INVESTIGATION · LAW, ETHICS AND REGULATION

Cross-Border and Transnational Investigation Challenges and Knowledge Sharing

Crime, corruption, fraud and data now cross borders routinely, but investigative powers stop at them. This article examines the challenges of transnational investigation, the legal routes for obtaining evidence abroad, the special problems of digital evidence held by global providers, models of international cooperation, and practices that make cross-border knowledge sharing work.

ModQu research article · 2,690 words · 28 references (APA 7th edition)

A fraud is planned in one country, carried out through websites hosted in a second, paid through banks in a third and laundered through companies registered in a fourth. A company bribes officials abroad. A survey platform holds respondent data on servers in several jurisdictions. A war crime is recorded on a phone and posted on a platform based on another continent. Modern wrongdoing, and much modern evidence, crosses borders as a matter of course. Investigative powers, however, are territorial. A police officer, regulator or court in one country generally cannot compel people, search premises or seize data in another. Transnational investigation is the effort to bridge this gap. This article examines its main challenges, the legal routes available, the special case of digital evidence, the models of cooperation that have developed, and the practices that make knowledge sharing across borders work.

Why borders matter

Sovereignty means that each state controls law enforcement within its territory. An investigator who needs evidence from abroad must usually ask the other state to obtain it, and that state will apply its own law, procedures and priorities. Nadelmann (1993) documented how the United States built up an extensive international law enforcement presence over the twentieth century, through liaison officers, treaties and informal networks, precisely because domestic powers could not reach the evidence and offenders that mattered. Andreas and Nadelmann (2006) describe how states have progressively harmonised criminal laws and built cooperation mechanisms in response to transnational crime, while each retaining control over its own territory.

Differences between legal systems create further obstacles. An act may be a crime in one country and not in another, and many cooperation mechanisms require "dual criminality", meaning the conduct must be an offence in both. Rules on evidence, privacy, privilege, the rights of suspects and the use of covert methods differ. Evidence lawfully gathered in one country may be inadmissible in another. Bowling and Sheptycki (2012) describe the resulting landscape of global policing as a patchwork of formal and informal arrangements, with uneven accountability.

Formal routes for obtaining evidence

Mutual legal assistance. The traditional route is a formal request from the authorities of one state to another, under a bilateral treaty, a multilateral convention or the principle of reciprocity. The request is usually sent through central authorities, reviewed for legal compliance, and executed by the receiving state's authorities, who then send the evidence back. Multilateral conventions, such as the United Nations Convention against Transnational Organized Crime (2000) and the United Nations Convention against Corruption (2003), oblige parties to provide wide mutual legal assistance and allow requests to be made in the absence of a bilateral treaty.

