Navigating Cross-Border Discovery and the GDPR

American Bar Association
Section of Taxation

Midyear Meeting
New Orleans, Louisiana
January 18, 2019

PANELISTS:
CHARLES E. HODGES II, JONES DAY, ATLANTA, GEORGIA
POLLY SPRENGER, KATTEN MUCHIN ROSENMAN, LONDON, U.K.
JOSEPH A. RILLOTTA, DRINKER BIDDLE & REATH LLP, WASHINGTON, D.C.
NATHANIEL PARKER, SENIOR COUNSEL, IRS ASSOCIATE CHIEF COUNSEL, WASHINGTON, D.C.
ROBERT KOVACEV, NORTON ROSE FULBRIGHT, WASHINGTON, D.C.

MODERATOR:
ARIELLE BORSOS, CAPLIN & DRYSDALE, WASHINGTON, D.C.
Topics

- Government Tools for Obtaining Foreign Records (pre-litigation)
- Cross-Border Discovery in Civil Litigation
- Cross-Border Criminal Investigations
- GDPR and Data Privacy Laws
- Asset Recovery Developments in English courts
IRS Summons under IRC § 7602

The summoned person must have:
- minimum contacts with the United States;
- “possession, custody, or care” of the information; and

The summons itself must be valid and enforceable under *United States v. Powell*, which the government can satisfy by showing that:
- The investigation is being conducted pursuant to legitimate purpose;
- The summons “may be” relevant to that purpose;
- The IRS does not already have the information it is seeking; and
- The IRS has followed the administrative procedures under the tax code.
Consent Directive

- A consent directive is a document signed by a taxpayer that authorizes and directs a specific foreign person (a bank, trustee, or other entity or individual) who possesses documents belonging to or controlled by the taxpayer, to disclose those documents to the IRS.

- Relevant when the IRS summonses a U.S. branch of a foreign bank or a U.S. bank with a foreign subsidiary and the bank claims that it cannot produce foreign records without violating the bank secrecy laws of the foreign jurisdiction.
  - A summons cannot be used to compel a taxpayer to sign a consent directive.
  - But, IRS can serve summons on taxpayer while in the US and a court may enforce the summons.

- A court may also issue an order forcing an account holder to authorize a foreign bank to disclose account information that otherwise may be protected by the foreign bank secrecy laws.

- Some foreign courts may not honor such directives because they do not constitute voluntary consent to disclosure.
Formal Document Request under IRC § 982

The taxpayer must either “substantially comply” with the FDR regarding foreign-based documentation or file a motion to quash the request within 90 days.

Failure to timely comply with this request will bar the taxpayer from using any foreign-based documents identified in the FDR in a civil tax case.

- Reasonable cause defense available for failure to comply.
- Foreign criminal or civil sanctions for disclosure of requested documents are not reasonable cause.
Tax Treaties-Exchange of Information Articles

A bilateral agreement between two countries with principal purposes of reducing or eliminating double taxation of income and preventing avoidance and evasion of income taxes of the two countries to the treaty.

Typically contains an Exchange of Information Article

- IRS and DOJ (through IRS) can use the treaties to obtain documents and conduct interviews of foreign persons.
- OECD standard: “information as is foreseeably relevant... to the administration or enforcement of the domestic laws concerning taxes of every kind and description imposed on behalf of the Contracting States.”
- Information received is confidential under IRC § 6105
Tax Information Exchange Agreements (TIEAs)

- A bilateral agreement between two countries that facilitates exchange of information for “tax-related purposes” between the countries.
- Typically used if there is no treaty.
- Information received is also confidential.
- TIEAs can be used in both civil and criminal matters, but most limit the use of tax information to only tax proceedings.
- Can be used to obtain foreign documents, including bank records, and testimony in admissible form.
Mutual Legal Assistance Treaties (MLATs)

• An agreement to gather and exchange information for criminal investigation, prosecution, and related matters.
  ◦ Can only be used by the government.
  ◦ Not all MLATs cover U.S. tax evasion.
  ◦ MLATs can override local laws pertaining to bank secrecy.

• MLATs typically contain provisions ensuring the admissibility of obtained evidence.

