Litigation & Arbitration Group

Milbank

Client Alert

Dos and Don’ts when using private investigators – some cautionary tales

12 March 2020

Key Contacts

Mona Vaswani
Partner
+44 207 615 3002
mvaswani@milbank.com

Joel Harrison
Partner
+44 207 615 3015
jharrison@milbank.com

Ulrike Friese-Dormann
Partner
+49 89 255593640
ufriese@milbank.com

Katie Goldstein
Partner
+1 212 530 5138
kgoldstein@milbank.com

Mark Padley
Associate
+44 207 615 3121
mpadley@milbank.com

Private investigators can provide crucial evidence needed to uncover and prove fraud or pursue litigation. They are also frequently used to conduct due diligence on counter parties in commercial and financial transactions. However, their use, and the techniques employed by some investigators, increasingly carry reputational, regulatory and legal risks for those instructing them.

In a number of recent cases, private investigators have been accused of posing as relatives to gain access to a private Caribbean island, installing camouflaged cameras on private property and chasing a former bank employee through the streets of Zurich. In another case, an employee of a litigation funder allegedly traded confidential information received in one case for video material of a sexual nature relevant to another case. Members of a wealthy family have also this year been embroiled in a case relating to the bugging of the Ritz hotel in London, which they own. A prominent lawyer in the US was also implicated in spying on journalists who were investigating his client’s alleged sexual misconduct. These incidents have resulted in claims for harassment, trespass, breach of confidence and breaches of data protection legislation, as well as investigations by public prosecutors and regulators.

While some of this activity is clearly illegal, in an industry that remains largely unregulated and fragmented, it is not always clear what methods private investigators are proposing to use and what they are legally able to do. It is, therefore, crucial to understand who will be investigating, what they will do, restrictions under local law and the wider implications of using them in the event that their use is publicised.

We discuss below some of the key issues that arise when using a private investigator:

Appointing a private investigator

Before appointing a private investigator, due diligence should be undertaken to ascertain the investigator’s areas of specialisation, years of experience, data protection training, liability insurance coverage, absence of a criminal record, client references and willingness to appear as a witness in court proceedings. Membership of a professional association is also a useful indicator of integrity and competence. For

example, the Association of British Investigators (ABI) mandates that members comply with its by-laws, which set out ten principles – including honesty, thoroughness and compliance with the law.[1] It is also important to consider not only the credentials of the company that is being appointed, but who will actually undertake the work, due to the frequent use of sub-contractors in the industry.[2] We advise having written engagement terms in place which expressly state that the private investigator will not, and it will ensure that none of its sub-contractors will, carry out any illegal activity in connection with the mandate and will observe all applicable laws.

Illegal activity

Whilst physical surveillance itself is not illegal in England (though it is in a number of other jurisdictions), protections for the privacy of individuals have increased considerably in recent years and in some cases it can give rise to claims including for harassment, trespass, breach of confidence and the misuse of private information (which has its roots in Article 8 of the Human Rights Act 1998). Certain activities may also attract criminal liability under the Investigatory Powers Act ("IPA") 2016, the Computer Misuse Act ("CMA") 1990, Bribery Act 2010 and the Data Protection Act ("DPA") 2018. Examples of conduct that would cross the line include:

- hacking into voicemails or intercepting telephone calls, which may constitute criminal offences under Section 3 IPA 2016 (punishable by up to 2 years imprisonment or a fine);[3]
- hacking into a computer or email account, which may constitute an offence under Sections 1-3 CMA 1990 (punishable by up to 12 months imprisonment or a fine);
- paying public officials or employees for confidential information, which may constitute an offence under Section 1 of the Bribery Act 2010 (punishable by up to 10 years imprisonment or a fine);
- taking items from rubbish bins, which may constitute theft or engage the laws of trespass; and[4]
- "pretexting" or "blagging", where information is obtained by deception, which may constitute an offence under the DPA 2018 (as to which, see below) or the offence of fraud by false representation under Section 2 of the Fraud Act 2006.

