INTELLIGENCE · ORGANISATIONAL INTELLIGENCE

Legal and Oversight Frameworks Governing Intelligence-Derived Knowledge

Knowledge produced by intelligence work is governed by law at every stage, from how it is collected to how long it is kept and who may see it. This article describes the main legal and oversight frameworks for state intelligence, the rules that apply to business intelligence, and how organisations can make sure their intelligence-derived knowledge stays lawful and usable.

ModQu research article · 1,897 words · 20 references (APA 7th edition)

Intelligence work produces knowledge: assessments, databases, profiles, reports and the expertise of analysts. That knowledge is only as useful as it is lawful. Information obtained by improper means may be unusable in court, may expose its holder to penalties, or may damage trust if its origin becomes known. Information kept too long, shared too widely or used for a purpose other than the one for which it was gathered can breach the law even if it was collected properly.

This article describes the legal and oversight frameworks that govern **intelligence-derived knowledge** across its life: collection, retention, use, sharing and disposal. It covers state intelligence, where these frameworks are most developed, and business intelligence, where the relevant rules come mainly from data protection, trade secret and competition law.

Why law follows knowledge through its life

It is tempting to think of legal controls as applying only at the moment of collection: a warrant to intercept a call, or permission to use a data source. But most legal frameworks follow information through its whole life. The principles agreed by the Organisation for Economic Co-operation and Development (1980) already distinguished collection limits from purpose specification, use limitation, security safeguards and accountability. Modern statutes, for state agencies and companies alike, work the same way. Knowledge gathered lawfully for one purpose can become unlawful if it is used for another.

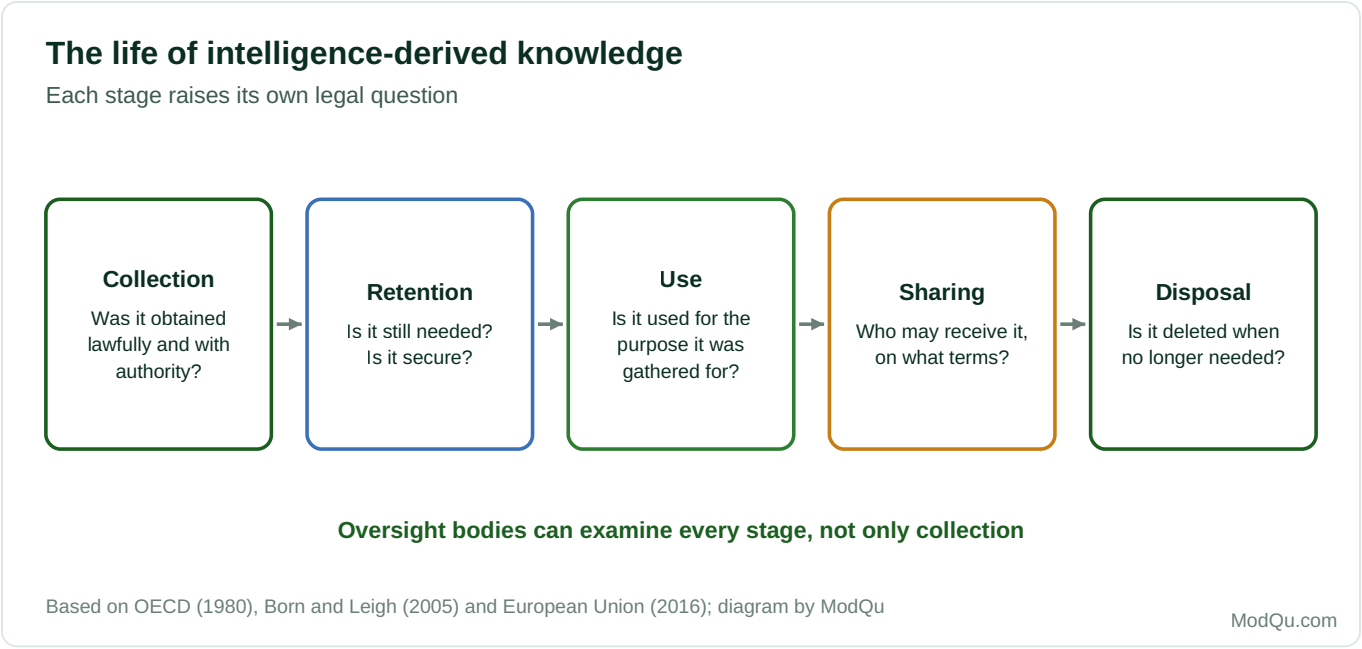


Figure 1. Legal questions across the life of intelligence-derived knowledge. Each stage has its own rules, and oversight bodies examine all of them. Based on Organisation for Economic Co-operation and Development (1980), Born and Leigh (2005) and European Union (2016); diagram by ModQu.

