INVESTIGATION · LAW, ETHICS AND REGULATION

Pretexting and Deception: Where Investigators Must Stop

Investigators sometimes hide their identity or purpose to obtain information, but pretexting to get confidential records is a crime in many countries, and deception can make evidence unusable. This article explains the forms of deception used in investigations, the laws and professional rules that limit them, landmark cases, and a practical test for deciding where to stop.

ModQu research article · 2,623 words · 29 references (APA 7th edition)

Deception has always been part of investigation. Detectives pose as buyers to catch fraudsters, journalists take jobs to expose abuse, researchers send fictitious applications to test for discrimination, and mystery shoppers pretend to be ordinary customers. Some of this work is lawful, valuable and widely accepted. But deception can also be used to obtain information that the law protects, such as bank, telephone and medical records, and to manipulate people into betraying confidences. Pretexting, obtaining information by pretending to be someone else or by lying about the purpose of a request, has been at the centre of several major scandals and is now a crime in many places.

This article explains the forms of deception used in investigation, the moral case against it and the arguments for limited exceptions, the laws and professional rules that set boundaries, and a practical test that investigators and their clients can use to decide where they must stop.

Forms of deception

Deception in investigation ranges from the minor to the serious.

Forms of deception in investigation

Legality depends on what is obtained and from whom, not only on the deception itself

	Usually acceptable when	Usually unlawful or improper when
Discretion	Investigator does not volunteer their purpose	A direct question is answered with a lie
Test purchase	Posing as an ordinary customer of a public business	Inducing an offence that would not otherwise occur
Mystery shopping	Assessing service of an organisation	Used to discipline staff who were not told
Undercover role	Serious public interest; no other way	Long-term intimate deception; trespass
Pretexting	Rarely acceptable	Obtaining confidential records by impersonation

Based on Marx (1988), ESOMAR (2016) and the statutes and cases cited in this article ModQu.com

Figure 1. Five forms of deception and the lines commonly drawn around them. The more confidential the information and the more active the lie, the harder deception is to justify. Diagram by ModQu.

At the mildest end is **discretion**: an investigator does not volunteer who they are or why they are asking, for example when looking at public records or chatting with a shop assistant. Next comes **posing as an ordinary member of the public**, such as making a test purchase or responding to an advertisement, to see how a business treats its customers. **Undercover roles** involve sustained deception, such as taking a job or joining a group under a false identity. At the most serious end is **pretexting**, in which an investigator impersonates someone, such as an account holder, an official or a colleague, to obtain information that the holder would release only to that person.

Pretexting is closely related to "social engineering", the manipulation of people to gain access to information or systems, which security specialists study in order to defend against it. Mitnick and Simon (2002) and Hadnagy (2018) describe how attackers exploit helpfulness, authority, urgency and trust to persuade staff to reveal passwords, account details or confidential records. The techniques used by unscrupulous investigators are often the same.

The moral case against deception

Bok (1978), in a classic study of lying, argued that deception is never morally neutral. Lies harm the person deceived by manipulating their choices, and they harm the liar and society by eroding trust. She proposed that those who wish to justify a lie should first ask whether any truthful alternative exists, then weigh the moral reasons for and against the lie, and finally ask whether the lie could be justified to a reasonable public. Lies that could not survive public scrutiny, she argued, are rarely justified.

Marx (1988), in a study of undercover policing in the United States, recognised that covert methods can expose crimes that would otherwise go undetected, but documented their costs: deception of innocent people, temptation and corruption of the investigators, the creation of crimes that would not otherwise have happened, and harm to trust in public institutions. He argued for strict controls, including clear legal authority, supervision and limits on what undercover agents may do.

Those who defend limited deception usually rely on a public interest argument: that the harm of the deception is small compared with the harm it exposes. The argument has force in some cases, such as exposing abuse in a care home that could not be documented in any other way. But it has two weaknesses. First, the person deciding whether the public interest justifies the deception is usually the person who wants to deceive, and is therefore inclined to overestimate the benefit. Second, the benefit is uncertain at the time the decision is made, because the investigator does not yet know what will be found, while the deception is certain. For these reasons, codes that allow deception usually require that the decision be made in advance, by someone senior and independent of the investigation, and that the reasons be recorded.

The law on pretexting

Several scandals led governments to make pretexting a specific offence.

The United States. The Gramm-Leach-Bliley Act of 1999 made it unlawful to obtain customer information from a financial institution by making false or fraudulent statements to the institution or its customers (Gramm-Leach-Bliley Act, 1999). Telephone records were not covered, and a market developed in which data brokers sold call records obtained by impersonating account holders. In 2006, it emerged that investigators hired by Hewlett-Packard to find the source of leaks from its board had obtained the telephone records of directors, employees and journalists by pretexting. The scandal led to congressional hearings (Committee on Energy and Commerce, 2006), the resignation of the company's chair, and criminal charges, and it helped prompt the Telephone Records and Privacy Protection Act of 2006, which made obtaining telephone records by false pretences a federal crime (Telephone Records and Privacy Protection Act of 2006, 2007).