• U.S. has also entered into a Mutual Legal Assistance Agreements (MLAAs) with several countries, which are executive agreements that operate similar to MLATs.
Simultaneous Criminal Investigation Programs (SCIP)

- SCIP is a formal non-judicial arrangement between similar law enforcement agencies of two countries to share evidence with an objective of:
  - Conducting investigations of taxpayers involved in substantial tax violations in the U.S. and other countries, and
  - Eliminating taxpayers’ ability to use the border to avoid production of records and reporting of income

- United States has SCIP with several countries.

- May limit use of evidence to “tax administration.”
Hague Evidence Convention/Letter of Request

Hague Evidence Convention:
- Only applicable if a country ratified it;
- Provides methods of cooperation for obtaining evidence abroad in civil or commercial matters;
  - Certain countries do not consider administrative matters, such as Tax Court proceedings, to be a “civil or commercial” matter.
- Contracting state may limit the scope of available discovery;
- Evidence gathering is requested by Letter of Request and/or by diplomatic or consular agents and commissioners.

Letter of Request -- the evidence is obtained by foreign authorities pursuant to the request.
Letters Rogatory

◦ An avenue if there is no treaty or convention in place.
◦ A time consuming process in which a court of one country requests a court in another country for judicial assistance.
◦ Generally transmitted via diplomatic channels.
◦ In order to justify letters rogatory, litigation must be “within reasonable contemplation.”
◦ A foreign court is not obligated to act on a letter rogatory and only acts based on comity between the nations.
Considerations for Foreign Discovery in Litigation

Are there alternatives to Hague Convention/Letters Rogatory?

- Discovery may be obtained through ordinary discovery processes rather than Hague Convention - *Societe Nationale Industrielle Aerospatiale v. Iowa* U.S. District Court, 482 U.S. 522, 556 (1987)

- Trial courts should weigh interests of comity when ordering foreign discovery
  - Importance of documents to the case
  - Degree of specificity of request
  - Whether the information originated in the US
  - Availability of alternative means of securing the information
  - Weighing the interests of the US in compliance versus the foreign state in noncompliance
Considerations for Foreign Discovery in Litigation

- Documents under the control of a party may be requested through normal discovery means even if located abroad
- Tax Court can compel a foreign petitioner to produce documents and strike pleadings or dismiss case if documents are not produced – I.R.C. 7456(b)
- District courts have the same authority through Fed. R. Civ. P. 37(b)(2)(A) sanctions.
- 28 U.S.C. 1783 gives US courts jurisdiction to issue and enforce subpoenas against US nationals/residents in a foreign country if “necessary in the interests of justice”
- Subpoenas to US branch offices of foreign entities may result in compliance
- Review contracts with foreign counterparties for provisions requiring the sharing of information or cooperation in litigation
- Try to obtain foreign evidence through voluntary means whenever possible
Considerations for International Discovery in Litigation

Plan early in the case
- Hague Convention requests and Letters Rogatory may take months or even years
  - Notify the trial judge as early as possible in the case that foreign discovery will be an issue
  - Opposed motions for foreign discovery can slow the process down considerably
  - Your request will be at the bottom of the pile for the foreign ministry or local court
  - Enforcement may require local counsel in the foreign jurisdiction
  - Opportunities to challenge opponent’s request in foreign forum
  - Government has better luck than taxpayers in obtaining foreign discovery

Requests should be narrow
- US trial judges more likely to approve requests that are narrowly tailored and concern important issues in the case
- Most countries have limited or no civil discovery
  - Some countries explicitly reserved pretrial discovery from their accession to the Hague Convention
  - “All documents concerning…” type requests may not be enforced
  - Requests for specific documents or narrow categories more likely to be enforced
Considerations for International Discovery in Litigation

Obtaining testimony may be challenging

- Some countries (e.g., Germany) forbid the taking of depositions on their soil
  - May have to take place at the US Embassy, or in a third country
- Many foreign courts (esp. in civil law jurisdictions) may be reluctant to enforce requests for depositions, particularly if the purpose is discovery as opposed to preserving testimony for trial
  - May have to submit written questions with treaty requests or letter rogatory
- Procedures for depositions may be unusual (e.g., a judicial officer presiding at the depo)
  - Even finding a qualified court reporter may be problematic in some jurisdictions
  - Using a translator makes a deposition much slower and more cumbersome
- Can get depositions in criminal as well as civil cases – Fed. R. Crim. P. 15.
  - Defendant need not be present in certain circumstances – Fed. R. Crim. P. 15(c)(3)
Considerations for International Discovery in Litigation