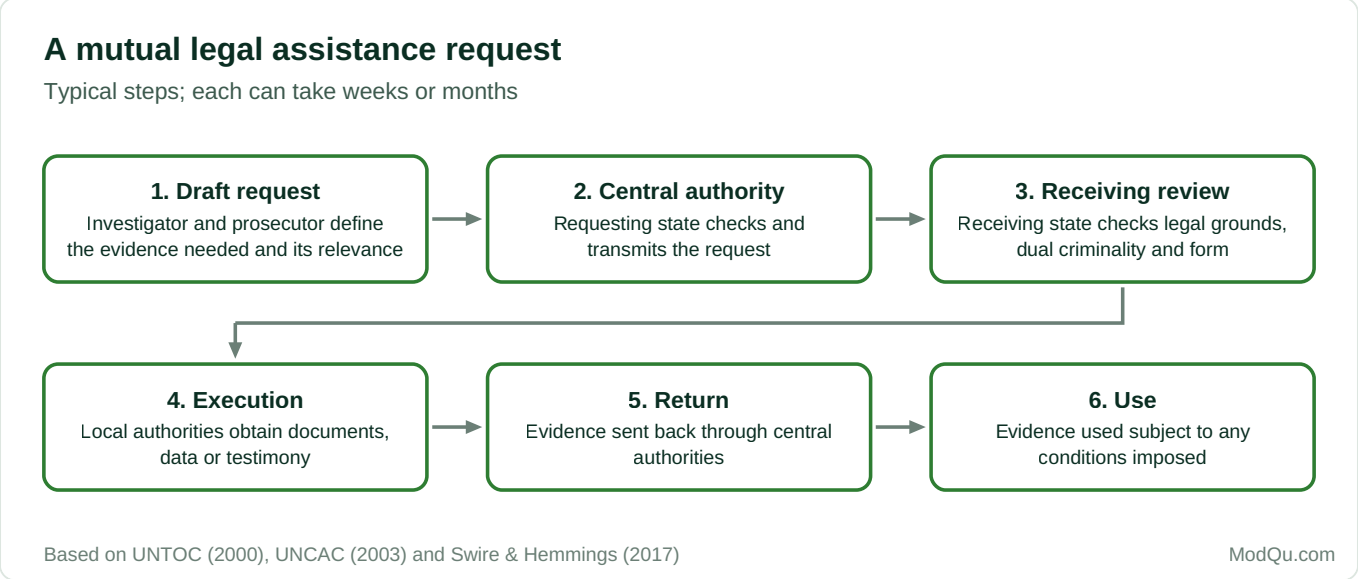


Figure 1. The main steps of a formal request for evidence from another state. The process protects sovereignty and legal rights but is slow, which is why faster routes have been developed for urgent and digital evidence. Diagram by ModQu.

Mutual legal assistance is reliable but slow. Swire and Hemmings (2017) found that requests to the United States for electronic communications typically took around ten months to complete, a delay that is often fatal to investigations of fast-moving online crime.

Mutual recognition in the European Union. Within the European Union, mutual recognition has largely replaced traditional requests. The European Investigation Order allows a judicial authority in one member state to issue an order for an investigative measure, such as a search or witness hearing, which the authority in another member state must recognise and execute within set time limits, subject to limited grounds for refusal (Directive 2014/41/EU of the European Parliament and of the Council, 2014).

Joint investigation teams. For complex cases, two or more states can form a joint investigation team for a specific purpose and period. Members work together and can share information and evidence directly, without formal requests for each item (Council Framework Decision 2002/465/JHA, 2002). Joint teams have been used extensively against trafficking, drug smuggling and cybercrime.

Police-to-police cooperation. Much information flows informally between police services, through liaison officers, Interpol notices and channels, and agencies such as Europol. Such exchanges are fast but usually provide intelligence rather than evidence usable in court. Deflem (2002) and Gerspacher (2008) trace how professional police networks developed over more than a century, often running ahead of formal legal arrangements.

Financial intelligence. Financial intelligence units in different countries exchange information about suspicious transactions through international networks, supported by standards set by the Financial Action Task Force (2012), which require countries to provide rapid and constructive international cooperation in money laundering cases.

Routes for obtaining information from abroad

Faster routes usually yield intelligence; slower routes yield court-ready evidence

	Typical speed and output	Main limitation
Police-to-police channels	Days; intelligence and leads	Often not usable as evidence
Financial intelligence exchange	Days to weeks; financial leads	Use restricted; needs formal follow-up
Mutual legal assistance	Months; admissible evidence	Slow; dual criminality and form requirements
European Investigation Order	Weeks to months within the EU	Limited to EU member states
Joint investigation team	Ongoing; shared evidence and intelligence	Effort to set up; needs aligned priorities
Direct requests to providers	Days to weeks; subscriber and content data	Depends on provider policy and legal framework

ModQu analysis of sources cited in this article ModQu.com

Figure 2. The main routes for obtaining information held abroad, and the trade-off between speed and evidential value. Investigators often use fast routes to identify what exists and formal routes to obtain it as evidence. Diagram by ModQu.

Digital evidence and global providers

Digital evidence poses the sharpest cross-border challenge. Emails, messages, cloud files and account records are often held by a small number of global companies, stored in data centres in several countries, and moved between them for technical reasons. Daskal (2015) argued that data's mobility and divisibility make territorial rules a poor fit: the location of data is often arbitrary and may change from moment to moment, yet traditional law makes access depend on it.