The United Kingdom. The Information Commissioner's Office (2006) reported on an extensive illegal trade in personal information, documenting how investigators obtained bank, telephone, vehicle and criminal records by impersonating account holders or officials, and sold the information to clients including newspapers, insurers and lenders. The phone-hacking scandal and the Leveson Inquiry later revealed how widely some newspapers had used private investigators to obtain information unlawfully (Leveson, 2012). A parliamentary committee found that the private investigation industry remained largely unregulated and recommended licensing (Home Affairs Committee, 2013). The Data Protection Act 2018 makes it an offence knowingly or recklessly to obtain personal data without the consent of the organisation that holds it (Data Protection Act 2018, s. 170).

In both countries, the person who commissions pretexting can be liable as well as the investigator who carries it out, and evidence obtained in this way may be excluded or may expose the client to civil claims.

Deception by lawyers and their investigators

Lawyers are bound by professional rules that prohibit making false statements of fact to others and engaging in dishonesty, fraud, deceit or misrepresentation (American Bar Association [ABA], 2020, Rules 4.1 and 8.4(c)). These rules also apply to investigators acting under a lawyer's direction. Courts and disciplinary bodies have had to decide whether they forbid all use of undercover investigators in litigation.

In *In re Gatti* (2000), the Oregon Supreme Court disciplined a lawyer who had posed as a chiropractor and a doctor to obtain information from an insurance company, holding that the rules contained no exception for lawyers investigating wrongdoing. In contrast, federal courts in New Jersey and New York accepted evidence gathered by investigators who posed as ordinary customers to test whether businesses were violating trademark agreements, reasoning that the investigators had only recorded the businesses' normal dealings with the public (*Apple Corps Ltd. v. International Collectors Society*, 1998; *Gidatex, S.r.L. v. Campaniello Imports, Ltd.*, 1999). The distinction that emerged is between posing as an ordinary member of the public to observe routine behaviour, which is generally acceptable, and using deception to obtain information that would not be given to an ordinary member of the public, which is not.

Undercover journalism

Journalists sometimes use deception to expose wrongdoing, and their professional codes permit it in limited circumstances. The Society of Professional Journalists (SPJ, 2014) code asks journalists to avoid undercover or other surreptitious methods of gathering information unless open methods will not yield information vital to the public. In the United Kingdom, the editors' code administered by the Independent Press Standards Organisation (IPSO, 2021) permits subterfuge only where it is justified in the public interest and the material cannot be obtained by other means.

The law can still impose costs. In *Food Lion, Inc. v. Capital Cities/ABC, Inc.* (1999), ABC journalists who took jobs at a supermarket chain to film food handling were held liable for breach of the duty of loyalty and trespass, though not for the damage to the company's reputation caused by the broadcast itself. The case shows that even investigations that expose genuine problems can lead to liability for the methods used.

Undercover policing and entrapment

Police use of undercover officers is governed by specific laws and court doctrines. Courts in many jurisdictions exclude evidence or stay prosecutions where officers induced a person to commit an offence that they would not otherwise have committed. In the United States, the entrapment defence focuses on whether the defendant was predisposed to commit the crime (*Sorrells v. United States*, 1932; *Jacobson v. United States*, 1992). In England and Wales, the House of Lords held that it is not acceptable for the state to lure citizens into committing acts forbidden by law and then to prosecute them, while accepting that officers may provide an ordinary opportunity to commit an offence (*Attorney General's Reference (No 3 of 2000)*, 2001).

Ross (2008) compares American and European approaches to undercover policing and shows how the legal controls differ, with European systems tending to require more advance authorisation. In the United Kingdom, the Regulation of Investigatory Powers Act 2000 requires authorisation for the use of covert human intelligence sources by public

authorities. Long-term undercover operations against protest groups, in which officers formed intimate relationships with women under false identities, led to a public inquiry, which has found that such deployments could not be justified (Undercover Policing Inquiry, 2023). The case shows how deception, once authorised, can extend far beyond what the public would accept.

Deception online

Social media have created new opportunities for deception. Investigators may be tempted to create fictitious profiles, sometimes called "sock puppets", to view private accounts, join closed groups or befriend the subject of an investigation. Much of this raises the same questions as offline deception, with added complications. Most platforms prohibit fake accounts in their terms of service. Information obtained by tricking a person into accepting a friend request is information that the person chose not to share publicly, so obtaining it is closer to pretexting than to observing public behaviour.

