INVESTIGATION · LAW, ETHICS AND REGULATION

Privacy Law and the Limits of Investigation

Every investigation collects information about people, and privacy law sets limits on what can be gathered, how and why. This article explains the main sources of privacy protection, the kinds of privacy harm investigations can cause, how courts balance privacy against legitimate investigation, and practical principles for staying within the law.

ModQu research article · 1,039 words · 12 references (APA 7th edition)

Investigations are, by their nature, intrusive. They gather information about what people did, said, owned and wrote, often without their knowledge and sometimes against their wishes. Privacy law exists to limit such intrusion. It does not forbid investigation, but it requires that intrusion be justified, proportionate and carried out by lawful means. Investigators who ignore it risk criminal and civil liability, the exclusion of their evidence and serious damage to the reputation of their clients.

Where privacy protection comes from

Modern thinking about privacy as a legal right is often traced to an 1890 article by Samuel Warren and Louis Brandeis, who argued, in response to intrusive newspapers and new portable cameras, that the law should protect "the right to be let alone" (Warren & Brandeis, 1890). Prosser (1960) later described four distinct privacy torts recognised by American courts: intrusion upon seclusion, public disclosure of private facts, false light and appropriation of a name or likeness.

Today, privacy protection comes from several sources:

- **Human rights law.** Article 8 of the European Convention on Human Rights protects the right to respect for private and family life, home and correspondence (Council of Europe, 1950). Interference must be in accordance with the law, pursue a legitimate aim and be necessary and proportionate.
- **Constitutional law.** In the United States, the Fourth Amendment protects against unreasonable searches by government. In *Katz v. United States* (1967), the Supreme Court held that it protects people's reasonable expectations of privacy, and in *Carpenter v. United States* (2018) it extended this protection to historical mobile phone location records.
- **Data protection law.** The European Union's General Data Protection Regulation requires that personal data be processed lawfully, fairly and transparently, for specified purposes, and limited to what is necessary (Regulation (EU) 2016/679, 2016).
- **Private law.** Courts in many countries allow people to sue for invasions of privacy. In England, the House of Lords in *Campbell v MGN Ltd* (2004) recognised a claim for misuse of private information. In Ontario, the Court of Appeal recognised the tort of intrusion upon seclusion in *Jones v. Tsige* (2012), a case in which a bank employee had repeatedly looked at a colleague's banking records.

Kinds of privacy harm

Solove (2006) argues that "privacy" covers many different problems, and that it is more useful to identify specific kinds of harm. His taxonomy is helpful for investigators, because it shows that privacy can be harmed at every stage of an investigation, not only when information is collected.