The problem came to a head in a dispute between Microsoft and the United States government over emails stored in Ireland. A federal appeals court held that a United States warrant could not compel Microsoft to produce data stored abroad (*Microsoft Corp. v. United States*, 2016). Before the Supreme Court could decide the appeal, Congress passed the

Clarifying Lawful Overseas Use of Data Act (2018), which clarified that United States providers must produce data in their control regardless of where it is stored, and created a framework for agreements under which qualifying foreign governments can request data directly from United States providers. The Supreme Court then dismissed the case as moot (*United States v. Microsoft Corp.*, 2018).

The Council of Europe's Convention on Cybercrime (2001) established common offences and procedural powers for computer-related crime and a framework for rapid cooperation, including preservation of data while a formal request is prepared. The European Union has adopted rules allowing judicial authorities to issue orders requiring service providers offering services in the Union to produce or preserve electronic evidence directly, wherever the data are stored (Regulation (EU) 2023/1543, 2023).

Privacy law complicates the picture. In *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* (2020), the Court of Justice of the European Union invalidated the main framework for transferring personal data from the EU to the United States because United States surveillance law did not provide equivalent protection. The ruling illustrates that cross-border access to data involves not only cooperation between investigators but also the rights of the people whose data are sought, and that arrangements acceptable in one legal system may be unlawful in another.

Suspects, witnesses and assets abroad

Evidence is not the only thing that crosses borders. Suspects may live in or flee to another country, witnesses may be scattered across several, and the proceeds of wrongdoing are often moved abroad quickly.

Suspects. Bringing a suspect to trial usually requires extradition, a separate legal process in which the requested state's courts examine whether the request meets treaty and domestic requirements. Many states do not extradite their own nationals, and extradition may be refused where the requested state considers that the suspect would face an unfair trial or inhumane treatment. Multilateral conventions require parties that refuse to extradite their own nationals to submit the case to their own prosecutors instead (United Nations Convention against Transnational Organized Crime, 2000). Investigators therefore need to consider early where any eventual trial is likely to take place, because that determines which country's evidential rules the investigation must satisfy.

Witnesses. Interviewing witnesses abroad raises questions of permission, language and procedure. In many countries, foreign investigators may not question witnesses without the consent and sometimes the presence of local authorities. Interpreters must be competent in the relevant dialect as well as the language, and interview methods that are standard in one country may be unfamiliar or even unlawful in another. Video links can reduce cost and delay, but the receiving state's rules on oaths, recording and the presence of lawyers still apply.

Assets. Following money across borders is often the most effective way to identify those behind transnational crime and corruption, and recovering it is often a central aim. The United Nations Convention against Corruption (2003) devotes a full chapter to asset recovery, requiring parties to cooperate in tracing, freezing, confiscating and returning the proceeds of corruption. In practice, freezing assets quickly matters most, because funds moved through several jurisdictions can disappear within days. Investigators should identify bank accounts, property and company interests abroad as early as possible and seek urgent freezing orders through the fastest available channel, while the formal case is built.

Corruption and corporate investigations

Cross-border bribery and fraud investigations increasingly involve coordinated action by authorities in several countries, alongside internal investigations by the companies concerned. The Foreign Corrupt Practices Act of 1977 allows United States authorities to pursue bribery of foreign officials by companies with sufficient connections to the United States, and the OECD Anti-Bribery Convention (Organisation for Economic Co-operation and Development [OECD], 1997) commits its parties to criminalise foreign bribery and cooperate in investigations. In 2008, Siemens pleaded guilty in the United States to violations of the Act and settled with German authorities at the same time, paying combined penalties of about 1.6 billion dollars, in a case that involved coordinated investigations across several countries (U.S. Department of Justice, 2008).

For companies, cross-border internal investigations raise practical questions: which country's data protection law governs the review of employee emails, whether documents can be transferred to lawyers in another country, how legal privilege applies in each jurisdiction, and how to coordinate with several authorities that may have different priorities and timetables.