State intelligence: mandates and powers

In democracies, the first legal control over state intelligence is the **mandate**: a law that says what an agency is for and what it may do. For much of the twentieth century, many agencies operated without one. Born and Leigh (2005), in a comparative study of oversight standards, argue that a clear statutory mandate is the foundation of accountable intelligence, since without it there is no standard against which conduct can be judged.

Canada's approach illustrates the model. The Canadian Security Intelligence Service Act (1985) defined the threats the service may investigate, required warrants from the Federal Court for intrusive measures and created an external review body. The National Security Act, 2017 (S.C. 2019) replaced several separate review bodies with a single agency able to examine all national security activity across government, reflecting the recognition that intelligence knowledge flows between agencies and must be reviewed as a whole.

In the United States, the abuses documented by the Senate's Church Committee, including surveillance of lawful political activity, led to new limits (Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1976). The Foreign Intelligence Surveillance Act of 1978 required court approval for electronic surveillance of foreign powers and their agents inside the country and introduced **minimisation procedures**: rules that limit how information about citizens, collected incidentally, may be retained and disseminated. Minimisation is a clear example of law governing knowledge after collection. The Intelligence Reform and Terrorism Prevention Act of 2004 later reorganised the intelligence community under a Director of National Intelligence, partly to improve sharing of knowledge between agencies, while adding a civil liberties oversight board.

In the United Kingdom, the Investigatory Powers Act 2016 sets out in a single statute the powers to intercept communications, acquire communications data, interfere with equipment and hold bulk personal datasets. It requires warrants to be approved by both a senior minister and an independent judicial commissioner, and includes specific safeguards on the retention, copying and disclosure of material obtained.

Human rights law and the courts

International human rights law sets the outer limits. Article 8 of the European Convention on Human Rights permits interference with private life only if it is in accordance with the law, pursues a legitimate aim and is necessary in a democratic society (Council of Europe, 1950). The European Court of Human Rights has used this provision to examine intelligence laws in detail. In *Big Brother Watch and Others v. the United Kingdom* (2021), the Court set out safeguards required at each stage of bulk interception, from the choice of search terms to the storage, examination and onward sharing of material. Its reasoning treats the whole knowledge life as subject to law, not only the initial collection.

Courts can also affect intelligence knowledge indirectly. In *Data Protection Commissioner v. Facebook Ireland and Schrems* (2020), the Court of Justice of the European Union held that transfers of personal data to a country whose intelligence agencies have broad access to it require protections equivalent to European law. The result was that intelligence law in one country altered how businesses in another could handle their customer data.

Oversight bodies

Laws need someone to enforce them. Born and Leigh (2005) describe oversight as operating at several levels: executive control, legislative scrutiny, judicial authorisation and review, and independent expert bodies. Each sees different things. Judges see individual warrants. Inspectors and commissioners can audit how knowledge is stored, searched and shared. Legislators can examine budgets, priorities and patterns of failure.

The effectiveness of oversight varies. Zegart (2011), studying the American Congress, found that intelligence committees often lacked the expertise, staff and political incentives to oversee agencies closely, and that the secrecy of the subject limited public pressure. Gill and Phythian (2018) note that oversight bodies depend on agencies for information about what agencies do, which creates a risk that overseers see only what they are shown. Lowenthal (2022) describes oversight as a continuing negotiation between the need for secrecy and the need for accountability.

Omand (2010) argues that oversight matters not only for preventing abuse but for sustaining public consent. Intelligence agencies need public trust to retain their powers, and that trust depends on confidence that someone independent is checking.

Business intelligence: the main legal frameworks

Businesses that gather and use intelligence are governed by a different set of laws, but the logic is similar.

Data protection law. Where intelligence work involves personal data, data protection law applies. The European Union's General Data Protection Regulation requires a lawful basis for processing, limits use to specified purposes, requires data to be kept no longer than necessary and gives individuals rights of access and objection (European Union, 2016). It also requires organisations to be able to demonstrate compliance, which means keeping records of what they hold and why.

Trade secret law. Trade secret law protects valuable confidential business information and prohibits obtaining it by improper means such as theft, bribery, misrepresentation or breach of a duty of confidence. In the United States, the Economic Espionage Act of 1996 made theft of trade secrets a federal crime, and the Defend Trade Secrets Act of 2016 created a federal civil remedy. Almeling et al. (2010), analysing trade secret cases in federal courts, found that most involved people the owner knew, such as employees or business partners. For intelligence teams, trade secret law marks the boundary between legitimate competitive intelligence and industrial espionage. Crane (2005) argues that the boundary is ethical as well as legal: methods such as misrepresenting one's identity to obtain information may be unethical even where enforcement is unlikely.

