INTELLIGENCE · ORGANISATIONAL INTELLIGENCE

Privacy, Proportionality, and Governance in Intelligence Work

Intelligence work often involves information about people. This article explains why privacy matters, how the principle of proportionality is used to decide when intrusion is justified, and how organisations, public and private, can govern their intelligence activities so that they stay lawful, ethical and trusted.

ModQu research article · 2,781 words · 24 references (APA 7th edition)

Almost all intelligence work touches information about people. A government security service may intercept communications. A police analyst may map a criminal network. A company's market intelligence team may study online reviews, track the hiring patterns of a competitor's staff or analyse customer behaviour. In each case, the work can reveal things about individuals that they did not choose to share. That creates a tension. Intelligence aims to know more; privacy protects people's ability to control what others know about them.

This article explains why privacy matters, how the principle of **proportionality** is used to decide when intrusion is justified, and how organisations can govern their intelligence activities so that they remain lawful, ethical and trusted. The examples come from both government and business, because the same principles apply, even if the laws and stakes differ.

Why privacy matters

The modern idea of a legal right to privacy is often traced to an 1890 article by two American lawyers who argued for a "right to be let alone", prompted by intrusive newspaper photography (Warren & Brandeis, 1890). Westin (1967), writing at the start of the computer age, defined privacy as the claim of individuals and groups to decide for themselves when, how and to what extent information about them is communicated to others. Westin's definition remains influential because it focuses on control rather than secrecy. Information may be known to some people, such as a doctor or a bank, without the person losing all say in how it is used.

Privacy matters for several reasons. It protects people from harm, such as discrimination, fraud or harassment. It supports freedom of thought and association, since people behave differently when they believe they are watched. It underpins trust: customers share data with companies, and citizens accept state powers, only if they believe their information will be handled fairly. And it is a legal right in most democracies. Article 8 of the European Convention on Human Rights protects respect for private and family life, and allows interference only where it is in accordance with the law and necessary in a democratic society for purposes such as national security, public safety or the prevention of crime (Council of Europe, 1950).

Data protection principles

Privacy law in many countries is built on a set of principles first agreed internationally by the Organisation for Economic Co-operation and Development (1980). They include limits on collection, the use of data only for specified purposes, data quality, security safeguards, openness, individual access and accountability. The European Union's General Data Protection Regulation (European Union, 2016) restates and strengthens these principles, requiring among other things that personal data be processed lawfully, fairly and transparently, collected for specified purposes, limited to what is necessary, kept accurate, retained no longer than needed and protected against misuse.

For a business intelligence team, these principles have direct consequences. Collecting personal data "just in case" is hard to justify. Using customer data gathered for one purpose to profile individuals for another may require a fresh legal basis. Data about named employees of competitors, gathered from social media, is still personal data. The regulation applies to organisations outside Europe if they process data about people in the European Union, so it reaches many businesses that are not based there.

The limits of anonymisation

A common response to privacy concerns is to anonymise data: to remove names and identifiers before analysis. This helps, but it is less protective than often assumed. Sweeney (2002) showed that a large proportion of Americans could be uniquely identified from just three attributes: postcode, date of birth and sex. Narayanan and Shmatikov (2008) re-identified individuals in a supposedly anonymous dataset of film ratings by comparing it with public reviews. Ohm (2010) argued that these results show that anonymisation often fails, and that laws treating anonymised data as harmless rest on a false premise.

The lesson for intelligence teams is that combining datasets, which is often the point of analysis, increases the risk of identifying individuals. Each dataset may seem harmless on its own; together they can reveal a great deal. Techniques such as aggregation, removing rare values and adding statistical noise reduce the risk, but they need to be applied with care, and data should be treated as personal unless there is good reason to believe otherwise.

Proportionality

The central concept for deciding when intrusion is justified is **proportionality**. Barak (2012), in a comprehensive study of the concept in constitutional law, describes it as a structured way of deciding whether a limit on a right is justified. Courts in many countries apply a similar sequence of questions.

In Canada, the Supreme Court set out an influential version in *R. v. Oakes* (1986). A measure that limits a right must pursue a pressing and substantial objective. The means chosen must be rationally connected to that objective. The measure must impair the right as little as reasonably possible. And there must be proportionality between the benefits of the measure and its harmful effects. The European Court of Human Rights applies a similar approach when it asks whether an interference is "necessary in a democratic society".

