



International Data Transmission

A Guide to Navigating Conflicting Laws in Cross-Border Discovery

Copyright © 2010 Kroll Ontrack Inc. All Rights Reserved.

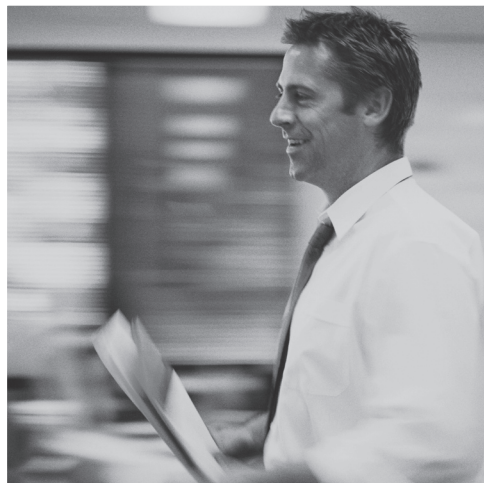
Kroll Ontrack, Ontrack and other Kroll Ontrack brand and product names referred to herein are trademarks or registered trademarks of Kroll Ontrack Inc. and/or its parent company, Kroll Inc., in the United States and/or other countries.

4	Introduction
5	What are Cross-Border Discovery Disputes?
6	Cross-Border Disputes are Increasing and Becoming More Complex
8	Challenges of International Data Transmission The European Union Data Protection Directive Nation-Specific Laws Jurisdiction
10	Overcoming the Prohibitions Against Data Transfers The Hague Convention Transferring Data Within the Constraints of the European Union Data Protection Working Within the Constraints of Nation-Specific Laws & Jurisdictional Concerns
14	References
15	About Kroll Ontrack

Introduction

Turbulent legal conflicts arise when liberal United States (U.S.) discovery rules require production of data stored in a nation with laws restricting the transference of that data. In a globalized world where oceans and national boundaries no longer create barriers to communication and business, clashes between seemingly incompatible discovery and privacy laws are inevitable. This raises the question – when the legal discovery obligations of one sovereign state clash with the sovereign laws of another state, what recourse is available?

The conflicts between sovereign laws are not insurmountable, although they may seem daunting at first. The key is to anticipate the conflicts, recognize them when they arise, and choose an appropriate resolution based on the facts and circumstances of the case. This guide provides an overview of the challenges of international data transmission and practical solutions to overcome these challenges. Armed with this knowledge, legal teams will be better positioned to capably represent their clients in cross-border discovery disputes.



What are Cross-Border Discovery Disputes?

What Are Cross-Border Discovery Disputes?

In the context of U.S. civil litigation, cross-border discovery disputes arise when U.S. courts, in accordance with the U.S. discovery system, order discovery of data physically located outside the U.S., but that discovery is prohibited or restricted by a data protection or privacy law in another nation.

To understand what cross-border discovery disputes are, it is first critical to understand why they arise. Countries around the world have widely divergent legal systems and hold vastly differing philosophies with regard to data privacy and discovery.

Discovery in the United States – A Broad Approach

The discovery system in the United States is based on the premise that broad discovery will lead to discovery of the truth. In furtherance of this goal, Federal Rule of Civil Procedure 26(b)(1) defines the general scope of discovery in the U.S., providing that parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense. The rule further provides that relevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. This federal rule and corresponding state rules are interpreted liberally to allow for broad discovery.

Courts in the U.S. will extend long-arm jurisdiction to seek pre-trial discovery of data located abroad.

