INVESTIGATION · LAW, ETHICS AND REGULATION

The Legal Framework for Private Investigation

Private investigators work for businesses, lawyers and individuals, but they have no special legal powers and must work within licensing, privacy, data protection and criminal laws. This article explains how private investigation is regulated in several countries and where the main legal limits lie.

ModQu research article · 1,184 words · 13 references (APA 7th edition)

Private investigators carry out a wide range of work: tracing debtors and witnesses, checking insurance claims, conducting due diligence on companies and individuals, investigating fraud and misconduct for employers, gathering evidence for litigation and, in some places, serving legal documents. Unlike police officers, they have no special powers to search, arrest, demand information or intercept communications. They act under the same laws as any other citizen, and in many jurisdictions under additional licensing rules. Understanding this legal framework is essential both for investigators and for the businesses and lawyers who hire them, because evidence gathered unlawfully can be excluded, and the client as well as the investigator may be liable.

Licensing

Countries and regions differ considerably in whether and how they regulate private investigators. Button (2019) describes a spectrum from jurisdictions with no specific regulation to those with detailed licensing, training and conduct requirements.

In Canada, regulation is provincial. Ontario's Private Security and Investigative Services Act, 2005 requires private investigators to hold a licence, complete training, pass an examination and follow a code of conduct, and prohibits them from holding themselves out as police. In the United States, most states license private investigators; California's Private Investigator Act, for example, requires applicants to have relevant experience, pass an examination and meet background requirements. In the United Kingdom, the Private Security Industry Act 2001 created a framework under which private investigators could be licensed, but the licensing of investigators was never brought into force. A parliamentary committee criticised the lack of regulation, noting evidence of investigators obtaining personal information unlawfully (Home Affairs Committee, 2013).

Gill and Hart (1997), in an early study of British private detectives, found a diverse industry ranging from small one-person businesses to large corporate firms, with widely varying standards, and argued that this diversity made regulation both necessary and difficult.

The main legal limits

Whether or not they are licensed, investigators must comply with general laws that set the boundaries of their work.

Common legal boundaries for private investigators

Details vary by jurisdiction; these are typical in common law countries

	Usually lawful	Usually unlawful
Information	Public records, open sources, voluntary interviews	Obtaining confidential records by deception
Surveillance	Observing people in public places	Trespass, harassment, stalking
Recording	Recording own conversations where consent rules allow	Intercepting others' calls or messages
Data	Processing personal data with a lawful basis	Unlawful obtaining or disclosure of personal data
Identity	Using discretion about one's purpose	Impersonating police or officials

Based on Button (2019) and the statutes cited in this article ModQu.com

Figure 1. Typical legal boundaries. Investigators must check the specific rules of each jurisdiction, especially on recording conversations and on pretexting. Diagram by ModQu.

Obtaining personal information. The most serious legal risks arise when investigators obtain confidential information, such as bank, telephone or medical records, without consent. In the United States, the Gramm-Leach-Bliley Act prohibits obtaining customer information from financial institutions by false pretences (Gramm-Leach-Bliley Act, 1999), and the Telephone Records and Privacy Protection Act of 2006 made it a federal crime to obtain telephone records by pretexting (Telephone Records and Privacy Protection Act of 2006, 2007). In the United Kingdom, the Data Protection Act 2018 makes it an offence knowingly or recklessly to obtain or disclose personal data without the consent of the controller (s. 170). The Information Commissioner's Office (2006) documented an extensive illegal trade in personal information involving investigators who obtained it from banks, telephone companies and government databases by deception and sold it to clients including journalists, insurers and lenders.

Data protection. In jurisdictions with comprehensive data protection laws, investigators who collect and use personal data must have a lawful basis, keep it secure and use it only for legitimate purposes. Under the European Union's General Data Protection Regulation, this applies to investigators and their clients alike (Regulation (EU) 2016/679, 2016). In Canada, the Personal Information Protection and Electronic Documents Act governs the collection of personal information in commercial activities, including investigations.