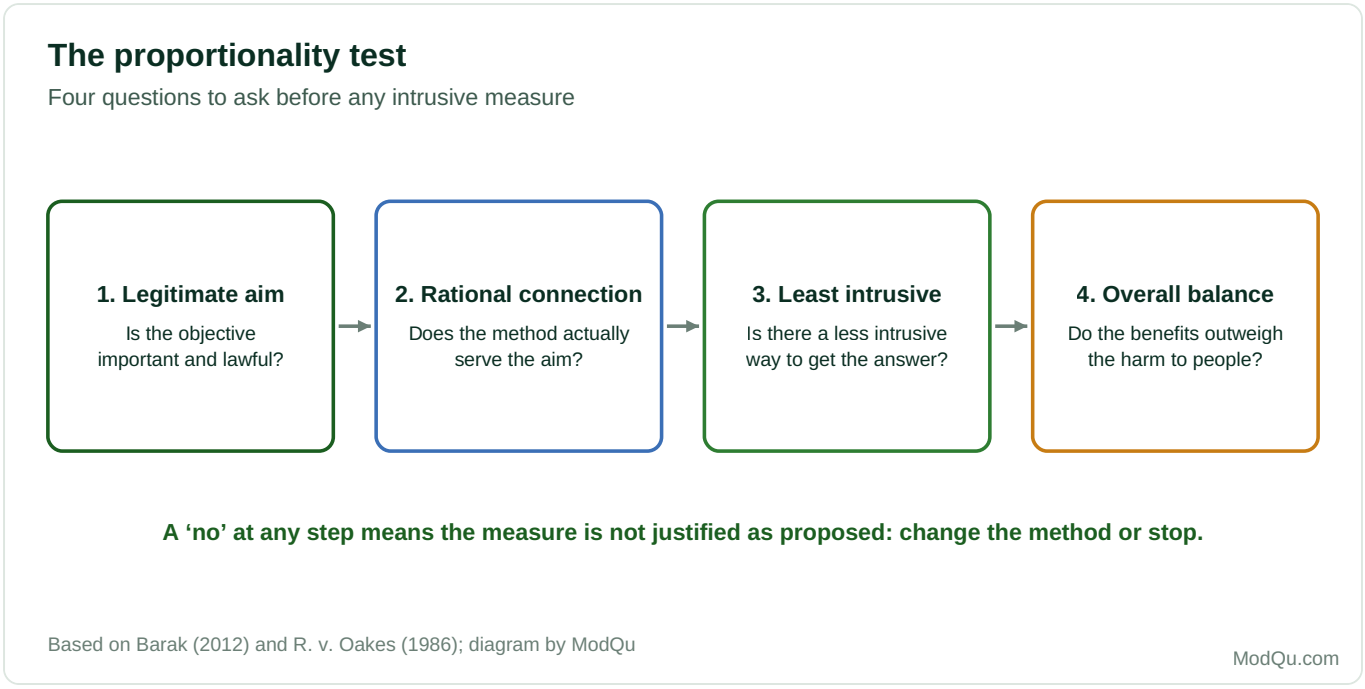


Figure 1. The proportionality test. Each question must be answered yes before an intrusive measure is justified. Based on Barak (2012) and R. v. Oakes (1986); diagram by ModQu.

These questions are useful well beyond the courtroom. Any intelligence team, public or private, can ask them before undertaking work that intrudes on people's privacy.

1. **Is the aim legitimate and important?** Protecting the company from fraud is a legitimate aim; satisfying curiosity about a competitor's chief executive's private life is not.
2. **Does the method actually serve the aim?** Collecting data that has no bearing on the question cannot be justified by the importance of the question.
3. **Is there a less intrusive way?** If aggregated data would answer the question, there is no need for individual-level data. If public company filings would do, there is no need to monitor employees' personal social media.
4. **Do the benefits outweigh the harms?** Consider the effect on the people concerned, including those who are not the target but whose data is caught up in the collection, and the risk to the organisation's reputation if the work became public.

Omand (2010) proposes a set of ethical principles for state intelligence that mirror this reasoning: sufficient sustainable cause, integrity of motive, proportionate methods, right authority, reasonable prospect of success and use of intrusion only as a last resort. These principles are drawn from the tradition of just war thinking, and they give intelligence officers a practical vocabulary for discussing when intrusion is justified.

Lessons from history

Concern about intelligence and privacy is not new. In the 1970s, investigations in the United States revealed that intelligence and law enforcement agencies had for years spied on American citizens, including civil rights leaders and anti-war activists, opened mail and kept files on people engaged in lawful political activity. The Senate committee

chaired by Frank Church documented these abuses in detail and concluded that intelligence activities had undermined the constitutional rights of citizens because the agencies had operated without clear legal limits or effective oversight (Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1976).