The judicial rationale is that persons who do business with individuals or entities located within the U.S. or otherwise bring themselves within the jurisdiction of the U.S. receive benefits and legal protections through their connections, and are correspondingly subject to the burden of U.S. law, including discovery laws.ⁱ For example, in a seminal case, the U.S. Supreme Court stated, "It is well settled that such [foreign blocking] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute."ⁱⁱ

Five factors have emerged that courts should consider in deciding whether to issue an order directing production of information located outside the U.S.: (1) The importance of documents or other information requested to the investigation or litigation; (2) the degree of specificity of the request; (3) whether the information originated in the U.S.; (4) the availability of alternative means of securing the information;

and (5) the extent to which non-compliance with the request would undermine important interests of the U.S., or the state where the information is located.ⁱⁱⁱ

Generally, U.S. courts have liberally construed discovery requests to be reasonable under these factors, thus compelling international discovery. For example, a U.S. circuit court of appeals upheld a district court sanction against a Chinese corporation who refused to comply with a discovery order because disclosure of the requested information was prohibited by China's State Secrecy Laws. The court found that the strong interest of the U.S. in enforcing its judgments outweighed China's interest in confidentiality.^{iv} American courts have also found that justifications such as adjudicating disputes^v; combating international terrorism^{vi}; and collecting taxes from and prosecuting tax fraud perpetuated by foreign subsidiaries^{vii}; among others, constitute important American interests which warrant compelling discovery abroad.

What are Cross-Border Discovery Disputes?

Discovery in Many Other Countries – A Narrow View

Many other countries, including Member States of the European Union, Canada and Asia, have a complex network of data protection, data privacy and state secret laws, which prohibit or restrict the liberal discovery approach taken by the U.S. legal system. The discovery systems in many of these nations have developed to allow for much narrower discovery. For example, most civil code countries do not have a formal discovery process, and prohibit the disclosure of evidence beyond that which is admissible at trial.

Europe particularly has a long history of fiercely preserving individuals' right to privacy. The development of stringent

data protection laws in Europe, which began in the early 1970s, originated in the European Convention on Human Rights of 1950, as well as many cultural and historical influences.^{viii} Article eight of the European Convention provides, "Everyone has the right to respect for his private and family life, his home and his correspondence."^{ix}

Companies, counsel and courts in civil and common law countries that have much narrower discovery systems often view the U.S. process of discovery as burdensome and in violation of privacy rights. While in some cases the need for production is understood, objections arise when the production requirements in the U.S. compromise the right to privacy.

When the legal discovery obligations of one sovereign state clash with the sovereign laws of another state, what recourse is available?

Cross-Border Discovery Disputes are Increasing and Becoming More Complex

A number of converging factors are rapidly increasing the occurrence of international discovery, and correspondingly the prevalence of cross-border discovery disputes. The increase in international discovery heightens both the frequency of cross-border discovery disputes and their intensity, reinforcing the need to be prepared for international discovery. Several factors that add to the complexity of international discovery are as follows.

The Consequences of Unlawful Cross-Border Discovery

The consequences of violating either U.S. discovery laws or international data privacy laws are tangible and real. U.S. courts have repeatedly sanctioned companies who have failed to comply with discovery requests. Recent case law in Europe indicates that Member States in the European Union will be enforcing previously under-enforced civil and criminal penalties for violating data

privacy laws. For example, the U.K. Financial Services Authority fined a subsidiary of American International Group £640,000 in 2008 for transferring data without adequately protecting the data prior to transfer.^x Similarly, the French Supreme Court upheld a criminal conviction and €10,000 fine against a French attorney who violated French privacy laws in order to comply with a U.S. discovery order.^{xi}

Globalization and the Proliferation of ESI

The advent of advanced technological communications and travel in recent years has made the international business community interconnected. Moreover, the proliferation of electronic communications has fundamentally changed the way international business is conducted; business documents created in Beijing can be transmitted to London in the blink of an eye, and accessed over the Internet at a coffee shop in Seattle. Many companies now have global operations, and trade and transactions take place internationally. The Internet has made it possible for us to conduct business with anyone, from anywhere in the world.

Zubulake v. UBS Warburg^{xii}, a series of landmark American discovery decisions, illustrate the legal ramifications of this transformation. In Zubulake, the court ordered UBS Warburg, a multinational corporation, to pay monetary sanctions for its failure to preserve relevant e-mail stored on its server in Hong Kong. UBS Warburg's Hong Kong office had the same responsibility under U.S. law to preserve relevant electronic evidence as if the office were located in Los Angeles.^{xiii} Communications technology has torn down practical barriers to crossing jurisdictional borders, and legal barriers are also under pressure.