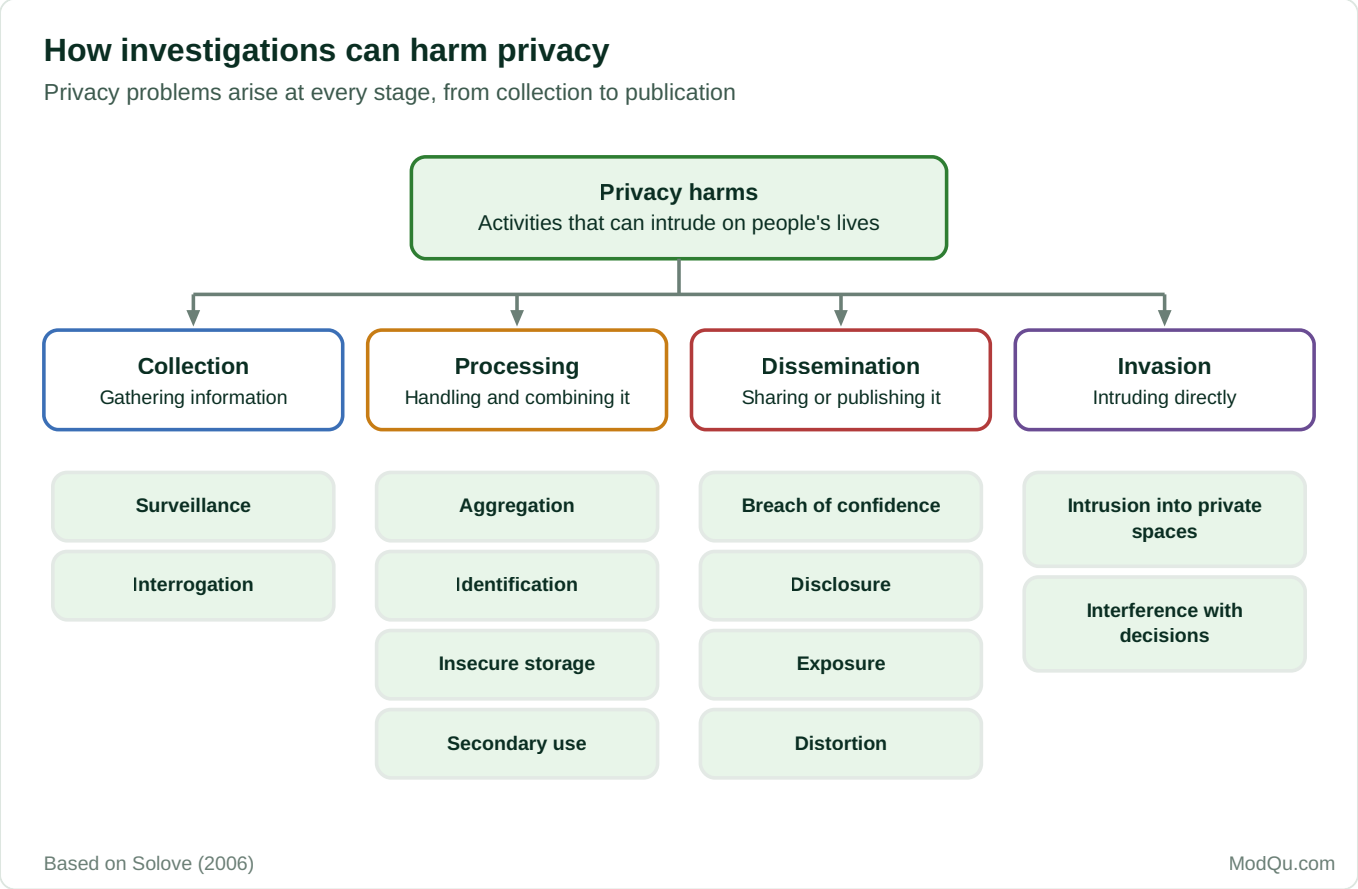


Figure 1. Four groups of privacy harm. Investigators often focus on lawful collection but overlook harms from aggregating, storing and sharing what they have collected. Diagram by ModQu.

Aggregation deserves particular attention. Individual pieces of public information, such as a person's employer, the car they drive and the gym they attend, may each be harmless, but combined they can reveal a detailed picture of someone's life. Nissenbaum (2010) argues that privacy is best understood as "contextual integrity": information flows appropriately when it respects the norms of the context in which it was shared. A post shared with friends, gathered and combined into an investigator's dossier, moves into a very different context.

Balancing privacy and investigation

Courts balance privacy against legitimate interests such as preventing crime, protecting a business from fraud or defending legal claims. None of these interests automatically outweighs privacy; the question in each case is whether the particular intrusion was necessary and proportionate to the aim. Employee monitoring illustrates the balance. In

Bărbulescu v. Romania (2017), the European Court of Human Rights held that an employer had violated an employee's privacy by monitoring his personal messages on a work account without adequate prior notice. The Court set out factors to consider, including whether the employee was told about monitoring, its extent, whether there were legitimate reasons, and whether less intrusive methods were available. European data protection authorities have given similar guidance on monitoring at work (Article 29 Data Protection Working Party, 2017).

Open sources are not a free-for-all

A common misconception is that anything publicly available online can be collected without restriction. In jurisdictions with data protection laws, this is not so: personal data remain personal data even when they are publicly accessible, and collecting, storing and combining them still requires a lawful basis and must be proportionate. Data protection authorities have taken action against organisations that scraped publicly available photographs and profiles on a large scale. Investigators who use open sources should therefore record why each search was necessary, avoid building general profiles of people beyond the scope of the investigation, and remember that the people concerned may have the right to ask what has been collected about them.

Practical principles

From these sources, several practical principles follow for investigators:

- **Have a legitimate purpose** and record it before the investigation starts.
- **Use the least intrusive method** that will achieve that purpose.
- **Collect only what is needed**, and avoid gathering information about people who are not relevant.
- **Use lawful sources and means**, avoiding deception to obtain confidential records.
- **Keep information secure** and delete it when it is no longer needed.
- **Limit disclosure** to those who need the findings.

A short example

The following hypothetical case illustrates these principles. A company suspects that an employee is leaking confidential product plans to a competitor. Before starting, the company records the specific concern and the reason it believes the leak is coming from one team. It reviews the access logs of the shared drive, which employees have been told are monitored, rather than reading anyone's personal emails. The logs show that one employee downloaded the plans shortly before each leak. The company interviews the employee, who admits sending the files. It keeps the investigation file in a restricted folder, shares the findings only with the managers who must decide on discipline, and deletes information collected about other team members once they are cleared.

Conclusion

Privacy law does not prevent investigation, but it shapes it. Investigators must have a legitimate purpose, use proportionate and lawful means, and handle what they collect with care at every stage. Following these principles protects the people being investigated and also makes the investigation's findings more likely to stand up when challenged. Where the law is unclear, documenting the reasons for each step is the best protection.

References

Article 29 Data Protection Working Party. (2017). *Opinion 2/2017 on data processing at work* (WP 249). European Commission.

Bărbulescu v. Romania [GC], no. 61496/08 (Eur. Ct. H.R. 5 September 2017).

Campbell v MGN Ltd [2004] UKHL 22.

Carpenter v. United States, 585 U.S. 296 (2018).

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

Jones v. Tsige, 2012 ONCA 32.

Katz v. United States, 389 U.S. 347 (1967).

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383–423. https://doi.org/10.2307/3478805

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). (2016). *Official Journal of the European Union, L 119*, 1–88.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564. https://doi.org/10.2307/40041279

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