Make sure the documents you obtain are admissible
- Fed. R. Evid. 902(3) certification for foreign public records
- Fed. R. Evid. 902(12) declaration for business records
- What is the foreign equivalent of “upon penalties of perjury”
- Residual hearsay/authenticity arguments are a last resort

Seek discovery on documents the other party may have received from overseas (e.g., treaty requests at the audit stage)

Resources:
Hypothetical

You represent Taxpayer ABC Corp. ABC entered into an agreement with XYZ Ltd., a foreign entity for sale-leaseback of power plant XYZ owns in its home jurisdiction. The foreign jurisdiction is a party to the Hague Convention but reserved from the article permitting pretrial discovery. XYZ has no US presence, but it used a law firm with offices in Manhattan for the transaction and its executives regularly visit the US for business. The IRS challenged ABC’s claim for depreciation deductions for the plant, alleging the sale-leaseback transaction lacked economic substance. You believe XYZ has important documents showing that the transaction had a non-tax business purpose, and you also believe that XYZ executives would provide helpful testimony. XYZ has not responded to informal requests for these documents or for a deposition of its executives.
Judicial Redress Act of 2015 ("JRA")

The JRA extends certain rights under the U.S.’s Privacy Act of 1974 (5 U.S.C. § 552a) to “covered persons” from “covered countries”.

What are the “covered countries”?

◦ The JRA implements the Data Protection and Privacy Agreement ("DPPA"), entered into between the U.S. and the European Union and finalized on December 2, 2016.

◦ The JRA initially covered every E.U. country except three, which reserved to opt out of the DPPA: Denmark, Ireland, and the United Kingdom.

◦ Ireland subsequently joined, and is now a covered country.

◦ Denmark and the U.K. still are not covered countries.

◦ The E.U. has enacted effectively reciprocal privacy provisions covering US citizens.
Judicial Redress Act of 2015 ("JRA")

Who is a “covered person”?

- A natural person (*i.e.*, an individual) who is a citizen of a “covered country”...
- ... And who is not a U.S. citizen or legal permanent resident.

What Privacy Act rights are extended to “covered persons”?

- The right to bring civil suit against a U.S. agency regarding the intentional or willful unlawful disclosure of records maintained by such agency, including financial and medical records, employment and criminal history, *etc.*
  
  (5 U.S.C. § 552a(a)(4), (g)(1)(D))

- The right to bring suit against a U.S. agency** regarding the improper refusal to allow access by the covered person to records pertaining to him/her, or to permit amendment of such records under established procedures.
  
  (5 U.S.C. § 552a(a)(1)&(2), (g)(1)(A)&(B))
JRA Limitations

JRA rights for foreign “covered persons” are subject to the same limitations as Privacy Act rights for U.S. individuals: e.g., no access to law-enforcement-sensitive information.

There are other more restrictive limitations under the JRA. For example:

- Suits for improper refusal to access/amend records may only be brought by covered persons against “designated” U.S. agencies or agency components.
  - These include: DOJ, DHS, SEC, IRS-CI, OFAC, and TIGTA.
  - Agency designations are to be made by DOJ pursuant to relevant international agreement, with the agency head’s consent.
  - JRA suits may only be brought in the U.S. District Court for the District of Columbia.
Expansion of the JRA’s Scope

The JRA can, at least theoretically, apply beyond the DPPA and E.U.

DOJ can add a “covered country (-ies)” if it determines (with the concurrence of State, Treasury, and DHS):

- That a country or regional organization, either by virtue of formal agreement or pattern and practice, both (a) “effectively” shares information for law enforcement purposes, and (b) affords “appropriate” privacy protections.
- That such country/-ies generally permit the transfer of personal data to and from the United States for commercial purposes.
- That such country’s/ -ies’ policies regarding the transfer of personal data for commercial purposes do not materially impede U.S. national security interests.