IT Infrastructure and Cloud Computing

Information technology (IT) systems, unlike legal systems, do not necessarily recognize international borders. For instance, cloud computing involves entrusting electronic data for storage and/or processing to a third-party provider, and then remotely accessing the data "in the cloud" via the Internet. The data is in-fact stored on a server operated by the cloud provider, and that server can often be located outside the jurisdiction where the data originated. So even where transactions and events themselves are not international, the data evidencing these activities may nevertheless be scattered around the globe. Data stored on a server may become subject to the laws of the jurisdiction where it is physically located, even if the data on that server did not originate or is never accessed in that jurisdiction.

The Economy and Increased Regulation

The global economic recession beginning in 2007 has been accompanied by a rise in the incidence of fraud. Increased incidences of fraud have led to a growing number of internal electronic investigations. The economic woes of recent times are prompting governments around the world to enact legislation for increased regulatory supervision and more aggressive investigations. It is hypothesized that this increased regulation and litigation will lead to increased cross-border discovery.

Legal complexities involved in the transfer of electronic data can complicate the exchange of cross-border discovery. The European Union Data Protection Directive 95/46/EC often serves as a roadblock to litigants that seek to transfer data from the U.K. to the US. Nation-specific laws and U.S. jurisdictional considerations may raise concerns as well.

Increased regulation and litigation will lead to more cases that involve cross-border discovery.

Challenges of International Data Transmission

The European Union Data Protection Directive

The European Union Data Protection Directive 95/46/EC^{xiv} (Directive) poses a significant challenge to parties needing to transfer data from the European Economic Area to the United States. The directive has been adopted by all Member States to the European Union, but has not been uniformly or consistently implemented.

The Directive, adopted by the European Commission in 1995, provides in its first article 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.” The rationale behind the Directive is that electronically stored personal data is particularly vulnerable to abuses

and in need of formal protection. Understanding that the Directive only applies to personal data is central to understanding why the Directive was framed and how it is implemented.

Nation-Specific Laws

While the EU Directive established a basis of minimum protections, individual EU Member States are free to provide more stringent protections, and some have. Elsewhere around the world, increasing numbers of nations have enacted laws and guidelines tailored to their specific data protection aims to protect data created or stored within their borders. Familiarity with the EU Directive is thus only the starting point; counsel must also become familiar with the state-specific data protection laws for

the countries in which they seek discovery. Counsel should look carefully at the following types of laws to ensure they are complied with when approaching a cross-border dispute within or across particular jurisdictions:

■ **State-Specific Data Protection Laws:** Nations frequently have laws that provide for the protection of personal data; these laws are sometimes codified in employment laws or statutes. For example, in Canada, foreign parties must comply with the Canadian Personal Information Protection and Electronic Documents Act that governs the use of personal data in commercial businesses.^{xxiii} Moreover, data protection laws will frequently govern the procedures of data collection, processing and onward transfer.

The Eight Principles Restricting the Handling of Personal Data under the Directive.

1. Limited purpose for collection and use: Data should be processed for a specific purpose, and subsequently used or communicated only in ways consistent with that purpose.^{xv}
2. Integrity: Data should be kept accurate, up-to-date and no longer than necessary for the purposes for which collected.^{xvi}
3. Notice: Data subjects should be informed of the purpose of any data processing and the identity of the data controller, whether or not the personal data is collected or obtained from the data subject.^{xvii}
4. Access, choice and consent: Data subjects have the right to obtain copies of their personal data, to rectify any inaccurate information, and object to processing in certain situations even when the Directive is otherwise satisfied. The Directive requires the data subject to provide unambiguous consent to personal data processing, unless certain exceptions discussed below apply.^{xviii}
5. Security: The data controller and processors must take appropriate measures to ensure adequate security and to protect the data.^{xix}
6. Onward transfer: Data controllers may not send data to countries that do not afford “adequate” levels of protection for personal data. The U.S. has not been deemed to provide adequate levels of protection.^{xx}
7. Special protections for sensitive data: Additional protections must be provided for special categories of data revealing the data subject’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.^{xxi}
8. Enforcement: Data subjects must have a remedy to redress violations.^{xxii}

