Where Discovery and Privacy Collide

Welcome to the Practical Guide to Cross-border Ediscovery by KLDiscovery.

Litigation teams face new challenges when an ediscovery project crosses borders – from multilingual data and unique cultural norms to unfamiliar laws, regulations and data privacy practices.

In addition, the international data protection landscape is changing, and U.S. businesses with global operations need to be prepared. Companies need to think carefully about the risks of transferring data across borders.

Litigation, compliance demands and investigations are part of the regular course of business for U.S. lawyers. With global considerations and cross-border implications, law firms and companies now rely on mobile ediscovery technologies, in-country data centers and local expertise to empower the processing and transferring of data in a compliant and cost-effective manner.

This guide includes practical insights into how organizations all over the world are managing a wide range of business challenges using ediscovery technology.

KLDiscovery is here to help you and your business thrive and adapt in a changing ediscovery world.
Table of Contents

Introduction 1

Setting the Stage: Global Case Studies 3

Laws and Rules: Countries at a Glance 5


Major Milestones: EU Data Privacy and Protection 11
Data protection is a cornerstone consideration in cross-border litigation, often demanding the processing and potential review of data without removing data from the organization or country. As a result, practitioners turn to mobile ediscovery technologies and local expertise to minimize risks associated with the transfer of data.

A Spanish bank faced a large, cross-border litigation matter that required data to remain onsite. The case was highly sensitive in nature and involved personal and financial information.

**Challenge**
- Highly sensitive matter
- Data protection regulations requiring data to remain onsite
- Review attorneys in Spain and Brussels

**Goal**
- Protect the business’ private financial information
- Comply with data protection regulations
- Execute solution that meets time and budget requirements

**Approach**
- Map and identify data locations
- Use mobile ediscovery technologies to process data onsite
- Isolate proprietary, sensitive company data
- Utilize flexible technologies to review documents from multiple geographies while keeping data on premise
FCPA Investigation

Investigative work becomes increasingly complex when data in multiple locations and languages collides with data sensitivity and protection. Whether looking into corruption allegations or deciphering communications between parties, successful cross-border cases start with sound forensic collection and result in case facts being uncovered.

A Swiss pharmaceutical company involved in an Foreign Corrupt Practices Act (FCPA) investigation needed to collect data strewn throughout several locations in Indonesia and conduct in-region review of Bahasa-language documents by native speakers.

Challenge
- Multi-location data collection including encrypted laptops, mobile devices and email
- Mixed-language review set
- Need to review Bahasa-language documents with native speakers

Goal
- Uncover facts surrounding the alleged corruption
- Respond to government inquiries in a timely manner

Approach
- Deploy collection engineers to the various locations
- Determine who key players were talking to and when communications occurred
- Determine scope of non-English documents
- Separate non-relevant data from key documents
- Leverage in-region resources, for native review
Canada

Legal System
Common law system, except in Quebec, where civil law based on the French civil code prevails

Applicable Rules
Personal Information and Electronic Documents Act
Ontario Rule of Civil Procedure 29.1.03
The Sedona Principles Canada
Ontario Ediscovery Implementation Committee

Ediscovery Practices
The Canadian ediscovery community is close-knit, with increasing numbers of practitioners embracing new technology workflows with each new matter.

United States

Legal System
Common law

Applicable Rules
Federal Rules of Civil Procedure 26, 34, and 37

Ediscovery Practices
In a system known for broad discovery, the 2015 amendments to the Federal Rules of Civil Procedure have taken steps to address proportionality and unfettered discovery requests.

Brazil

Legal System
Civil law

Applicable Rules
The Federal Constitution contains privacy protections.
The Brazilian Code of Civil Procedure
The Civil Rights Framework (“Marco Civil da Internet”)

Ediscovery Practices
While there is no legal requirement to produce data in Brazilian litigation, data collection and processing protocols are sometimes adopted in regulatory matters, international arbitration issues, mergers and acquisitions, and out-of-country litigation extending into Brazil.

Spain

Legal System
Civil law

Applicable Rules
Data Protection Act (Law 15/1999)
EU Data Protection Laws

Ediscovery Practices
While Spain itself does not have a formal discovery requirement, there is legislation that demands data production in certain instances. Regulatory investigations also drive some of the ediscovery conducted in Spain.

France

Legal System
Civil law

Applicable Rules
French Blocking Statute (French Statute No. 68-678 of 26 July 1968 [as modified in 1980])
EU Data Protection Laws
Sapin II

Ediscovery Practices
A civil law system and strict data protections laws limit litigation-based ediscovery in France and complicate obtaining data for discovery in common law jurisdictions.
United Kingdom
Legal System
Common law
Applicable Rules
Civil Procedure Rules (Part 31 and associated Practice Directions)
Ediscovery Practices
Ediscovery is well practiced and judicial decisions on keywords, proportionality and predictive coding have been handed down over the past decade.