DOJ (again with the concurrence of State, Treasury and DHS) can remove a country from the “covered countries” list if it determines that the above requirements are no longer met.
Practical Considerations for Cross-Border Criminal Investigations

Be mindful that, relative to the U.S., other countries may have more expansive, or more restrictive, procedural protections. For example:

- Some countries allow for more robust investigation-phase discovery, even beyond JRA/DPPA-type access. In some countries, the “accused” (akin to U.S. grand jury “targets”) have some access to the government’s investigative file.

- However, some countries take a more limited approach to the privilege against self-incrimination, and/or have higher thresholds for its assertion.

- Some countries take a more restrictive view of the attorney-client privilege and attorney work-product protection, at least in the criminal investigation context.

- Many countries do not have an exclusionary rule or a robust “fruit of the poisonous tree” doctrine.

Cross-border information-sharing can potentially taint U.S. investigations, or raise other constitutional issues.
Use of Evidence Obtained in Violation of Foreign Law

“One-Bite” Rule: The U.S. government can legally use information received from a private party even if such information was obtained illegally or illicitly, so long as the government is solely a passive recipient.

- See IRS Chief Counsel Notice CC-2008-011 (citing Burdeau v. McDowell, 256 U.S. 465 (1921)).

If the U.S. government is actively involved in obtaining foreign evidence, the Fourth Amendment reasonableness standard applies, at least with respect to the conduct of U.S. officials in such searches and seizures.

- See United States v. Juda, 46 F.3d 961 (9th Cir. 1995); United States v. Getto, 729 F.3d 221 (2d Cir. 2013).

If evidence was otherwise obtained in violation of foreign law, such evidence can generally be used by the U.S. government.

- But not if evidence was acquired in a manner that shocks the judicial conscience, or if U.S. cooperation with foreign law enforcement implicates separate constitutional restrictions. See United States v. Getto, 729 F.3d 221 (2d Cir. 2013); United States v. Peterson, 812 F.2d 486 (9th Cir. 1987).
Use of Evidence Obtained in Violation of Foreign Law

The Fourth Amendment does not apply to a search by U.S. agents of property owned by a non-resident alien and located in a foreign country.


A defendant lacks **standing** to suppress evidence illegally seized from a third-party (e.g., his/her bank or banker), because the defendant has no operative privacy interest in the documents and records of third-parties (even if the records are his/her bank records).


- Query whether this case law survives the international proliferation of privacy rules like the DPPA and GDPR.
Information Exchange Mechanisms for Financial Account Information

DOJ’s **Swiss Bank Program** of 2013-14
- Limited “amnesty” program effected by bilateral negotiation.
- Swiss banks produced information to DOJ, with the blessing of their regulators.
- Other jurisdictions to follow?

**FATCA**: A Foreign Financial Institution (“FFI”) or its local government must enter into a FATCA disclosure agreement with the IRS or else subject to 30% withholding of U.S.-source income going to the FFI.
- Required disclosures aimed at identifying U.S. accounts in foreign jurisdictions.

**OECD’s Common Reporting Standard (“CRS”)**
- Member countries of the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes (including the U.S.) are committed to participating in automatic exchanges of information covered by the CRS.
Between a Rock and a Hard Place

What if you receive a discovery request from U.S. investigators requiring you to produce information in violation of foreign law?

◦ Faced with such a grand jury subpoena, one option would be to move to quash under Fed. R. Crim. P. 17(c)(2), on the grounds that it would be “unreasonable or oppressive” to require the subpoena recipient to violate foreign law, especially in its home jurisdiction, where it or its affiliates may be subject to prosecution or regulatory consequence.

◦ This is what “Company A” recently argued (under seal) in the Mueller Investigation. See In Re Grand Jury Subpoena, Case No. 18-3071 (D.C. Cir. Dec. 18, 2018). Supreme Court review is pending.

◦ Presumably, a similar argument could be made for an IRS summons under United States v. Powell, 379 U.S. 48 (1964).

◦ These arguments could put U.S. courts in the position of interpreting, e.g., the GDPR.
Data Privacy: What is it?