Journalists and open-source investigators

Some of the most important transnational investigations have been carried out by journalists and open-source researchers rather than official agencies. The Panama Papers investigation, coordinated by the International Consortium of Investigative Journalists, involved hundreds of journalists in many countries analysing a leaked archive of offshore company records, and led to official investigations around the world (Obermayer & Obermaier, 2016). Higgins (2021) describes how open-source researchers traced the movements of the missile launcher involved in the downing of Malaysia Airlines Flight MH17 across the border between Russia and Ukraine using publicly available images. International criminal investigations increasingly use such material, and the Berkeley Protocol provides standards for collecting and verifying it so that it can be used in proceedings (Human Rights Center, University of California, Berkeley, School of Law & United Nations Office of the High Commissioner for Human Rights, 2022). Where national systems cannot or will not act, the International Criminal Court can investigate the most serious international crimes under the Rome Statute (1998).

Barriers to knowledge sharing

Beyond formal legal obstacles, several practical barriers limit cross-border knowledge sharing.

- **Speed.** Formal processes take months, while digital evidence may be deleted in days.
- **Trust.** Agencies may hesitate to share with counterparts whose integrity, data security or human rights record they doubt.
- **Language and translation.** Requests and evidence must be translated, adding cost, delay and the risk of misunderstanding.
- **Incompatible systems.** Different case management and intelligence systems make it hard to match records.
- **Competing priorities.** A case that is urgent for one state may be a low priority for another.

- **Information silos.** Within and between agencies, information may be hoarded or duplicated rather than shared. Sheptycki (2004) described such "organisational pathologies" in police intelligence systems.
- **Data protection.** Rules on transferring personal data abroad, such as those in the European Union's law enforcement data protection directive, require safeguards that can slow sharing (Directive (EU) 2016/680, 2016).

Political sensitivity is a further barrier. Requests that touch on a state's officials, security services or strategic industries may be delayed or refused, and some states use international channels, such as requests for the arrest of people abroad, to pursue political opponents rather than genuine criminals. Investigators receiving requests or intelligence from other states therefore need to assess not only the information but the motives behind it, and international bodies have introduced review procedures to reduce misuse of their systems. Equally, investigators sending requests should consider whether the information they share could expose witnesses, sources or suspects to persecution or unfair treatment in the receiving state, and should limit what they send accordingly. Bowling and Sheptycki (2012) note that the accountability of transnational policing remains weak compared with domestic policing, which makes such judgements by individual investigators and agencies more important.

Hufnagel (2013), comparing police cooperation in the European Union and Australia, found that practical cooperation often depends as much on personal relationships, trust and shared working practices as on formal legal frameworks.

Practices that work

Experience and research suggest several practices for transnational investigations:

- **Map the evidence early.** Identify at the outset what evidence is held abroad, by whom and under what law, and which route is fastest for each item.
- **Preserve first.** Ask providers and foreign authorities to preserve data immediately, then pursue formal requests.
- **Use fast channels for intelligence, formal channels for evidence.** Police and financial intelligence networks can confirm what exists and where; formal requests obtain it in admissible form.
- **Involve prosecutors and lawyers early.** Ensure requests meet the requirements of the receiving state and that evidence will be admissible where it will be used.
- **Write clear requests.** Explain the facts, the offence, the evidence sought and why it is relevant, avoiding jargon that may not translate.
- **Build relationships.** Liaison officers, joint training and regular contact build the trust that makes cooperation faster.
- **Consider joint teams.** For complex, multi-country cases, a joint investigation team can replace dozens of separate requests.
- **Respect rights.** Apply the strictest relevant standard for privacy, privilege and the rights of suspects, so that evidence is not lost to a challenge.
- **Coordinate outcomes.** Agree which country will prosecute, how penalties will be credited and how assets will be recovered, to avoid conflicting proceedings.

A short example

The following hypothetical case illustrates these practices. A survey research firm based in one country discovers that a panel of respondents has been infiltrated by a network of fake accounts claiming incentive payments. The accounts were created through servers in a second country, the payments went to digital wallets operated by a company in a third, and some of the people involved appear to live in a fourth.