■ **State Secrecy Laws:** Some countries may also have laws designed to protect information deemed to be a state secret. State secrecy laws frequently arise in countries such as China and Vietnam where the economies may be transitioning towards capitalism but the governments maintain strict control over information. Violations of state secrecy laws are frequently punishable by criminal prosecution.

■ **Banking Laws:** Nations may have banking laws that affect the transfer of data internationally. The protection of financial information (or other subject-specific information) may have heightened privacy protections over information generally.

■ **Blocking Statutes:** Some nations may enact blocking statutes specifically intended to block international data transmission, even if the collection, processing or other use of information would be permissible within the country's borders. For instance, French Penal Law 80-538 provides: "Subject to international treaties or agreements and laws and regulations in force, it is forbidden for any person to request, seek or communicate in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures, or in the context of such procedures."^{xxiv} U.S. courts

do not view blocking statutes as an absolute bar on discovery. According to recent U.S. case law, blocking statutes do not usurp an American court's power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute.^{xxv}

Jurisdiction

Jurisdiction also poses a challenge to litigators who must transfer data to the U.S. in response to a discovery request. Even if data can be lawfully transferred into the U.S., some corporations still have major concerns about transferring data into the U.S. because third-parties and government agencies in the U.S. could potentially subpoena the foreign documents. Corporations have a business incentive to keep their company information confidential, and are not subject to demand under the U.S. subpoena power, or search and seizure under the USA Patriot Act.

Key Terms Under Directive

Personal Data – Any information relating to an identified or identifiable natural person. This broad definition includes names, e-mail addresses, telephone numbers and birthdays, as well as identifiable physiological, mental, economic, cultural and social traits (not merely "identification" numbers such as national identity card numbers, etc.).

Data Subject – A natural person who can be identified, directly or indirectly, by the personal data. Even non-EU citizens can be considered data subjects under the Directive.

Data Processing – Any operation(s) performed upon personal data, such as "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." A February, 2009 working document by an independent European advisory body clarified that any retention, preservation or archiving of data constitutes processing.

Data Controller – A person or entity that determines the purposes and means of the processing of personal data.

Data Processor – A person or entity that carries out the processing of the data at the instructions of the data controller.

European Economic Area – Consists of all 27 EU Member States, as well as Norway, Iceland and Liechtenstein.

Overcoming the Prohibitions Against Data Transfers

The Hague Convention

The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Convention)^{xxvi} presents one method for overcoming international data transmission hurdles. The Hague Convention is a multilateral treaty originally signed in 1970 and currently subscribed to by the U.S., the European Union and 67 other countries. Article 23 of the Hague Convention sets forth a uniform procedure for the issuance of letters of request. The letters of request are petitions from a court in one nation to a designated central authority in another country requesting assistance from that authority in obtaining information that is located within the central authority's borders. An approved letter of request permits the transfer and processing of data.

The Hague Convention is impractical, seldom used and severely limited in several respects. Many states are not signatories to the Hague Convention and even a signatory nation may declare that it will not approve letters of request for the purpose of obtaining pre-trial discovery of documents; many nations have filed such reservations, including France, Germany, Spain and the Netherlands.^{xxvii} Moreover, a signatory nation may ignore or deny any request if it "considers that its sovereignty or security would be prejudiced" by executing the request.^{xxviii} Also, the process of obtaining an approved letter of request is painfully time consuming – often taking six to twelve months – rendering the solution impractical in light of often tight court-appointed deadlines.