Netherlands
Legal System
Civil law
Applicable Rules
Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens (Wbp))
Dutch Telecommunication Act (Telecommunicatiewet, implementing Directive 2002/58/EC)
EU Data Protection Laws
Ediscovery Practices
Ediscovery demand is growing due to increased regulatory activity and Dutch companies taking a more proactive approach to compliance.

Nordics
Legal System
Civil law
Applicable Rules
EU Data Protection Laws
Country-specific privacy laws
Ediscovery Practices
With no formal litigation discovery requirements, most Nordic ediscovery is performed in compliance audits. The intricate privacy laws in the region complicate any multinational data processing.

Switzerland
Legal System
Civil law system; judicial review of legislative acts
Applicable Rules
Federal Data Protection and Information Commissioner ("FDPIC")
Ediscovery Practices
While limited by privacy laws and no legislative requirement, ediscovery is still developing in Switzerland.

Italy
Legal System
Civil law
Applicable Rules
Legislative Decree No. 196/2003, which contains the Italian Personal Data Protection Code (Code), EU Data Protection Laws
Ediscovery Practices
Although cautious about using new technologies, growing regulatory investigations are the driving force behind Italy's ediscovery market.

Belgium
Legal System
Civil law
Applicable Rules
EU Data Protection Directive 95/46/EC
The Data Protection Act of December 8, 1992 EU Data Protection Laws
Ediscovery Practices
On international cases, large corporations and global law firms located in Brussels are sophisticated users of ediscovery technology. On matters outside of Brussels, there is a greater need for education on the use of ediscovery technology.
China
Legal System
Based primarily on the civil law model
Applicable Rules
Chinese State Secrets laws
Chinese Counter-Terrorism laws
Cybersecurity Law
Ediscovery Practices
China does not have formal discovery practices in civil litigation. Further, the Chinese government has several regulations that impose possible restrictions on gathering data in China for an investigation or litigation. The most impactful regulation is the State Secrets law. Other ediscovery barriers in China revolve around language and culture, with the work culture in China being very family-oriented and controlled by personalized networks of influence and reciprocity.

Japan
Legal System
Based primarily on the civil law model
Applicable Rules
Japan’s Act on the Protection of Personal Information (APPI)
Personal Information Protection Commission (Japan’s data protection authority)
Ediscovery Practices
Japan is the most developed ediscovery market in the APAC region and continues implementation of the APEC Cross-Border Privacy Rules (“CBPR”) system in order to foster the protection of personal information transferred across borders.

Hong Kong
Legal System
Common law
Applicable Rules
Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) (Ordinance)
Practice Direction PDSL 1.2
Ediscovery Practices
Hong Kong is a global center of finance, with many banks, brokerages, private equity funds and other financial institutions based there. As such, demand for ediscovery in Hong Kong is largely driven by regulatory scrutiny. Hong Kong has also adopted limited procedures, which provide a framework for ediscovery that encourages parties to be reasonable, proportionate and cost-effective.

Singapore
Legal System
Common law
Applicable Rules
Personal Data Protection Act (PDPA)
Ediscovery Practices
Singapore is the first country in the APAC region to have opt-in ediscovery guidance written into legislation. Although this guide was introduced in 2009, companies and law firms have been slow to adopt ediscovery technology. Further, Singapore has the most recent and strictest data protection laws, and it is best if personal data does not leave Singapore.

Australia
Legal System
Common law
Applicable Rules
Federal Practice Note CM6 applies for federal courts.
State courts also have relevant ediscovery and predictive coding guidance: New South Wales Practice Note SC Gen 7 and Victoria Practice Note SC Gen 5.
Ediscovery Practices
Ediscovery demand is growing and Australians aspire to have an ediscovery system that takes the best from the United States and the United Kingdom.
United States

In December 2015, the Federal Rules of Civil Procedure were amended with the aim of putting a stronger lid on growing discovery. For example, the new version of the Rule 26(b)(1) contains a new emphasis on the need for proportionality in discovery and there has been a movement by the courts to use this rule to restrain unnecessary discovery. Given these new rules, U.S. legal practitioners are smart to make use of the latest ediscovery technologies, such as predictive coding and information governance platforms, to meet court deadlines and reduce expenses.

Canada

Ediscovery practices in Canada are quite similar to the processes, principles and goals of the United States and the United Kingdom. But, there is a general sense that Canada leads the global ediscovery community in terms of cooperation and proportionality. We attribute this to two things: (1) reforms by some provinces like Ontario, British Columbia and Alberta designed to narrow the scope of documentary discovery and provide increased judicial oversight of litigation plans, and (2) a close-knit Canadian ediscovery community with strong relationships between corporations, law firms and ediscovery providers.

Brazil

There is no legal requirement in Brazil to produce evidence like in the United States. Yet, change is creeping in, just like in other civil law jurisdictions. Companies are finding the benefit in using ediscovery technologies in certain legal and regulatory scenarios. In fact, when ediscovery technology has been used in Brazil, parties have found they gain advantage in legal proceedings by adding credibility to evidence and discrediting the opposing party’s evidence.
What Makes Ediscovery Unique?

