Complying Across Continents: At the Intersection of Litigation Rights and Privacy Rights

Milton H. Luoma[1] and Vicki M. Luoma[2]

[1] Information and Computer Sciences
Metropolitan State University
700 East 7th Street
St. Paul, Minnesota USA 55106-0500
Tel.: 651 793-1481; Fax: 651 793-1246
Milt.Luoma@metrostate.edu
[2] Accounting and Business Law
Minnesota State University
145 Morris Hall
Minnesota State University
Mankato, Minnesota USA 56001
Tel.: 507 389-1916; Fax: 507 389-5497
Vicki.Luoma@mnsu.edu

Abstract. This paper addresses the issues and challenges facing multinational corporations when they become involved in litigation that crosses international borders. The conflict of litigation discovery rights and individual privacy rights in different international jurisdictions can present a very challenging situation for litigants. This paper addresses the conflict inherent between litigation discovery rights versus individual privacy rights and how different nations deal with this conflict. The authors offer several pre-litigation recommendations for those corporations that anticipate the possibility of litigation involving parties in more than one international jurisdiction.

Keywords: multinational litigation, electronic discovery, privacy rights, litigation rights.

Complying with legal restrictions on litigation rights and privacy rights in different international jurisdictions has proven to be one of the most difficult challenges facing multinational corporations. At the heart of this challenge are the different priorities that different nations place upon an individual's right to litigate disputes and an individual's right to privacy. Those countries that place a higher priority on the rights of individuals to seek full satisfaction of their claims against other parties than they do upon the right of privacy tend to have much more liberal discovery rights in the litigation process than do countries that place a higher priority on the rights of individuals to retain their privacy. Those countries that value privacy rights over litigation discovery rights tend to restrict and severely limit the ability of parties to litigation to seek information that may be essential to prosecuting their claims in court.

M. Sorell (Ed.): e-Forensics 2009, LNICST 8, pp. 186 – 194, 2009.
© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2009

It is not difficult to imagine that if one were to ask any citizen of any country whether he or she would want full satisfaction of his or her claims against another party and whether he or she would want complete privacy in his or her dealings, both questions would receive a resounding affirmative response. Unfortunately, the nature of the issues precludes anyone from having a full measure of both of these rights simultaneously. This dichotomy of choices presents extremely difficult choices for multinational corporations that try to operate in diverse cultures when they become involved in litigation. This paper addresses the issues and challenges facing multinational corporations when they become involved in litigation that crosses international borders. A review of privacy rights and litigation rights both within and outside the United States will provide some important background and insights into the nature of the problem as it affects U.S. multinationals. One proposed solution to this problem, namely The Hague Convention, will be reviewed in light of Societe Nationale v. District Court, 482 U.S. 522 (1987). The authors conclude by offering some suggestions for multinationals for surviving the challenges presented by litigation that extends beyond the borders of one country.

1 Litigation Discovery Rights in the United States

In the United States electronic discovery cases and rules are changing, but one thing is consistent in U.S. discovery rules: If something exists, it is discoverable if the information to be obtained might lead to something relevant. This approach to litigation discovery places the highest priority on having disputes fully litigated in the light of all possible facts that might have a bearing on the issues in controversy.

The U.S. Federal Rules of Civil Procedure Rule 26 allow "any matter not privileged that is relevant to the claim or defense of any party"[1] to be discoverable. The rule goes on to explain that "relevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to the discovery of appears reasonably calculated to lead to the discovery of admissible evidence."[2] Such a rule is not only abhorrent to privacy minded countries but illegal in these countries as well. In the countries that guard personal privacy, litigants can obtain information only if they know exactly what they want, where it is located, how it is relevant. Only then might it be ordered produced.

United States discovery allows almost any information requested to be produced. When these early rules and traditions were established, no one anticipated a paperless society in which not only could the document be requested, but the electronic metadata associated with that document, digital artifacts, fragments and multi-versions of data could be requested as well. In addition, these digital electronic footprints are left not only on computer hard drives, but on digital telephones, cell phones, PDAs, copy machines and Internet history files. In the United States information stored on personal computers, phones or PDAs are not considered private if anything relevant to the lawsuit could be stored there. Further, employees who use home electronic equipment for work purposes can have those devices subject to discovery procedures.