The Article 29 Data Protection Working Party (EU Working Party) urges the Hague Convention to be considered first as a method of providing for data transfer.^{xxix}

The U.S. Supreme Court held that the Hague Convention is merely an optional method of obtaining evidence internationally, referring to the procedures as "unduly time consuming and burdensome."^{xxx}

The Hague Convention, when it was drafted nearly four decades ago, was not designed to accommodate the massive amounts of electronically stored information commonly involved in litigation today, nor was it designed for the frequency and pace of modern international litigation.

Tips to Transfer Data Within The Constraints Of The European Union Data Protection Directive

Obtain Consent from Data Subjects

The Directive expressly provides that personal data may be processed with a data subject's unambiguous consent. Accordingly, counsel involved in international data transmission can transfer data in response to a U.S. discovery request if they obtain the consent of every data subject – that is, any natural person who can be identified through the personal data. The process of obtaining consent in order to accomplish international data transmission is challenging for two principal reasons.

First, obtaining consent from every data subject is time consuming and logistically difficult. Data subjects in the EU are typically well informed regarding their privacy

Questions to Consider When Engaged in Cross-Border Discovery:

- Is it necessary to report the processing of data that is contemplated and seek approval from the local data protection authority or works councils elected by employees?
- Is it necessary to notify or obtain the express consent of data custodians before collecting their data?
- Do the data custodians have to be told how the data is going to be used?
- Are individuals entitled to be present when data is collected from their computers?
- Can data be transferred to the U.S. for processing?
- Can data in the EU be reviewed in the U.S. via a Web-based review tool?
- Do you need a local agent or nominated representative in the jurisdiction present when the collection takes place?

rights and not eager to waive them, especially with the understanding that their employment cannot be jeopardized if they refuse to provide blanket consent. Data subjects frequently refuse to provide consent until all personal items (e.g. personal photos and non-work related e-mail on a work computer) are removed. It is fairly common for employees to edit data consent documents before signing, and to negotiate their own terms.

Second, consent is only valid under the Directive if it is fully revocable at any time – even after the data has been transferred to the U.S. and becomes part of the litigation. Should a data subject revoke his or her consent during litigation, heated disputes and evidentiary issues may arise surrounding that data.

The consent method is riddled with difficulties, is time consuming and very expensive. Also, there are cases where obtaining consent may defeat the purpose of the data collection, such as cases where collection of data is best done without telling the subject out of fear of spoliation or destruction of the data. Attorneys who nonetheless opt for the consent method should make sure to provide data subjects with sufficient time to consider the proposed consent in order to avoid claims of coercion that might later be used to nullify consent. Also, counsel should advise the U.S. court early on that the process of obtaining consent will be time-consuming, and seek the appropriate discovery extensions.

Attempt to Fall Within the Legal Necessities Exemption to the Directive

The Directive permits onward transfer of data without individual consent from data subjects in certain circumstances. The most important exception for cross-border discovery is the legal necessities exemption, which provides that personal data is exempt from the prohibition of data transfers set out in the Directive if it is necessary to transfer the data in order to comply with the legal obligations of the controller.^{xxx} It is currently an unresolved issue whether legal obligations from U.S. discovery requests trigger the legal necessities exemption.

The EU Working Party posits that foreign discovery obligations will not usually trigger the legal necessities exception unless an “individual member state has a legal obligation to comply with an Order of a Court in another jurisdiction seeking such discovery.”^{xxxii} The EU Working Party further opines that data controllers in the EU have no legal ground to store personal data for an unlimited period of time because of the mere “possibility of litigation in the U.S., however remote this may be.” The EU Working Party does acknowledge that relevant data to be used in a “specific or imminent litigation process” should be retained until the conclusion of the litigation and any period allowable for appeal in the particular case.

The most significant difficulty with the legal necessities exemption is that its parameters are ill-

defined. Thus, reliance on self-determination of data protection laws and legal exemptions as a basis for onward transfer is fraught with risk. An alternative method to cross-border discovery, as discussed below, should be considered in most cases.