The response shaped intelligence governance for decades. The Foreign Intelligence Surveillance Act of 1978 created a special court to approve electronic surveillance for foreign intelligence purposes, and permanent intelligence committees were established in both houses of Congress. Zegart (2011) argues that congressional oversight nonetheless remained weak, owing to limited expertise, secrecy and the political incentives of legislators. Later reforms, including the Intelligence Reform and Terrorism Prevention Act of 2004, which created the Director of National Intelligence, focused more on coordination than on privacy, though the act did establish a Privacy and Civil Liberties Oversight Board.

Other democracies have followed similar paths. Canada placed its security intelligence service on a statutory footing with the Canadian Security Intelligence Service Act (1985), which defined its mandate and created an independent review body. The National Security Act, 2017 (S.C. 2019) later consolidated review of all Canadian national security agencies under a single body. In the United Kingdom, the Investigatory Powers Act 2016 brought interception and bulk data powers under a single statute, with warrants subject to approval by independent judicial commissioners.

Bulk collection and the courts

The question of proportionality has become sharper as intelligence agencies have acquired the ability to collect communications data in bulk. In *Big Brother Watch and Others v. the United Kingdom* (2021), the European Court of Human Rights held that bulk interception is not in itself incompatible with the Convention, but that the British regime then in force lacked adequate safeguards, including independent authorisation and sufficient oversight of how selectors were chosen. The judgement set out the "end-to-end safeguards" a lawful bulk regime must include.

In *Data Protection Commissioner v. Facebook Ireland and Schrems* (2020), the Court of Justice of the European Union went further, invalidating an arrangement for transferring personal data from the European Union to the United States because American surveillance law did not offer protection essentially equivalent to European law. The case showed that intelligence governance in one country can have direct commercial consequences for businesses in another: thousands of companies had to change how they transferred data.

Governance

Proportionality is a test applied to individual decisions. **Governance** is the system that makes sure the test is actually applied, consistently and honestly. Born and Leigh (2005), in a study of oversight practice across democracies, identify several layers of control over state intelligence: the executive, which directs and authorises; the legislature, which makes the law and scrutinises; the judiciary, which authorises intrusive measures and hears complaints; independent bodies such as inspectors and commissioners; and internal controls within agencies themselves. Gill and Phythian (2018) add that the media and civil society play an informal but important role in exposing abuses.

Layers of governance

State intelligence oversight and business equivalents

Layer	In state intelligence	In a business
Law and regulation	Statutes defining mandates and powers	Data protection, competition and employment law
Authorisation	Ministers and judges approve warrants	Senior approval for sensitive work
Independent review	Commissioners, inspectors, review bodies	Internal audit, compliance, ethics committee
Legislative scrutiny	Parliamentary or congressional committees	Board or audit committee reporting
Internal controls	Policies, legal advisers, audit logs	Policy, privacy assessments, access logs
Transparency	Public reports, media, civil society	Privacy notices, openness with customers

Based on Born and Leigh (2005) and Gill and Phythian (2018); table by ModQu

ModQu.com

Figure 2. Layers of governance. State intelligence is governed by several layers of control; businesses can build their own equivalents. Based on Born and Leigh (2005) and Gill and Phythian (2018); table by ModQu.

Lowenthal (2022) notes that oversight always involves a trade-off: overseers need enough access to judge what agencies are doing, while agencies need enough secrecy to operate. Effective oversight depends less on formal powers than on the expertise, independence and persistence of those exercising them.

Businesses do not face the same formal oversight as state agencies, but they do face regulators, courts, customers, employees and the media. A company whose intelligence practices are exposed as intrusive can suffer serious reputational damage, as well as legal penalties. Building internal governance is therefore in the company's own interest.

Privacy by design

Cavoukian (2009), then Information and Privacy Commissioner of Ontario, proposed the idea of **privacy by design**: building privacy protection into systems and processes from the start, rather than adding it afterwards. Its principles include being proactive rather than reactive, making privacy the default setting, embedding privacy into design, and maintaining visibility and transparency. The approach has since been written into European data protection law (European Union, 2016).

For intelligence teams, privacy by design means asking privacy questions when a new collection method, data source or analytic tool is being planned, not after it has been used. It means designing reports so that they show aggregated patterns unless individual detail is genuinely needed, setting retention periods so that data is deleted when no longer required, and limiting access to sensitive material to those who need it.

A governance framework for business intelligence

A practical governance framework for a business intelligence function might include the following elements.