---

[1] Federal Rules of Civil Procedure, Rule 26.
[2] Id.

2 Litigation Discovery Rights Outside the United States

Litigation discovery rights outside the United States are generally limited by the laws and customs of countries that value privacy rights over litigation discovery rights. Some countries more severely limit discovery rights than others. In all cases, a country's emphasis on personal privacy rights is the determining factor in the level of restriction of litigation discovery rights. In light of this assertion, it is useful to briefly review the differences in various countries' privacy legislation.

In Europe, countries belonging to the European Union developed the European Union Privacy Directive, which is valid in 25 countries. As part of these directives personal data (data which identifies or concerns a specific named person) cannot be transmitted outside the European economic area (EU nations, plus Iceland, Norway and Lichtenstein) to a country which does not provide by national law protection commensurate with the EU. Presently, only two countries meet these standards outside the EU, namely, Canada and Argentina. These protective directives are not perfect since many of the EU countries interpret them differently.

The EU data directive[3] provides that all computer processed personal data must allow the individual the absolute right to access data concerning themselves, must prove that individuals have freely given consent, the use of the data must be lawful and fair, adequate, relevant and accurate and may be used only as long as necessary and have adequate security. Further discovery of any personal data will be allowed only if the party seeking the information can prove that the document exists and is essential to the litigation.[4] Each member country is then required to adopt laws that comply with the directive and all EU countries have passed these laws.[5] As a result each countries interpretation is somewhat different.

The directives state that personal data is not only information related to a particular person but all information that is identifiable. There are some exceptions including processing all data that is necessary for litigation.[6] However the EU countries have consistently decided that the interests of company subsidiaries are not sufficient legal nexus to be considered an exception under this provision.[7]

Most civil code countries have no custom or laws concerning formal discovery and rarely allow disclosure of evidence that is known to be relevant.[8] In addition, some countries such as France have criminal statutes known as the French Blocking Statute if information is provided that has not met these requirements. Even the common law countries of Australia and United Kingdom have blocking statutes. The Australian Commonwealth Attorney General may prohibit compliance with foreign discovery orders and judgments in foreign antitrust proceedings when Australian

[3] Directive 95/46/EC.
[4] Id.
[5] Id.
[6] Council Directive 95/46/EC, art. 2(b), O.J. (L281).
[7] See European Commission, Justice and Home Affairs -- Data Protection, Adequacy of Protection of Personal Data in Third Countries, at http://ec.europa.eu/justice_home/fsj/privacy/ thridcountries/ index_en.htm
[8] UK Data Protection Act of 1998, 1998 Chapter 29, Schedule 4(5)(a).

sovereignty is infringed or where the foreign court determines Australia is the correct jurisdiction.[9]

In the defining U.S. case a French bank, Société Générale, was unwilling to examine email of their trader Jérôme Kerviel. Even though Kerviel's actions were about to destroy the company, they were still afraid of the French privacy laws.[10] The defendant sought relief through the Hague convention but the plaintiff refused and the court agreed. The court found that even though the United States had signed The Hague convention participation was voluntary and not mandatory on litigants.

In another case the U.S. courts held that the U.S. Federal Rules should apply even though the Italian litigants argued that to provide the information would be violating Italian laws.[11] In Enron v. J.P. Morgan Securities Inc.,[12] the U.S. Bankruptcy Court held that even though providing the information would be in conflict with the French Blocking Statute the party still had to provide the information requested under U.S. discovery requests. One problem has been that the French government consistently did not actually find anyone guilty under the French Blocking Statute until recently, and accordingly, U.S. courts were not taking the threat seriously. However, in a recent case a French lawyer was held criminally responsible under the statute.[13]

3 Litigation Discovery Rights Versus Privacy Rights

The main reason for this difference in litigation discovery practices is the difference in various countries' views of personal privacy. Privacy has never been a guarantee in the United States Constitution, so privacy rights have developed in a sporadic and unsystematic manner. There is no one comprehensive privacy law in the United States, but rather, privacy law in the United States can be characterized as a myriad of cases, statutes, administrative rules that rule on component of privacy. U.S. privacy laws are general and decentralized. To determine the privacy law in the United States one must examine the Federal Trade Commission rules, a variety of federal regulations, various individual state consumer and fraud acts and some sector specific acts such as the FERPA[14], Gramm Leach Bliley Act[15], HIPAA[16] and others.