Look for a Service Provider that is Safe Harbor Certified

The U.S. and EU have developed a safe harbor agreement that allows U.S. organizations to certify to the U.S. Department of Commerce that they will provide privacy protections that meet the Directive’s adequacy standards when transferring personal data outside of the EU. A safe harbor certified organization can transfer data lawfully from the EU to a compliant facility in the U.S. in compliance with the Directive for data processing and reviewing without obtaining the data subjects’ consent. Safe harbor certification requires that U.S. organizations meet the following “principles” or adequacy standards:

- **Notice:** Certified organizations must notify and provide certain information to individuals about the purposes for which they collect and use information about them.
- **Choice:** Certified organizations must give individuals the chance to “opt out” or “opt in” to certain uses of the disclosed information, depending on the circumstances.
- **Onward Transfer to Third-Parties:** Certified organizations must apply the notice and

Overcoming the Prohibitions Against Data Transfers Cont.

choice principles to disclose information to a third-party, and may do so only if certain conditions are met that ensure the third-party will provide adequate privacy protections.

- **Access:** Certified organizations must provide individuals access to information about themselves and the ability to redress inaccurate information in certain circumstances.
- **Security:** Certified organizations must take reasonable precautions to protect personal information from alteration, destruction or unintended use.
- **Data Integrity:** Certified organizations must take reasonable steps to ensure that the data is relevant for the purpose which it is to be used.
- **Enforcement:** Certified organizations must meet certain requirements that allow for verification that the previous six requirements have been satisfied.

Counsel should verify that any service providers they partner with in international discovery between the U.S. and EU are safe harbor certified. The safe harbor provides a blanket grant of authority for international data transmission so long as the service provider or entity conducting the data transmission is safe harbor certified.

Tips to Work Within the Constraints of Nation-Specific Laws & Jurisdictional Concerns

Look for a Service Provider with an International Presence to Assist in Collection, Processing and Review Abroad

Counsel should look for a service provider with offices and personnel located abroad to assist in collection, processing and review outside the U.S. The EU Directive and the laws of many nations are much more favorable to processing and review within the boundaries of the European Union or their country than if it is done outside their jurisdiction, where they have less assurance that the levels of protection their law requires are being met.

■ **Collection:** The logistical challenge of collecting data in remote jurisdictions (often simultaneously in multiple locations) means companies' IT departments may need the support of external experts, especially when time is of the essence. When data collected in these countries needs to be transferred to the U.S., companies can rely on a service provider with an international presence to harvest data on-site in a targeted and rapid manner. These providers will have knowledge of local privacy customs and language, which can dramatically speed up the collection process and decrease the risk of running afoul of laws regulating the collection process.

Moreover, a provider with experience in the area will be familiar with working alongside local authorities;

for example, collection in the EU often requires collection in the presence of regulatory authorities. Often, local laws require the submission of collection documentation, which may include a written letter of invitation from the local office of the company seeking the collection, documentation of the source of the data, the purpose of the collection, and the destination of the data. Document collection efforts should be well documented to demonstrate the thoroughness of the data collection, and to assure regulators that the collection has been performed lawfully.

■ **Processing:** Attorneys should partner with a service provider who has an international presence sufficient to process data outside the U.S., preferably in the nation where the data originated. Data protection laws usually allow data to be processed locally. Service providers with advanced technological aides can effectively search potentially relevant data to identify the information that is most likely responsive, needing to be produced in response to the U.S. discovery request. Counsel should ensure that any service provider they partner with has a data processing engine that is Unicode compliant, recognizes multilingual character sets, and can reliably filter and search multilingual data. Apart from ensuring that data protection laws are not breached, this technology-driven approach also ensures that discovery costs are kept to a minimum.

Performing processing in the nation where the data originated significantly reduces the risk of unlawfully transferring personal data to the U.S. Processing data abroad prior to transferring the data is an approach endorsed by the EU Working Group: “When personal data is needed, the ‘filtering’ activity should be carried out locally in the country in which the personal data is found before the personal data that is deemed to be relevant to the litigation is transferred to another jurisdiction outside the EU.”^{xxxiii} The approach is also recommended by the Sedona Conference, a private legal think-tank in the U.S.: “Any processing needed to determine the relevance of the personal data should be done within the EU before any transfer.”^{xxxiv} This sound advice is likely equally applicable in other jurisdictions where data protection regimes are in place.