Surveillance and harassment. Observing people in public is generally lawful, but trespassing on private property, following someone in a way that amounts to harassment, or placing tracking devices on vehicles without consent may be unlawful.

Recording and interception. Laws on recording conversations vary. Some jurisdictions allow a party to record their own conversation without telling the other party; others require all parties' consent. Intercepting other people's communications is a serious offence almost everywhere.

Background checks. Where investigators prepare reports used to decide on employment, credit or insurance, consumer reporting laws may apply. In the United States, the Fair Credit Reporting Act requires accuracy, permissible purposes and, in many cases, notice to the person concerned (Fair Credit Reporting Act, 1970).

Investigations for litigation

Much private investigation is done for lawyers preparing civil or criminal cases. When an investigator is instructed by a lawyer for the purpose of litigation, the investigator's work may be protected from disclosure to the other side by legal privilege, which in common law systems covers documents prepared mainly for the purpose of actual or anticipated litigation. The protection is not automatic. It depends on who instructed the investigator, for what purpose and when, so investigators and clients should agree at the outset how the work will be commissioned and recorded.

Investigators working on litigation must also remember that their methods may be examined in court. A witness statement obtained under pressure, a recording made unlawfully or a report that cannot show where its information came from may be excluded or may damage the credibility of the whole case. Courts may also criticise, or order costs against, a party whose investigators behaved improperly.

A short example

The following hypothetical case illustrates the boundaries. An insurer suspects that a claimant who says he cannot work because of a back injury is in fact working on building sites. It hires a licensed investigator. The investigator checks public company records and the claimant's public social media posts, and conducts surveillance from public roads, filming the claimant carrying heavy materials on two days. The investigator does not enter the building site, does not contact the claimant under a false identity, and does not try to obtain his bank records or medical files. The report sets out each observation with dates, times and locations, and explains how each piece of information was obtained. When the claim goes to court, the claimant's lawyer challenges the evidence, but because the investigator kept within the law and documented each step, the evidence is admitted.

Responsibility of clients

Clients cannot avoid responsibility by delegating unlawful work. A company that instructs or knowingly benefits from an investigator's unlawful conduct may face criminal or civil liability, regulatory penalties and serious reputational damage. Evidence obtained unlawfully may be excluded in court or may undermine the client's case. Good practice for clients is to hire licensed and reputable investigators, set out in writing the lawful methods to be used, ask how information was obtained, and keep records showing that the investigation was proportionate to a legitimate purpose.

Conclusion

Private investigators have no special legal powers. They work within licensing rules where these exist and within general laws on privacy, data protection, harassment, recording and deception. Where regulation is weak, as in the United Kingdom, inquiries have documented serious abuses. For investigators and their clients alike, the safest course is to use lawful sources and methods, document how information was obtained, and remember that unlawfully obtained evidence

can harm the case it was meant to support. Because laws differ between countries, provinces and states, investigators working across borders should take local legal advice before using methods such as recording, tracing or surveillance, and clients should expect to see that advice reflected in the investigation plan.

References

Button, M. (2019). *Private policing* (2nd ed.). Routledge.

Data Protection Act 2018, c. 12 (UK).

Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (1970).

Gill, M., & Hart, J. (1997). Exploring investigative policing: A study of private detectives in Britain. *British Journal of Criminology, 37*(4), 549–567. https://doi.org/10.1093/oxfordjournals.bjc.a014197

Gramm-Leach-Bliley Act, 15 U.S.C. § 6821 (1999).

Home Affairs Committee. (2013). *Private investigators* (Fourth Report of Session 2012–13, HC 100). House of Commons.

Information Commissioner's Office. (2006). *What price privacy? The unlawful trade in confidential personal information* (HC 1056). The Stationery Office.

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Canada).

Private Investigator Act, Cal. Bus. & Prof. Code § 7512 et seq.

Private Security and Investigative Services Act, 2005, S.O. 2005, c. 34 (Ontario).

Private Security Industry Act 2001, c. 12 (UK).

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.

Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039 (2007).