---

[9] Foreign Proceedings (Excess of Jurisdiction) Act 1984 No. 3, 1984 (Mar. 21, 2004), *available at* http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200403254?OpenDocumet Foreign Proceedings (excess of Jurisdiction) Act 1984, s. 6.

[10] London Guardian September 2007 Page 1.

[11] Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., 2005 U.S. Dist. LEXIS 20049, at *14 (N.D. Ill. Sept. 12, 2005).

[12] Enron v. J.P. Morgan Secur. Inc., No. 01-16034 (Bankr. S.D.N.Y. July 18, 2007).

[13] Commission Nationale de L'informatique et des Libertés, Délibération n°2006-281 du 14 décembre 2006 sanctionnant la société Tyco Healthcare France.

[14] The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

[15] Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, provides protection of consumers' personal financial information held by financial institutions.

[16] Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996 to address the security and privacy of health data.

In the U.S. electronic data was everywhere before anyone thought of the implications of this free flowing information. No one foresaw hackers, identity thieves, phishers or pharmers. Once the problems surfaced there were too many well established institutions with vested interests and strong lobbyists who prevented any possibility of stopping the information from continuing to flow. Lobbyists[17] are individuals who are paid by special interest groups to make direct contact with members of Congress to influence their views.

A further reason for different rules is countries' views on the collection of information. In the United States discovery is handled entirely by the litigants and outside of the courts involvement unless a conflict occurs. In fact, a litigant "must, without awaiting a discovery request, provide to the other parties… a description by category and location — of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses…[18] In addition, under U.S. Federal Rules even non-parties can be compelled to produce documents to a litigation.[19] In most civil law nations gathering information is a judicial function. The civil law system of courts is based on inquisition rather than the common law adversarial system.[20] The judge normally questions the witnesses and makes a summary of the information. The United States system of discovery is unlike most other common law countries.

The problem arises for multinational corporations when they are involved in litigation that involves the United States and a country with strict privacy and limited discovery laws. If a litigant fails to provide information requested in a USA lawsuit, sanctions can be ordered. These sanctions can be anything from adverse inference instructions, fines, and default judgments. On the other hand providing the information could result in criminal and civil consequences if it involves countries that have laws against providing the information. As a result international cases are often commenced in the United States because of the more liberal discovery laws and larger judgments.

4 The Hague Convention

Some felt The Hague convention on "The taking of evidence abroad in Civil and Commercial Matters" was going to resolve this international legal conflict. The United States, France and 15 other countries agreed to The Hague Evidence Convention. This convention has procedures in which one country can request evidence located in another country. Despite the demand in international litigation, United States courts rarely grant a request to invoke The Hague Convention in litigation. In the leading case of Societe Nationale v. District Court the plaintiffs, the pilot and passenger in a Rallye plane manufactured by the defendants, sued for personal injuries resulting from the crash of an aircraft built by two French

---

[17] Lobbying Disclosure Act (2 U.S.C. § 1601–1612).

[18] Federal Rules of Civil Procedure Rule 26.

[19] Federal Rules of Civil Procedure Rule 45.

[20] Council Directive 95/46/EC, art. 2(b), O.J. (L281) See European Commission, Justice and Home Affairs -- Data Protection, Status of Implementation of Directive 95/46/EC.