■ **Document Review:** Legal teams may consider partnering with a legal services provider that has an international presence to review the data in its country of origin. A data set that has been reduced in volume through processing can be reviewed for confidentiality outside the U.S., and references to personal data can be removed or redacted

before it is transferred. In cases where personal data is relevant, it is necessary to ensure that the personal data is being permissibly transferred. Even the transfer of relevant personal data can violate international laws.

Redacting as much personal data as possible prior to transferring data to the U.S. reduces the risk of violating an international data protection law, and also reduces company concerns that personal data in U.S. jurisdiction will be accessed by a third party or government agency through the U.S. subpoena power.

There is some legal debate whether remote access via the Internet constitutes a transfer of data. For example, in one case in the EU, the European Court of Justice on appeal held that the upload of personal data to an Internet Web site did not constitute onward transfer of data when the person posting the information and the Internet service provider hosting the Web site were both in an EU Member State. The court held that a “transfer” under the Directive required more than the ability to access data from a third country rather, it required that a transfer of personal data occur from one place and person to another place and person.^{xxxv}

Partner with Local Counsel

Partnering with local legal experts to navigate the complexities of data protection and privacy law abroad is absolutely essential. Many countries that have data protection laws have very specific provisions and procedures governing the transfer across international lines of that data. Knowing these laws will help dictate every step you should take during cross-border discovery matters.

Seek a Court Order in the Nation Where Data is Located

Attorneys are well advised to seek a legal opinion or court order in the nation where data is located. Data can be transferred where any enactment, rule of law or court order authorizes the transfer. For example, in *Re Madoff Securities International, Ltd.*, a United Kingdom court approved an onward data transfer to the U.S. as an exception to U.K. data protection law because the transfer was “necessary for reasons of substantial public interest” – the unraveling of fraud that would “undoubtedly involve legal proceedings, and the establishment of legal rights would be necessary to wind up the affairs of both parties.”^{xxxvi}

This is a safe course of action to avoid penalties for breaking data protection laws, as any transfer would be acting under express legal authority. Moreover, an express denial of the transfer would be useful in demonstrating to a U.S. court that the transfer is in-fact unlawful, and arguing that discovery of the international data should not be compelled.

The key to overcoming disparate sovereign privacy laws is to anticipate conflicts and choose a resolution based on the facts of the case.