Professional bodies for lawyers have addressed the issue directly. The Philadelphia Bar Association's Professional Guidance Committee (2009) advised that a lawyer could not ask a third party to send a friend request to a witness without revealing that the purpose was to obtain information for litigation, because doing so would be deceptive. The New York City Bar Association (2010) reached a similar conclusion, while accepting that a lawyer or investigator may send a truthful friend request under their real name without stating the purpose. Investigators should treat closed online spaces as private and use only information that is genuinely public or that has been shared with them honestly.

The consequences of crossing the line

The consequences of unlawful deception can be severe and can fall on the client as well as the investigator. They include criminal prosecution under pretexting and data protection laws; civil claims for invasion of privacy, breach of confidence or fraud; exclusion of the evidence obtained, which may destroy the case it was meant to support; professional discipline for lawyers who directed or knowingly used the deception; regulatory penalties; and reputational damage, which in the Hewlett-Packard case far outweighed whatever the investigation discovered about the original leaks. Organisations that commission investigations should therefore require written assurances about methods, ask how each piece of information was obtained, and refuse to accept material whose origin cannot be explained.

Defending against pretexting

Organisations that hold confidential information are the targets of pretexting as well as potential users of it. Banks, telephone companies, hospitals and employers can reduce the risk by verifying identity before releasing information, training staff to recognise common manipulation techniques such as false urgency and claims of authority, limiting what can be disclosed by telephone, and monitoring for repeated or unusual requests (Hadnagy, 2018). Testing staff with simulated pretexting calls, with appropriate safeguards and consent from the organisation, is now a common part of security assessments.

Research and mystery shopping

Researchers and businesses also use deception. Audit studies of discrimination and mystery shopping involve posing as customers or applicants. Research ethics frameworks permit such methods when their value is significant, no non-deceptive method would work, and harm is low (Bulmer, 1982; Calvey, 2017). The market research industry's code accepts mystery shopping to assess organisations, but requires that it not be used to deceive individuals in ways that harm them, and that staff be informed in general terms that mystery shopping may occur if results are to be used in assessing them (ESOMAR, 2016).

A practical test

Drawing these sources together, investigators and their clients can apply a series of questions before using any deception.

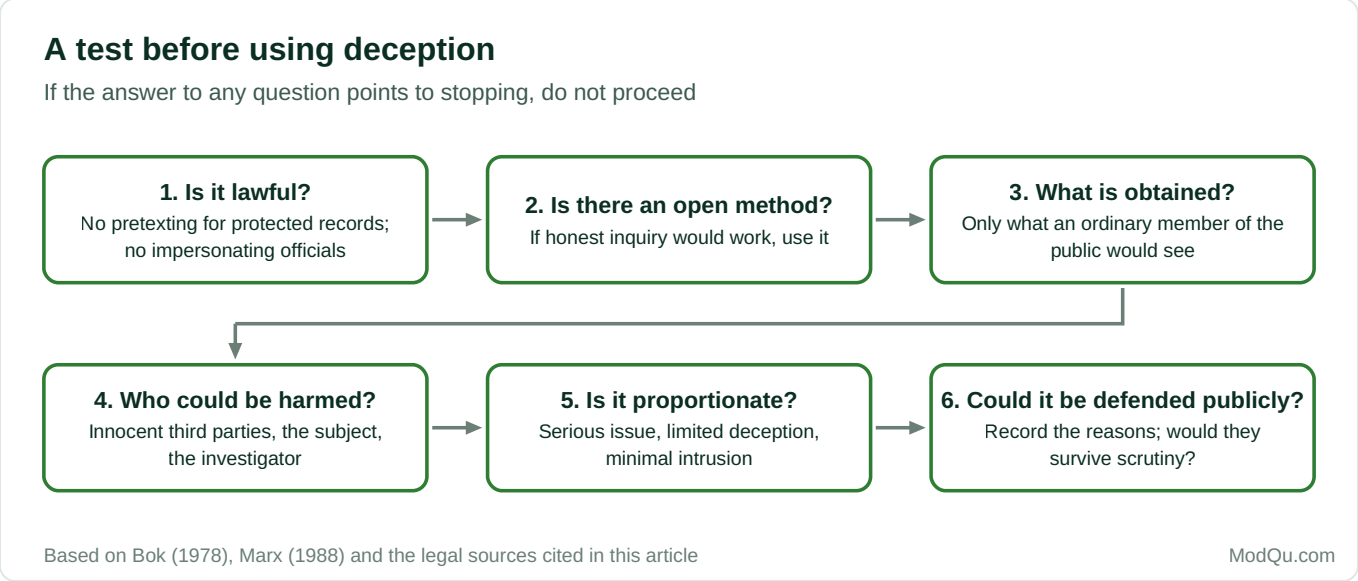


Figure 2. Six questions to ask before using deception. The first is decisive: no public interest argument makes pretexting for protected records lawful. Diagram by ModQu.