United Kingdom
Unlike many of its European neighbors, edisclosure has been part of the United Kingdom’s Civil Procedure Rules for over a decade. During that time, practical know-how regarding ediscovery technology has spread beyond litigation, so most U.K. lawyers are comfortable with the advantages a full analysis of electronic evidence can bring to their case. However, with uncertainty brought about by Brexit, the new EU-U.S. Privacy Shield and the impending EU General Data Protection Regulation, there will be more scrutiny than ever on the holding of personal data and tougher penalties for mishandling personal data in the future.

Germany
As the world’s fourth largest economy, German companies or subsidiaries are often brought into cross-border disputes, usually involving the United Kingdom and the United States where ediscovery is required. What is unique is that German lawyers are using ediscovery technology to not only search and analyze data, but to discover material facts and redact personally identifiable information in accordance with Germany’s strict data protection laws. In addition, German companies are also closely regulated. Germany’s independent competition authority, the Bundeskartellamt, is one of the most active in Europe and has a reputation for its meticulous and demanding approach to investigations.

France
French litigators are not consistently familiar with ediscovery, since discovery is not a defined part of the French legal system. Apart from pure U.S. litigation, which happens from time to time when a French company is asked to produce evidence before a U.S. court, ediscovery tools and techniques mainly are used for internal investigations and fact-finding purposes. That means that most of the time, ediscovery is for internal use only and documents are not called to be disclosed to any other party.

Belgium
As the de facto capital of Europe and the formal center of the European Union, Belgium is at the core of European ediscovery, particularly investigation matters, even though it has no formal discovery requirement itself. Despite this, law firms based in Brussels work globally, whether it is a competition or litigation matter. They rely on sophisticated ediscovery technologies to not only help manage the significant volumes of electronic data, but also the many different languages that feature in each case.
Australia

While ediscovery is not as prevalent as in the United States or United Kingdom, Australia is no stranger to ediscovery. In fact, Australian lawyers at large firms have used home-grown as well as international ediscovery technologies for most of the last decade. The courts’ civil procedure rules, which are largely based on those of England and Wales, require parties to engage in discovery and court practice notes in one state recently embraced predictive coding protocols. Further, while Australia has data protection laws (such as the Privacy Act at the federal level), they are less stringent in comparison to other European or Asian countries.

Japan, Hong Kong & Singapore

Japan, Hong Kong and Singapore are geographically small countries, but each one is an important global economic power. Japan is the third largest economy by GDP, Hong Kong is a global center for banking and financial services, and Singapore has been ranked as one of the most open and pro-business economies in the world. However, in terms of ediscovery, all three countries are very much emerging markets, with Japan being the most developed ediscovery market in the APAC region. Although there is no formal ediscovery requirement in Japanese law, Japanese businesses and subsidiaries often involve U.S. and EU-based litigation and regulatory investigations.

China

Doing business in China comes with its own set of laws, practices and customs that often clash with foreign legal obligations. The conflict between China’s guarding of data and the demand from the United States or other countries for production make ediscovery in China a balancing act between accessing the necessary data for a case and complying with local laws. The state-owned sector dominates and onerous laws such as the State Secrets Law can be a burden for privately-owned companies operating in China. The status of China as a global economic giant combined with its complicated legal system has made it one of the newest and fastest growing ediscovery markets.
Major Milestones:
EU Data Privacy & Protection

There is a significant amount of uncertainty and upheaval with regards to the data privacy and protection landscape in the EU. How should U.S. in-house counsel and their law firms manage through this change?

All of this change leaves many legal professionals asking, “Data protection—new horizons or business as usual?” Until the implications of these new data protection regimes and the impact of Brexit are fully known, companies and counsel need to think carefully about the risks of transferring data across borders.

- **2000**: July: The EU issued the Safe Harbor Adequacy Decision, which created the “Safe Harbor Agreement” between the EU and the United States.
- **2011**: December: The first draft of the new EU General Protection Regulation (GDPR) disclosed.
- **2012**: January: Official draft of GDPR released.

In the late 1990s, the European Data Protection Directive was designed to protect personal data in a world that was becoming increasingly digital. As technology developed over the next decade, the need for a new law in the EU was realized, and thus a successor to the European Data Protection Direction, the EU General Protection Regulation (GDPR), was created.
In order to allow data transfers with United States, the EU entered into the “Safe Harbor Agreement” with the United States which allowed U.S. organizations to self-certify that they will provide privacy protections that meet the Directive’s standards when transferring personal data outside of the EU. However, in 2015, the Safe Harbor Agreement was deemed invalid. The replacement legislation, the EU-U.S. Privacy Shield, was finalized in July 2016, following protracted discussions and a rejected draft agreement.

**October:** European Court of Justice, in *Maximilian Schrems v. Data Prot. Commr* (Case C-362/14) declares “Safe Harbor Agreement” between the EU and the United States invalid.

**April:** GDPR finalized.

**July:** European Union adopts the new EU-U.S. Privacy Shield to replace Safe Harbor.

**May:** GDPR will be enforced.