1. **A written policy.** State what kinds of information the team collects, the methods it may and may not use, and the principles that guide it, including legality, honesty and proportionality.
2. **Clear authorisation.** Require senior approval for work that involves personal data, covert methods or sensitive targets. Record who approved what and why.
3. **Privacy impact assessments.** Before starting a new project or using a new data source, assess the privacy risks and how they will be reduced, applying the four proportionality questions.
4. **Legal review.** Consult lawyers on data protection, competition law, employment law and any sector-specific rules.
5. **Data minimisation and retention.** Collect only what is needed, keep it only as long as needed, and delete it securely afterwards.
6. **Access controls and audit.** Restrict access to sensitive data and keep logs of who accessed what.
7. **Independent review.** Have someone outside the team, such as an internal audit, compliance or ethics function, periodically review the team's activities.
8. **Training and culture.** Make sure that analysts understand the rules and feel able to raise concerns without fear of retaliation.
9. **Transparency.** Where possible, be open with customers and the public about the kinds of data used and why.

Open sources and people

Much business intelligence relies on open sources: news, company filings, websites, job advertisements, online reviews and social media. These are generally lawful to consult, but open sources raise privacy questions when the analysis focuses on individuals. Reading a competitor's annual report is uncontroversial. Building a profile of a named engineer from their professional networking page, conference talks, personal social media and family photographs is different, even if each item was published voluntarily. Westin's (1967) emphasis on control is helpful here: people who publish a professional profile expect it to be read by recruiters and colleagues, not compiled into a dossier by a rival company.

A useful rule is to separate information about organisations from information about people. Where the question concerns a company's strategy, capabilities or performance, analysis should focus on the company and use information about individuals only where it is necessary, such as the public statements of executives acting in their official roles. Where individuals must be studied, the purpose should be recorded and the collection kept to what that purpose requires.

Questions to ask before collecting

Before starting any piece of work that involves personal data, a team can ask:

1. What decision will this information support, and who asked for it?
2. Could we answer the question with aggregated or non-personal data?
3. Would the people concerned be surprised or upset to learn of it?

4. How long will we keep the data, and who will see it?
5. Could we explain and defend the method if it were reported in the press?

If the answers are uncomfortable, the work should be redesigned or referred for approval.

Common mistakes

- **Assuming that public data is fair game.** Information that is technically accessible, such as social media profiles, is still personal data and may be protected by law. Collecting and combining it can be intrusive.
- **Treating anonymised data as risk-free.** As the research on re-identification shows, combining datasets can reveal individuals.
- **Skipping the necessity question.** Teams often ask whether a method is legal but not whether it is needed. A less intrusive alternative may answer the question just as well.
- **Relying on outsourcing.** Hiring a contractor to collect data does not transfer responsibility. If the contractor uses unlawful methods, the client may share the legal and reputational consequences.
- **Governing on paper only.** A policy that no one reads or enforces offers no protection.

A business illustration

A retail bank's intelligence team wants to understand why customers are leaving for a digital competitor. One proposal is to monitor the social media accounts of customers who have closed their accounts, to see what they say about the competitor. The team applies the proportionality questions. The aim, understanding customer loss, is legitimate. But monitoring named individuals is intrusive, and there are less intrusive ways to answer the question. The team instead analyses aggregated data on account closures, runs an anonymous survey of former customers who agree to take part, and reviews public discussion of the competitor in general terms without identifying individuals.

The team records its reasoning in a short privacy impact assessment, which the bank's data protection officer reviews. The analysis produces useful findings about fees and mobile app features, and the bank avoids a practice that, had it become known, could have damaged trust and drawn the attention of regulators.

Conclusion

Privacy and intelligence are often presented as opposites, but the relationship is more subtle. Intelligence that respects privacy is more likely to be trusted, sustained and lawful; intelligence that ignores it risks legal challenge, public backlash and the loss of the very access on which it depends. The principle of proportionality offers a practical way to decide when intrusion is justified, and governance makes sure that the principle is applied in practice. For businesses and governments alike, the goal is not to know everything, but to know what is needed, by means that can be defended openly.

References

Barak, A. (2012). *Proportionality: Constitutional rights and their limitations*. Cambridge University Press. https://doi.org/10.1017/CBO9781139035293

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).

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.

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

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).

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.

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy* (pp. 111–125). IEEE. https://doi.org/10.1109/SP.2008.33

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

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*, 1701–1777.

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*.

R. v. Oakes, [1986] 1 S.C.R. 103 (Supreme Court of Canada).

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

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(5), 557–570. https://doi.org/10.1142/S0218488502001648

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220. https://doi.org/10.2307/1321160

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

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