First, is it lawful? If the deception would obtain financial, telephone, medical or other protected records, or involves impersonating a police officer or official, the answer is no, whatever the purpose.

Second, is there an open alternative? Bok's (1978) first test applies: if the information can be obtained truthfully, deception is not justified.

Third, what will be obtained? Posing as an ordinary customer to see how a business treats the public is very different from using a false identity to obtain information the business would give only to its own staff or to the account holder.

Fourth, who could be harmed? Consider the people deceived, third parties whose information may be exposed, the subject of the investigation and the investigator.

Fifth, is it proportionate? The seriousness of the issue should justify the degree of deception and intrusion.

Sixth, could it be defended publicly? Record the reasons for using deception at the time. If the justification would embarrass the client if it were published, stop.

A short example

The following hypothetical case illustrates the test. A company suspects that a former employee has set up a competing business using its confidential customer list. Its lawyer suggests hiring an investigator.

The investigator proposes three steps. First, searching company records and the competitor's website, which is lawful and open. Second, having an investigator contact the competitor as a prospective customer to ask about its services and prices, recording only what the competitor would tell any prospective customer. Third, calling the former employee's mobile phone provider, posing as the former employee, to obtain a list of the numbers he has called, to see whether he has been contacting the company's customers.

Applying the test, the company approves the first two steps and rejects the third. Obtaining telephone records by impersonation would be a criminal offence in many jurisdictions and would expose the company to liability. Instead, the company's lawyers ask the court for an order requiring the former employee to disclose his customer contacts. The customer enquiry reveals that the competitor is offering the company's own customers specific discounts that could only be based on confidential pricing information, which supports the application. The court grants the order, and the evidence obtained is admissible.

Conclusion

Deception is sometimes a necessary tool for exposing wrongdoing that would otherwise remain hidden, and the law and professional codes allow limited forms of it, such as posing as an ordinary customer or, in serious cases, undercover work. But pretexting to obtain protected records crosses a clear legal line in many countries, and scandals from Hewlett-Packard to the trade in personal information show the damage it causes to the people deceived, to the clients who commission it and to public trust in investigation. Investigators and their clients should apply a simple discipline: use open methods wherever possible, never use deception to obtain information the law protects, keep deception to the minimum needed, and record reasons that could be defended in public.

References

American Bar Association. (2020). *Model rules of professional conduct*.

Apple Corps Ltd. v. International Collectors Society, 15 F. Supp. 2d 456 (D.N.J. 1998).

Attorney General's Reference (No 3 of 2000) [2001] UKHL 53.

Bok, S. (1978). *Lying: Moral choice in public and private life*. Pantheon Books.

Bulmer, M. (1982). When is disguise justified? Alternatives to covert participant observation. *Qualitative Sociology, 5*(4), 251–264. https://doi.org/10.1007/BF00986753

Calvey, D. (2017). *Covert research: The art, politics and ethics of undercover fieldwork*. SAGE.

Committee on Energy and Commerce. (2006). *Hewlett-Packard's pretexting scandal* (Hearing before the Subcommittee on Oversight and Investigations, 109th Cong.). U.S. House of Representatives.

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

ESOMAR. (2016). *ICC/ESOMAR international code on market, opinion and social research and data analytics*.

Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505 (4th Cir. 1999).

Gidatex, S.r.L. v. Campaniello Imports, Ltd., 82 F. Supp. 2d 119 (S.D.N.Y. 1999).

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

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

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

Independent Press Standards Organisation. (2021). *Editors' code of practice*.

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

In re Gatti, 330 Or. 517, 8 P.3d 966 (2000).

Jacobson v. United States, 503 U.S. 540 (1992).

Leveson, B. (2012). *An inquiry into the culture, practices and ethics of the press* (HC 780). The Stationery Office.

Marx, G. T. (1988). *Undercover: Police surveillance in America*. University of California Press.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.

New York City Bar Association. (2010). *Formal opinion 2010-2: Obtaining evidence from social networking websites*. Committee on Professional and Judicial Ethics.

Philadelphia Bar Association Professional Guidance Committee. (2009). *Opinion 2009-02*.

Regulation of Investigatory Powers Act 2000, c. 23 (UK).

Ross, J. E. (2008). Undercover policing and the shifting terms of scholarly debate: The United States and Europe in counterpoint. *Annual Review of Law and Social Science, 4*, 239–273. https://doi.org/10.1146/annurev.lawsocsci.3.081806.112803

Society of Professional Journalists. (2014). *SPJ code of ethics*.

Sorrells v. United States, 287 U.S. 435 (1932).

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

Undercover Policing Inquiry. (2023). *Tranche 1 interim report*.