References

- i Restatement (Third) of Foreign Relations Law of the United States, § 442, Reporter's Notes for the Restatement (2008).
- ii Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for Southern Dist. of Iowa, 482 U.S. 522 (1987).
- iii Restatement (Third) of Foreign Relations Law of the United States, § 442 (2008).
- iv Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468 (9th Cir. 1992).
- v Strauss v. Credit Lyonnais, S.A., 249 F.R.D. 429, 443 (E.D.N.Y. 2008) ("It is axiomatic that the United States has a substantial interest in fully and fairly adjudicating matters before its courts.") (internal citations omitted).
- vi See Strauss v. Credit Lyonnais, S.A., 249 F.R.D. 429 (E.D.N.Y. 2008); Weiss v. Nat'l Westminster Bank, PLC, 242 F.R.D. 33 (E.D.N.Y. 2007).
- vii United States v. Vetco, 691 F.2d 1281 (9th Cir. 1981).
- viii The Sedona Conference® Framework for Analysis of Cross Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery (August 2008) (Public Comment Version), A Project of the Sedona Conference® Working Group 6 on International Electronic Information Management, Discovery and Disclosure.
- ix European Convention on Human Rights of 1950, Article 8; See also Dorothy Heisenberg, Negotiating Privacy: The European Union, The United States and Personal Data Protection (2005).
- x Cook, Brandon, Why Cross-Border Litigation is a Compliance Concern, Sarbanes-Oxley Compliance Journal (May 21, 2009), available at http://www.s-ox.com/dsp_getNewsDetails.cfm?CID=2599 (last accessed 7/14/09).
- xi In re Advocat "Christopher X," No. 07-83228 (Cour de Cassation Dec. 12, 2007); See also Strauss v. Credit Lyonnais S.A., 242 F.R.D. 199 (E.D.N.Y. 2007).
- xii See Zubulake v. Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003); 220 F.R.D. 212 (S.D.N.Y. 2003); 229 F.R.D. 422 (S.D.N.Y. 2004); and 382 F.Supp.2d 536 (S.D.N.Y. 2005).
- xiii See Zubulake v. Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003) and 229 F.R.D. 422 (S.D.N.Y. 2004).
- xiv Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data , available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm (last accessed 12/28/09).
- xv Id., Art. 6, ¶ 1(b).
- xvi Id., Art. 6, ¶ 1(d).
- xvii Id., Arts. 10, 11.
- xviii Id., Arts. 7, 12, 14.
- xix Id., Art. 17.
- xx Id., Arts. 25, 26.
- xxi Id., Art. 8, ¶ 1.
- xxii Id., Arts. 22-24.
- xxiii Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/legislation/02_06_01_e.cfm (last accessed 7/14/09).
- xxiv French Penal Law 80-538.
- xxv In re Global Power Equipment Group, 2009 WL 3464212 at 12 (Bkrcty.D.Del. Oct. 28, 2009).
- xxvi Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (concluded Mar. 18, 1970) (entered into force Oct. 7, 1972), available at http://www.hcch.net/index_en.php?act=conventions.text&cid=82 (last accessed 7/14/09).
- xxvii The Sedona Conference® Framework for analysis of cross border discovery conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery (August 2008) (Public Comment Version), A Project of the Sedona Conference® Working Group 6 on International Electronic Information Management, Discovery and Disclosure.
- xxviii Id.
- xxix Working Document 1/2009 on pre-trial discovery for cross-border civil litigation, Article 29 Data Protection Working Party (adopted on Feb. 11, 2009), available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm (last accessed 7/14/09).
- xxx Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for Southern Dist. of Iowa, 482 U.S. 522, 544 n. 28 (1987).
- xxxi Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data , available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm (last accessed 12/28/09).
- xxxii Working Document 1/2009 on pre-trial discovery for cross-border civil litigation, Article 29 Data Protection Working Party, 9 (adopted on Feb. 11, 2009), available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm (last accessed 7/14/09).
- xxxiii Id. at 11.
- xxxiv The Sedona Conference® Framework for analysis of cross border discovery conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery (August 2008) (Public Comment Version), A Project of the Sedona Conference® Working Group 6 on International Electronic Information Management, Discovery and Disclosure.
- xxxv Bodil Lindqvist v. Sweden, Case C-101/01 (2003).
- xxxvi Re Madoff Securities International, Ltd - [2009] All ER (D) 31 (Mar).

About Kroll Ontrack

About Kroll Ontrack

Kroll Ontrack provides technology-driven consulting services and software to help legal, corporate and government entities as well as consumers manage, recover, search, analyze, produce and present data efficiently and cost-effectively. In addition to its award-winning suite of software, Kroll Ontrack provides data recovery, paper and electronic discovery, document review, computer forensics, secure information services, ESI and jury consulting, and trial presentation services. Kroll Ontrack is the technology services division of Kroll Inc., the global risk consulting company. For more information about Kroll Ontrack and its offerings please visit: www.krollontrack.com; www.ontrackdatarecovery.com.

Kroll Ontrack holds a Safe Harbor Certification and can assist you in your cross-border discovery with its cutting-edge technologies, customized approach to each case and its experts, technology and offices located internationally.





9023 Columbine Road
Eden Prairie, MN 55347
800 347 6105
www.krollontrack.com

Copyright © 2010 Kroll Ontrack Inc.
All Rights Reserved.

All other brands and product names are
trademarks or registered trademarks of
their respective owners.