Competition law. Exchanging competitively sensitive information, such as future prices or capacity plans, directly with competitors can breach competition law even if it was never written down. Intelligence teams need to make sure that knowledge about competitors comes from legitimate independent sources, not from contacts with rivals that could be seen as collusion.

Employment and contract law. Confidentiality clauses, restrictions on former employees and terms of use for websites and data services all affect what knowledge may be gathered and how it may be used.

From intelligence to evidence

A recurring difficulty is the move from intelligence to evidence. Intelligence is gathered to inform decisions; evidence must meet the standards of a court or tribunal. Knowledge that is perfectly adequate for a decision may be inadmissible as evidence, because its source cannot be revealed, because the chain of custody was not recorded, or because the method of collection would not survive scrutiny. Governments have long struggled with this problem in terrorism and organised crime cases, where revealing the source of intelligence may endanger people or methods (Omand, 2010).

Businesses face a smaller version of the same problem. A company that suspects a former employee of taking trade secrets may have strong intelligence suggesting it, but will need properly preserved logs, documents and witness statements to obtain an injunction. Intelligence teams that expect their work may one day be tested in court should preserve original material, record how it was handled and avoid any method that would taint it.

Keeping intelligence-derived knowledge lawful

Several practices help organisations keep their intelligence knowledge lawful and usable.

1. **Record provenance.** For each important item of knowledge, record where it came from and how it was obtained. Knowledge whose origin cannot be shown is hard to defend and may be impossible to use.

2. **Record purpose.** Note why the information was gathered. Using it for a different purpose may require a fresh legal basis.
3. **Set retention periods.** Decide how long each kind of knowledge will be kept and delete it when that period ends.
4. **Control sharing.** Agree in advance who may receive intelligence products and under what conditions, especially when sharing with partners, suppliers or other countries.
5. **Separate tainted material.** If information is found to have been obtained improperly, isolate it, take legal advice and do not use it.
6. **Prepare for review.** Keep records that would allow an auditor, regulator or court to see what was done and why.

Common mistakes

- **Thinking only about collection.** Lawfully obtained knowledge can still be misused, kept too long or shared improperly.
- **Losing the trail.** Reports that combine many sources without recording them make it impossible to show that knowledge was obtained lawfully.
- **Assuming foreign rules do not apply.** Data protection law can apply to organisations far from where the data subjects live.
- **Treating oversight as an obstacle.** Review by lawyers, auditors or ethics committees protects the organisation and improves the quality of its knowledge.

A business illustration

A pharmaceutical company's intelligence team receives an anonymous email containing what appears to be a competitor's internal clinical trial plan. The team does not open the attachment further once its nature is clear. It isolates the email, informs the legal department and records what happened. On legal advice, the company notifies the competitor and deletes the material. Separately, the team reviews its own knowledge base and finds that several competitor profiles contain personal details about named scientists gathered from social media years earlier. It deletes the details that are no longer needed, adds a retention period to its procedures and records the source and purpose of each remaining item. When a regulator later asks about the company's competitive intelligence practices, the team can show clear records.

Conclusion

Intelligence-derived knowledge is governed by law from the moment it is gathered to the moment it is deleted. For state agencies, the frameworks consist of statutory mandates, warrants, minimisation rules, human rights law and layered oversight. For businesses, they consist mainly of data protection, trade secret, competition and contract law, supported by internal governance. In both cases, the organisations that record provenance and purpose, control sharing and retention, and welcome review are the ones whose knowledge remains usable and trusted.

References

Almeling, D. S., Snyder, D. W., Sapoznikow, M., McCollum, W. E., & Weader, J. (2010). A statistical analysis of trade secret litigation in federal courts. *Gonzaga Law Review, 45*(2), 291–334.

Big Brother Watch and Others v. the United Kingdom, Nos. 58170/13, 62322/14 and 24960/15 (European Court of Human Rights, Grand Chamber, 25 May 2021).

Born, H., & Leigh, I. (2005). *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies*. Publishing House of the Parliament of Norway.

Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23 (Canada).

Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms* (European Treaty Series No. 5).

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons, 48*(3), 233–240. https://doi.org/10.1016/j.bushor.2004.11.005

Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559 (Court of Justice of the European Union, 16 July 2020).

Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (1996).

European Union. (2016). Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88.

Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world* (3rd ed.). Polity Press.

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

Investigatory Powers Act 2016, c. 25 (UK).

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.

National Security Act, 2017, S.C. 2019, c. 13 (Canada).

Omand, D. (2010). *Securing the state*. Hurst.

Organisation for Economic Co-operation and Development. (1980). *Guidelines on the protection of privacy and transborder flows of personal data*.

Select Committee to Study Governmental Operations with Respect to Intelligence Activities. (1976). *Final report* (S. Rep. No. 94-755). U.S. Government Printing Office.

Zegart, A. B. (2011). *Eyes on spies: Congress and the United States intelligence community*. Hoover Institution Press.