- A multinational enterprise (MNE) conducts business and executes transactions throughout the world over the internet, telephone, social networks, texts, and even via facsimile.
- The correspondence transmitted by the MNE could contain information on the company’s employees, competitors, and global partners.
- This correspondence may contain sensitive “personal data”.
- In a general sense, data privacy and data security deal with the collection, storing, and disclosure of personal information.
- And to the extent the MNE has a significant presence in a particular country (or state), the MNE may find itself subject to data protection laws of that country (or state).
In the EU, “personal data” is broader and usually refers to any information that relates to an identified or identifiable person. According to the EU, personal data can include:

- a name and surname
- a home address
- An e-mail address referencing a specific name: cehodges@jonesday.com
- An identification card number
- Location data
- IP address
- Data held by a hospital or doctor

Personal data usually does not include a company’s EIN or a company’s general e-mail address: info@jonesday.com
Data Privacy Laws

• Many data privacy laws focus on whether data can be legally collected and stored as well as shared with third parties, such as the IRS.

• Data privacy laws regulate collection and use of personal data.

• In many instances, an employer cannot rely upon the consent of an employee for the collection and distribution of personal data based on the perceived unfair balance in the employer-employee relationship.

• In many instances, e-mails and other correspondence possessed by a MNE contain personal data of employees around the world.

• Laws or guidelines can be imposed at the federal, state, as well as industry-specific level regarding the collection, storage, and disclosure of personal data.

• The penalties for violating privacy laws are generally severe.
General Data Protection Regulation (GDPR)

• Most significant change in EU data protection law in 20 years
• GDPR is a switch from a Directive (need national laws) to a Regulation (direct effect)
• GDPR replaced EU Data Protection Directive on May 25, 2018
• Applies to all companies across all industry sectors – in and outside the EU
• “Demonstration of compliance” will be key from a management perspective
• Sanctions increase to 4% of annual worldwide turnover
GDPR cont.

GDPR applies to:
- EU established entities where personal data processed “in the context of its activities”
- Other entities where:
  - An EU resident’s personal data is processed in connection with **goods or services offered** to such EU resident; or
  - The **behavior** of individuals within the EU is **monitored**.
GDPR, cont.

The principles of data processing include (i) lawfulness, (ii) fair processing, (iii) transparency, and one of a list of conditions are satisfied:

- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity & confidentiality
- Accountability

Controller must have legal basis for data processing, including either consent, performance of contract, compliance with legal obligation, vital interest of individual, public interest, or “legitimate interest”.
GDPR, cont.

The key issues under GDPR include:
- Information obligations
- Accountability and record keeping
- Data Protection Officer
- Third party processing agreements
- Privacy by design
- Data Protection Impact Assessments

Customers/employees/vendors have rights under GDPR such as:
- Right of access to data
- Right to rectification & right to erasure
- Right to restriction of processing
- Right to data portability
- Right to not be subject to automated decision making
GDPR International Data Transfers

General prohibition of data transfers to countries outside the EU, when safeguards are in place:

◦ Adequacy decision of European Commission (Andorra, Argentina, Canada (where PIPEDA applies), Switzerland, Faero Islands, Guernsey, Israel, Isle of Man, Jersey, Uruguay and New Zealand)

◦ EU Standard Contractual Clauses

◦ Binding Corporate Rules (intra-group data transfers)

◦ For the US: EU-U.S. Privacy Shield

◦ Approved Code of Conduct or Certification mechanism

◦ Derogations (consent, contract, establish legal claims)

Data disclosure request by non-EU authority only enforceable if based on international agreement such as mutual legal assistance treaty
Who is Covered by GDPR?

- Common misconception that GDPR protects all EU citizens, regardless of physical location.
  - Not so. GDPR Protects individuals located within the EU at the time data is collected and processed.
- Applies to controllers and processors based outside the EU territory where the processing of personal data regarding EU data subjects relates to:
  - the offering of goods or services (regardless of payment)
  - the monitoring of data subjects’ behavior within the EU
- Penalties for breach of GDPR – up to higher of 4% global turnover or €20,000,000
- Personal data must processed fairly and lawfully, with legitimate purpose
- Controllers and processors will be directly liable under GDPR
What is personal data under GDPR?