corporations. The French corporations submitted answers to the complaint without challenging the jurisdiction of Iowa. Initial discovery was conducted under the Federal Rules of Civil Procedure without objection. Then, when the plaintiffs served additional discovery requests that the defendants claimed would violate French penal laws, the defendants filed for a protective order. The defendants argued that The Hague convention should be followed since the defendants were French. They further argued that the information requested was held in France and so the discovery requested was inappropriate under French law. The Republic of France weighed in on the litigation and stated, "The Hague Convention is the exclusive means of discovery in transnational litigation among the Convention's signatories unless the sovereign on whose territory discovery is to occur chooses otherwise."[21] According to Article 2 of the French Blocking Statute the defendants could attempt to secure a waiver from the French government.[22] In this case there was no indication that the defendants attempted to see the waiver nor is it likely the French government would have consented. The trial magistrate found that he was performing a balancing act between protecting citizens of the United States from harmful foreign products against France's interest in protecting its citizens from "intrusive foreign discovery procedures." When the district court denied the motion on the grounds that when the district court has jurisdiction over a foreign litigant, the Convention does not apply even though the information is physically located in a foreign country.[23] The defendants appealed and argued that the United States had agreed to The Hague Convention. The appellate court held that The Hague Convention does not provide exclusive or mandatory procedures for obtaining documents and information located in a foreign country. The court went on to find that The Hague Convention's plain language and the history of the United States ratification that it was only intended to be an optional procedure.[24] The case was then appealed to the United States Supreme Court.

The Supreme Court concluded that to take the interpretation of the defendants would mean the U.S. was giving up regulation of its courts to the Convention, which would be a serious interference with the jurisdiction of the United States courts. Further, if Congress had meant to give up control of multinational litigation, it would have been clearly stated in the agreement. The Supreme Court found that the American courts should "…take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or location of its operations, and for any sovereign interest expressed by a foreign state."[25] However, the Supreme Court confirmed the lower court's findings that the denied the defendants' request for protective orders. The Supreme Court disagrees with the appellate court's finding that The Hague Convention was not appropriate for this litigation. Instead, the Supreme Court found that litigants could use The Hague Convention if they chose to but were not required to do so. As a result of this decision, U.S. courts simply do not refer cases to The Hague Convention.

[21] Id.
[22] French Blocking Statue, Section 2.
[23] Id.
[24] 482U.S.529-540.
[25] Id.

5 Recommendations

The authors recommend the following pre-litigation practices:

- Multinational corporations should obtain consent for both the processing and the transfer of personal data. However, this has limited effect since the EU directives require that an individual must have the right to withdraw their consent at anytime.
- Multinational corporations should include clauses in their contracts that require agreement to an alternate dispute resolution process or agree to submit a dispute to The Hague Convention.
- Corporations attempting to acquire interests in foreign corporations or that are involved in cross border outsourcing should review possible legal conflicts before making decisions to acquire or use a particular outsourcing vendor corporation. The acquiring company must determine the organizational litigation risk factor.
- All employees must be educated on both local and international compliance regulations regarding electronic discovery.
- U.S. litigants requesting information must provide state-of-the-art security in the collection of personal data and its transmission.
- Litigants involved in multinational litigation must limit the requested personal data to information that is absolutely essential to the litigation. A litigant might look at the Third Restatement of Foreign Relations Law, which states that before deciding if information is needed a litigant should do a balancing test – how important are the documents, how specific is the request, where did the document originate, what are alternate means to secure information, and what is the importance of the competing governmental interests? [26] Countries with blocking statutes must also release information that is essential to litigation so long as transmission is secure. Along with accepting the benefits from the multi-national corporations some of the burdens must be accepted. These countries must also establish safe harbors for individuals or companies that have no choice but to be in conflict with some countries law.
- U.S. litigants must comply with cross-border data transfer laws to protect personal data. On the other hand, multi-national corporations outside the U.S. need to be as vigilant in retention and deletion of data as U.S. law requires.
- Litigants should seek discovery through the host venue country's court. The problem is that the process can be extremely time intensive. Balancing the requirements of two countries’ litigation timetables can be difficult. Courts in either jurisdiction must be willing to cooperate with one another. This discovery request should be a priority since it affects the courts in other countries.

---

[26] Restatement Third, Restatement of the Foreign Relations Law of the United States by The American Institute The American Journal of Comparative Law, Vol. 39, No. 1 (Winter, 1991), pp. 207-213.