The firm preserves its own records, including account registration logs and payment records, and reports the matter to police in its home country. The police use international police channels to confirm that the wallet operator holds records for the relevant accounts and ask it to preserve them. They then prepare a formal request to the third country for the records, written with the help of a prosecutor and translated. Meanwhile, they use a direct request procedure to obtain subscriber information about the servers from a provider that accepts such requests. The records reveal identities in the fourth country, whose authorities open their own investigation. The two countries agree to form a joint team, share evidence directly, and agree that the main prosecution will take place where most of the suspects live. The firm's own investigation report, which documents how each record was obtained and preserved, becomes part of the evidence.

Conclusion

Transnational investigation is necessary because wrongdoing and evidence cross borders while investigative powers do not. Formal mutual legal assistance provides admissible evidence but is slow; mutual recognition, joint investigation teams, police and financial intelligence networks, and direct requests to service providers have developed to make cooperation faster. Digital evidence held by global companies poses particular difficulties, and new laws in the United States and the European Union are changing how it can be obtained, while privacy rulings remind investigators that access must respect people's rights. Beyond legal frameworks, knowledge sharing depends on trust, relationships, clear requests and early coordination. Investigators who map the evidence early, preserve it quickly, choose the right channel for each item and build relationships with counterparts abroad can turn fragmented international information into reliable knowledge.

References

Andreas, P., & Nadelmann, E. (2006). *Policing the globe: Criminalization and crime control in international relations*. Oxford University Press.

Bowling, B., & Sheptycki, J. (2012). *Global policing*. Sage.

Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018).

Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Council of Europe).

Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams. (2002). *Official Journal of the European Communities, L 162*, 1–3.

Daskal, J. (2015). The un-territoriality of data. *Yale Law Journal*, *125*(2), 326–398.

Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, EU:C: 2020:559.

Deflem, M. (2002). *Policing world society: Historical foundations of international police cooperation*. Oxford University Press.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. (2016). *Official Journal of the European Union, L 119*, 89–131.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. (2014). *Official Journal of the European Union, L 130*, 1–36.

Financial Action Task Force. (2012). *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations* (updated periodically).

Foreign Corrupt Practices Act of 1977, 15 U.S.C. §§ 78dd-1 et seq.

Gerspacher, N. (2008). The history of international police cooperation: A 150-year evolution in trends and approaches. *Global Crime*, *9*(1–2), 169–184. https://doi.org/10.1080/17440570701862892

Higgins, E. (2021). *We are Bellingcat: An intelligence agency for the people*. Bloomsbury.

Hufnagel, S. (2013). *Policing cooperation across borders: Comparative perspectives on law enforcement within the EU and Australia*. Ashgate.

Human Rights Center, University of California, Berkeley, School of Law, & United Nations Office of the High Commissioner for Human Rights. (2022). *Berkeley protocol on digital open source investigations: A practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law*. United Nations.

Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016).

Nadelmann, E. A. (1993). *Cops across borders: The internationalization of U.S. criminal law enforcement*. Pennsylvania State University Press.

Obermayer, B., & Obermaier, F. (2016). *The Panama Papers: Breaking the story of how the rich and powerful hide their money*. Oneworld.

Organisation for Economic Co-operation and Development. (1997). *Convention on combating bribery of foreign public officials in international business transactions*.

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. (2023). *Official Journal of the European Union, L 191*, 118–180.

Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90.

Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology, 1*(3), 307–332. https://doi.org/10.1177/1477370804044005

Swire, P., & Hemmings, J. D. (2017). Mutual legal assistance in an era of globalized communications: The analogy to the visa waiver program. *NYU Annual Survey of American Law, 71*(4), 687–800.

United Nations Convention against Corruption, Oct. 31, 2003, 2349 U.N.T.S. 41.

United Nations Convention against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209.

United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

U.S. Department of Justice. (2008, December 15). *Siemens AG and three subsidiaries plead guilty to Foreign Corrupt Practices Act violations and agree to pay $450 million in combined criminal fines* [Press release].