◦ “Personal Data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

◦ Updated private notices

◦ **Data protection impact assessment**: prior to processing if high risk for individuals

◦ **Data Protection Officer**: for controllers/processors processing substantial sensitive personal data or who have core activity of monitoring individuals on a large scale or public body

◦ Notify data breach to DPA without undue delay/within 72 hours and to individuals without undue delay if there is likely to be risk to individuals

◦ Consent standard higher: explicit, freely given, fully informed
  ❖ Consent given in the context of employment is **not** considered “freely given.”
GDPR Summary

New system for regulatory oversight
- One Stop Shop with lead data protection authority (DPA) for pan-European/international matters – involvement of other DPAs
- Local DPAs for local matters

Broader scope of application
- Extraterritorial application to non-EU based companies
- Broader definition of personal data and sensitive data, new data categories

Focus on accountability, governance
- Information obligations
- Data protection by design
- Data security and data breach notification
- Data processor agreements
- Data Protection Officer
- International data transfers
- Code of Conduct/Certification
- Documentation

Strengthened rights of individuals
- Right to access
- Right to deletion
- Right to data portability
- Right not to be subject to automated processing, including profiling
- Right to object

Increased enforcement, fines, liability
- Administrative fines up to 2% or 4% of annual worldwide turnover
- Individual actions, claims for damages
- Collective actions
- Criminal sanctions (in national laws)
GDPR Examples

- GDPR “applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.” GDPR Art 3(1).

- **Example:**

  A car manufacturing company headquartered in the US wholly- owns a branch/office in Brussels overseeing European operations, including marketing and advertisement.

  The “Belgian branch could therefore be considered as an establishment in the Union, within the meaning of the GDPR.” GDPR Guidelines, 1.a.

- Result could be different “in the absence of any representation or stable arrangement in the EU.”

- The data processing need not be carried out by the EU establishment; the controller or processor will be subject to GDPR wherever the processing occurs.
Mexican Data Privacy Laws

- The protection of personal data is a fundamental right contained in the Mexican Constitution.
- Every individual has the right to the protection of their personal data and the right to access, rectify, oppose and cancel personal data.
- The Mexican laws contain a specific scope of protection depending on the type of organization or individual responsible for gathering and storing the information or data (data controller).
- If personal data gathered and stored by a private organization or private individual the organization or individual must comply with the Federal Law of Protection of Personal Data held by Private Parties, effective as of July, 2010 (FLP of 2010).
- The FLP of 2010 governs how companies and individuals collect, use, store, protect, and manage personal data internally as well as the sharing of the information with third parties.
Redaction of Personal Data

- In many instances, the document requested may have to be turned over to the IRS, but the personal data may have to be redacted.
- For example, the Swiss Federal Supreme Court held that the names of bank employees and other third parties had to be redacted before being turned over to the IRS. The IRS had requested the information regarding Swiss bank accounts of US taxpayers. Decision 2C_640/2016.
- Redactions should be made similar to those communications that fall within the attorney-client privilege.
Examples of Redactions of Personal Data in Other Contexts

**Court filings**
- Federal Rules of Civil Procedure requires the following information be redacted from any filing with a federal court:
  - Social Security Number (last 4 digits is allowed)
  - An individual’s taxpayer identification number (last 4 digits is allowed)
  - Birth date (year of birth is allowed)
  - The name of a minor
  - A financial account number (last four digits is allowed)

Fed. R. Civ. P. 5.2(a)

**Mergers and Acquisitions**
- Where the submission of documents to a regulator is required prior to a merger or acquisition, sensitive PII must be redacted.
- The FTC’s instructions for production of documents states “Do not produce any Sensitive Personally Identifiable Information (“Sensitive PII”) or Sensitive Health Information (“SHI”) prior to discussing the information with a Commission representative. If any document responsive to a particular Specification contains unresponsive Sensitive PII or SHI, **redact** the unresponsive Sensitive PII or SHI prior to producing the document.”