- U.S. courts need to review foreign statutes and make every effort accommodate litigants that are under threat of criminal statutes. Corporations need to demonstrate efforts in complying with law and show that actions are taken in good faith.
- Legal representatives and corporate leaders from around the world need to convene at conferences in attempt to solve the problems of conflicting electronic discovery rules and regulations. The Sedona conferences have started this process of meeting and recognizing areas of disagreement.
- Corporations must appoint a technology counsel and establish litigation teams long before litigation occurs. In a recent survey, 67% of large companies (defined as with more than 200 employees) have been involved in litigation in which electronic discovery was requested. Establishing this team would determine the legal requirements of each jurisdiction and the legal penalties for complying or not complying.
- Multinational companies must develop a record-retention policy and schedule based one the top five business drivers of compliance, privacy, litigation readiness, end-user needs and cost. Multinational companies must address country specific requirements on an exceptions basis. Establish a plan that limits access to personally identifiable information and secure the privacy data. Multinational companies must conduct periodic audits to verify compliance and automate as much as possible.
- Companies must review regulations in all possible jurisdictions and prepare for potential litigation. Preparation is important and compliance with as many jurisdictions as possible is essential for preparation. Companies must set up a strategic plan in case of litigation. Multinational corporations may want to keep duplicate sets of data in various locations.

6 Conclusions

There are no easy answers to the problem posed by conflicting electronic discovery and personal privacy laws crossing international borders. At the present time, U.S. courts will continue to put litigants in the precarious positions of violating EU directives and worldwide blocking statutes. Countries with blocking statutes have begun prosecuting violators of their blocking statutes. Multinational companies are left in the middle of these conflicting rules and laws. The American system plays havoc with individual privacy rights, but it provides the best opportunity for a party to prove its case. The problems with international data collection are just beginning to surface and action should be taken to deal with these issues preemptively. Countries vary on retention regulations that affect the ability of litigants to collect and preserve relevant material. It is unlikely either side of the issue will change its mind on what is more important – litigation discovery rights or individual privacy rights – but a spirit of compromise or consideration must prevail with disputes not decided on a parochial basis.

There are ethical issues involved in enforcing one nation's laws over another's with important implications and the other consequences. The present system simply is not working well. Nations and their litigation and privacy policies do not exist in isolation. The nations of the world are too interdependent for any single one to assert

supremacy of its particular litigation point of view, customs or traditions. This can happen only if all countries – regardless of whether they are common law or civil law countries, or whether their bias is in favor of privacy protection, or whether their bias is in favor of information disclosure – can find common ground and be willing to compromise.

Ultimately, there are no simple and universal answers to the challenges and issues posed in cases of international litigation where the jurisdictions involved have diametrically opposed laws and customs. All organizations that operate in multiple international jurisdictions must be fully aware of the rights and duties of all potentially interested parties and prepare for the challenges.

References

1. Federal Rules of Civil Procedure, Rule 26
2. Council Directive 95/46/EC, art. 2(b), O.J (L281)
3. European Commission, Justice and Home Affairs – Data Protection, Adequacy of Protection of Personal Data in Third Countries, http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm
4. UK Data Protection Act of, 1998 Chapter 29, Schedule 4(5)(a) (1998)
5. Foreign Proceedings (Excess of Jurisdiction) Act 1984 No. 3, 1984 (March 21, 2004), http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200403254? Open Document Foreign Proceedings (excess of Jurisdiction) Act 1984, s. 6
6. London Guardian, p. 1 (September 2007)
7. Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., 2005 U.S. Dist. LEXIS 20049, at *14 (N.D. Ill. September 12, 2005).
8. Enron, v.J.P.: Morgan Secur. Inc., No. 01-16034 (Bankr. S.D.N.Y. July 18, 2007)
9. Commission Nationale de L'informatique et des Libertés, Délibération n°2006-281 du 14 décembre 2006 sanctionnant la société Tyco Healthcare France (2006)
10. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
11. Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, provides protection of consumers' personal financial information held by financial institutions (1999)
12. Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996 to address the security and privacy of health data (1996)
13. Lobbying Disclosure Act (2 U.S.C. § 1601–1612)
14. Federal Rules of Civil Procedure Rule 26
15. Federal Rules of Civil Procedure Rule 45
16. Council Directive 95/46/EC, art. 2(b), O.J (L281) See European Commission, Justice and Home Affairs – Data Protection, Status of Implementation of Directive 95/46/EC
17. French Blocking Statue, Section 2
18. Societe Nationale v. District Court, 482 U.S. 522 (1987)
19. Restatement Third, Restatement of the Foreign Relations Law of the United States by The American Institute The American Journal of Comparative Law 39(1), 207–213 (Winter, 1991)