breach [of privacy law] takes place outside the U.K.”<sup>10</sup>

With the growth of outsourcing of back-office services such as data storage and processing, the location of data cannot be taken for granted. Data protection laws in Japan, India, and Singapore vary widely in their restrictions upon the use and transmission of personal data. South America is fast becoming a location for outsourcing,<sup>11</sup> and its data privacy regulations follow a different philosophy from that of Europe or Asia—one in which individuals may, under certain circumstances, request destruction of their personal data.<sup>12</sup>

This seeming Rubik’s Cube of regional and local statutes and regulations may provoke headaches in the heartiest of litigators, but the pain can result in gain: Europe and Asia also maintain networks of very specific document-retention regulations requiring preservation of data (including emails, in certain circumstances) on toxic exposures,<sup>13</sup> disposal of electronic equipment,<sup>14</sup> and so-called “tracking data” (the identity of the sender and the course of transmission of certain electronic communications).

Knowledge of these retention regulations can lead the litigator to evidence because the law—*somewhere*—may mandate preservation of the data. The next challenge, though, will be to know where to seek the data and how to ensure that transfer to the U.S. for purposes of litigation does not run afoul of regional or local law. ●

CONTINUED >

<sup>1</sup> No. 502003CA005045XXOCAI, 2005 WL 679071 at \*5 (Fla. Cir. Ct. Mar. 01, 2005).

<sup>2</sup> See e.g., 97/66, 1997 O.J.(L 24) 1 (EC), available at [http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l\\_024/l\\_02419980130en00010008.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf); 2002/58, 2002 O.J. (L 201) 37 (EC), available at [http://europa.eu/eur-lex/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://europa.eu/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf).

<sup>3</sup> See *Durant v. Fin.IServ. Auth.*, 2003 EWCA Civ. 1746 (Eng. C.A.), for a discussion of the trend in the U.K. to narrow this definition.

<sup>4</sup> Directive 95/46 art. 26 (4), 1995 O.J. (L 281) 31 (EC), available at <http://www.datenschutz-berlin.de/gesetze/europa/den.htm>; Commission Decision 2002/16, 2002 O.J. (L 51) 27 (EC), available at [http://www.fsai.ie/legislation/food/eu\\_docs/Materials\\_Articles/Dir2002\\_16.pdf](http://www.fsai.ie/legislation/food/eu_docs/Materials_Articles/Dir2002_16.pdf).; ICC Model Data Transfer Agreement is an alternative to the EU model clauses. Both are discussed at [http://iccwbo.org/home/e\\_business/ICC\\_model\\_clauses\\_FAQs.pdf](http://iccwbo.org/home/e_business/ICC_model_clauses_FAQs.pdf).

<sup>5</sup> Commission Decision 108/2000, 2000 O.J. (L 45) 47 (EC), available at [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l\\_045/l\\_04520010215en00470048.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l_045/l_04520010215en00470048.pdf); see [http://export.gov/safeHarbor/sh\\_overview.html](http://export.gov/safeHarbor/sh_overview.html).

<sup>6</sup> Binding corporate rules, a privacy code of conduct, are also finding acceptance in Asia and Latin America and thus are being considered as a viable form of data protection for companies with facilities outside as well as within Europe. However, several countries require that they be filed with and/or approved by the country's central data protection authority.

<sup>7</sup> Personal Information Protection and Electronic Document Act, 2000 c.5 (Can.), available at <http://lois.justice.gc.ca/en/P-8.6/258031.html>.

<sup>8</sup> Act No. 78-17 of January 1978 on Data Processing, Data Files and Individual Liberties (hereafter "French data Protection Act"), (amended by the Act of 6 Aug. 2004 relating to the protection of individuals with regard to the processing of personal data), available at <http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf>.

<sup>9</sup> Data Protection Act, 1998, c. 29 (Eng.), available at <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>.

<sup>10</sup> Tom Blass, *U.K. Data Protection Office Issues Guidance On Transfer of Personal Data Outside EEA*, PRIVACY AND SECURITY REPORT (BNA) July 17, 2006

<sup>11</sup> Thomas L. Friedman, *Latin America's Choice*, THE NEW YORK TIMES, June 21, 2006, at A17 (discussing a Uruguayan office of Tata Consultancy Services, India's largest outsourcing company).

<sup>12</sup> See Andres Guadamuz, *Habeas Data: The Latin-American Response to Data Protection*, J. INFO. L. & TECH. §3.2, available at <http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html>.

<sup>13</sup> European Council, Registration, Evaluation, Authorization and Restriction of Chemicals ("REACH"), available at [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003PC0644\(02\):EN:HTML\(amending Council Directive 67/548/EEC, 1967 O.J.\(196\) \(EC\)\)](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003PC0644(02):EN:HTML(amending Council Directive 67/548/EEC, 1967 O.J.(196) (EC))).

<sup>14</sup> See Directive 2002/95, 13.2, 2003 O.J. (L 37) (EC) available at [http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l\\_037/l\\_03720030213en00190023.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_037/l_03720030213en00190023.pdf).

*Kenneth N. Rashbaum, Esq., is a partner in the New York office of Sedgwick, Detert, Moran & Arnold LLP. He concentrates his practice in compliance, information management, and e-discovery.*