Best Practices

Before producing documents to the IRS:
  ◦ Consider what personal data taxpayer possesses

Implement a collection and review protocol
  ◦ Include safeguards to protect personal data
  ◦ Instructions on redacting: what to redact and how to redact

If you rely on vendors, make sure you have an adequate data security agreement in place that:
  ◦ Restricts the vendor’s use of your data
  ◦ Requires the vendor to maintain reasonable technical and administrative safeguards to protect your data.
  ◦ Gives you the right to audit

Follow a strict collection and review protocol
Sources of Authority

Guidelines of the European Data Protection Board

UK.practicallaw.thomsonreuters.com

“Resolving Data-Privacy Conflicts in Cross-Border Investigations and Litigation,” Callaghan, ABA Section of Labor and Employment Law, Boston, MA meeting, August, 2014.
Overview

- Identify Assets
- Obtain Evidence
- Provenance and validate
- Enforcement and Recovery
Asset recovery tools – civil parties

Domestic Freezing Order (WFO)

Norwich Pharmacal Order (NPO)

Worldwide Freezing Order (WFO)

European Account Preservation Order (EAPO)

Civil

CPR 25.1(1)(g)
Asset recovery tools – law enforcement

Account Monitoring Orders (s370 Proceeds of Crime Act 2002)

Restraint Orders (s40 Proceeds of Crime Act 2002)

Unexplained Wealth Orders (UWO)*

Civil Recovery Orders (s243 Proceeds of Crime Act 2002)*
CIVIL ACTIONS
Norwich Pharmacal Order (1)

A NPO enables a claimant to seek disclosure from third parties to a dispute.

They are often sought to obtain information relating to the whereabouts of assets and applications are typically made against a defendant’s bank for disclosure of:

- banking records;
- statements; and
- other correspondence.

*(see Bankers’ Trust Company v Shapira [1980] 1 WLR 1274)*

They are usually made without notice and before proceedings commence in order to prevent further dissipation of assets.

**NEW: the extension of the NPO jurisdiction**
Norwich Pharmacal Order (2)

The Applicant must show:

- Good arguable case
- No other CPR provision could apply
- Respondent is likely to have relevant documents or information
- Respondent is involved or mixed up in wrongdoing
- Respondent is a mere witness
- The order is in the interests of justice
Domestic Freezing Order (1)

A device to restrict a defendant from dealing with his assets within the UK.

Court has jurisdiction to grant a freezing order pursuant to s37 Senior Courts Act 1981.

Types of asset over which an order can be obtained include:

- Bank accounts
- Credit cards
- Property, vehicles etc
- Furniture/personal antiquities
Domestic Freezing Order (2)

Freezing Orders will only be granted where the following conditions are met:

- The Applicant will also be required to make a cross-undertaking in damages.
- Court has jurisdiction
- Just and convenient to grant the order
- Good arguable case
- Underlying cause of action
- Real risk of dissipation
- Assets within the jurisdiction
Worldwide Asset Freezing Orders

The court may grant a Freezing Order that extends to assets located anywhere outside of the UK (i.e. a WFO).

Applicant must demonstrate that the Respondent (1) does not have sufficient assets within the jurisdiction to satisfy the claim and (2) has assets outside of the UK.

Once WFO has been obtained, the Applicant must apply to the courts of the jurisdiction where assets are located to enforce the WFO.

In certain circumstances, the court has been willing to grant a WFO against persons unknown (fraud claim – CMOC v Persons Unknown [2017] EWHC 3599 (Comm)).
European Account Preservation Order (“EAPO”)

A device to assist a creditor in freezing funds held within a bank account held by a debtor located within participating Member States of the EU.

Creditors apply by submitting a standard form application (without notice).


The UK and Denmark has opted out of EAPOs – so it will not be possible for (1) a UK claimant to obtain an EAPO in the UK, or (2) an EAPO to be obtained over a UK bank account.

However, a UK business could find itself subject to an EAPO where it has a bank account located in a Member State of the EU (other than Denmark).
CPR 25.1(1)(g)

Pre- or post-freezing order application for disclosure

The court can exercise its power under CPR 25.1 (1) (g) if:

1. there are, or may be, assets which would form the subject of a freezing injunction; and
2. it is just and appropriate to grant the relief in the circumstances.

Lower threshold than when pursuing a freezing order—would require respondent to disclose assets exceeding a certain value.

Also mechanisms under CPR 31.16 and CPR 31.17
Extension to the tort of “unlawful means conspiracy”

Assisting the subject of a freezing order to “evade its impact” can be a stand-alone cause of action in civil proceedings [16].

Claimant obtains freezing injunction against defendant.

Defendant breaches freezing injunction and is found to be in contempt of court.

Third party assisted the defendant in committing that breach.

Claimant may recover loss from third party by way of action in the tort of conspiracy.

Actions of defendant and third party have caused claimant a loss.
CRIMINAL ACTIONS
Unexplained Wealth Order (1)

A mechanism to confiscate the proceeds of crime introduced by s1 Criminal Finances Act 2017.

UWO requires the respondent to:

- Set out the nature of his interest in respect of property to which the order relates
- Explain how he obtained the property
- Set out the details of any trust settlement holding the property
- Set out such other information as specified in the Order
An “enforcement authority” (NCA, SFO, FCA, CPS, HMRC and police forces) can make an application to the High Court for a UWO.

A UWO can be made in respect of any property and without notice.

**Requirements:**

1. Respondent holds the property
2. Value of the property greater than £50,000
3. Reasonable grounds for suspecting known source of respondent’s income would have been insufficient for the purposes of obtaining the property
4. Respondent is either a politically exposed person or there are reasonable grounds to suspect (i) he is, or has been, involved in serious crime in the UK or elsewhere or (ii) a person connected to the Respondent has been so involved.
Civil Recovery Orders

Part 5 POCA 2002 – enforcement authorities (SFO, NCA and CPS) can bring civil proceedings to recover property obtained through unlawful conduct.

Court will decide on the balance of probabilities whether unlawful conduct occurred.

The effect of a CRO is:

- Interim receiver appointed
- Property detained
- Ongoing civil recovery investigation ceases
- Respondent prevented from dealing with property
Restraint Order (1)

The Crown Court can exercise its power to grant a Restraint Order in the following circumstances:

1. Criminal investigation has started
2. Proceedings for an offence have started but not concluded
3. An application by the prosecutor has been made under s19, 20, 27 or 28 POCA 2002, or the court believes it will be made
4. An application by the prosecutor has been made under s21 POCA 2002, or the court believes it will be made
5. An application by the prosecutor has been made under s22 POCA 2002, or the court believes it will be made

For (1) – (3) the court must also reasonably believe the defendant has benefitted from his criminal conduct.
Similar to a Freezing Order, but permitted expenditure by the defendant following the grant of the Restraint Order is usually significantly lower than under a civil Freezing Order.

Application can be made by any prosecutor—including private prosecutors.
S370 POCA 2002 allows an appropriate officer to apply to the court for an order requiring the provision of information relating to specified accounts held by an identified person for a period not exceeding 90 days.

There must be reasonable grounds for believing that the account information is likely to be of substantial value to the investigation.

An application for an account monitoring order can be made without notice.

**A private prosecutor cannot obtain an account monitoring order—NPO can be used as an alternative.**
INVESTIGATIONS POST GDPR
The General Data Protection Regulation ("GDPR") has been in force since 25 May 2018.

GDPR introduces significant fines for non-compliance — up to EUR 20 million or 4% of global annual turnover.

It applies to all organisations whose processing activities relate to offering goods or service within the EU.
Key principles of GDPR

**Art 5(1):** Personal data shall be:

- processed lawfully, fairly and transparency
- collected for a specified and legitimate purpose;
- accurate and up to date;
- kept for no longer than is necessary; and
- processed in a manner than ensures security.

**Art 6:** there must be a lawful basis for obtaining and using the personal data. In addition, the processing must be “necessary”. 
How does GDPR impact investigations? (1)

**Cross-border investigations:**
- Transmission of evidence outside the EU - ensure Data Transfer Agreement in place

**External investigations:**
- Ensuring third parties comply with GDPR obligations
- Covert surveillance

**Internal investigations:**
- Record keeping in investigations: data subject access request
- Surveillance of employees subject to investigation: data privacy impact assessment

**GDPR**
How does GDPR impact investigations (2)

Organisations which plan to carry out internal investigations into the conduct of their employees or agents should carry out a data protection impact assessment ("DPIA").

DPIA where:

- systematic and extensive evaluation of personal aspects (i.e. profiling, criminal convictions, use of CCTV)
- Likely to result in high risk to rights and freedoms of natural persons (i.e. covert monitoring)
How does GDPR impact investigations (3)

Organisations should consider:

- Nature and scope of investigation
- Reason(s) why an individual is being pursued
- Necessity and proportionality of the measures
- Impact on individual’s privacy