As indicated above, surveillance may become problematic if it crosses the line into harassment. For example, repeated surveillance of an individual which is likely, or designed, to cause distress or to intimidate, may amount to harassment.[5] Similarly, while making secret recordings for personal use may not

---

1 The Law Society of England and Wales endorses and recommends that solicitors use investigators who are members of the ABI. The ABI's by-laws can be found here: https://www.theabi.org.uk/assets/uploads/Policies%20and%20Guidance/BYE-LAWS.pdf

2 See report of the House of Commons Home Affairs Committee on Private Investigators dated 6 July 2012 at [22].

3 As to civil liability, see the phone hacking case of *Gulati and others v MGN Newspapers* [2015] EWHC 1482 (Ch) and, on appeal, *Representative Claimants v MGN Ltd* [2015] EWCA Civ 1291.

4 Placing something in a rubbish bin does not necessarily mean that it has been abandoned and it will remain the property of the individual or company that has placed it in the rubbish bin for collection. See *Williams v Phillips* (1957) 41 Cr App Rep 5, DC and a more recent case where taking food from a rubbish bin outside of Tesco was alleged to be theft. Some investigators may get around this issue by "borrowing" the item and photocopying it, then returning it to the rubbish bin.

5 See the case of *Howlett v Holding* [2006] EWHC 41 (QB) where the judge noted that "*to keep someone on tenterhooks, knowing that she is likely to be watched as she goes about her daily life, seems to me remarkably cruel*".

be criminal, it may give rise to liability for breach of confidence, the misuse of private information or under the data protection legislation discussed below.[6]

It is worth emphasising that this activity will not only result in liability for the private investigator, but may also result in liability for the organisation or individual that has appointed them. For example, in a recent case where information received in relation to one claim was traded for video material of a sexual nature relevant to another claim, the party that had engaged the investigator was sued for breach of the confidentiality provisions in the settlement agreement that had ended the first claim.

Data protection considerations

The appointing party and the private investigator will also need to comply with data protection legislation, particularly the General Data Protection Regulation ("**GDPR**") and the DPA 2018. Conducting investigations into an individual will necessarily result in the processing of their personal data, which is very widely defined under the GDPR[7], and in many cases the GDPR will apply to that processing[8].In circumstances where the GDPR applies, it will be necessary to identify a lawful basis for the processing. In most cases this will be the legitimate interests basis, which requires that there is a legitimate interest in the processing of data (such as the investigation of suspected wrongdoing), that the processing is necessary for purposes of this interest, and that this interest has been balanced against the interests of the individual whose data is being processed.[9]

The GDPR's data protection principles will also need to be adhered to, particularly the principle of data minimisation which requires that the processing of personal data is limited to what is necessary to achieve the intended purpose. For example, a private investigator may uncover compromising personal data which is not relevant to the investigation – such data should not be retained.

Consideration should also be given to whether 'special category' data is being collected (such as data that reveals racial or ethnic origin, political opinions or religious beliefs, or data that pertains to health or sexual orientation). The processing of such data will need to benefit from one of the exceptions in Article 9(2), GDPR. The most likely to apply is the exception where processing is necessary for the establishment, exercise or defence of legal claims.[10]

Where personal data is being processed, it is advisable to keep a record of the assessment made as to the applicability of the legitimate interests basis (where this is the lawful basis under the GDPR), in addition to the other records required in relation to compliance with the GDPR more generally. Failure to comply with the GDPR may result in claims for compensation by individuals[11] or a monetary penalty by the Information Commissioner. Many of the criminal activities listed above are also likely to constitute an offence of unlawfully obtaining, disclosing, or procuring the disclosure of personal data without consent (punishable by an unlimited fine).[12] In 2017 a firm of loss adjusters was found guilty of unlawfully disclosing personal data obtained by private investigators, following a prosecution brought by the Information Commissioner

---

6 See the case of *Mustard v Flower and others* [2019] EWHC 2623 (QB), in which a claimant was permitted to use secret recordings made for personal use. See, however, the case of *DSM SFG Group Holdings Ltd v Kelly* [2019] EWCA Civ 2256, where the court refused a claimant permission to rely on covert recordings of confidential conversations (most of them privileged) in order to bring claims.

7 Articles 4(1) and 4(2), GDPR.

8 GDPR applies to processing of personal data carried out wholly or partly by automated means, and also to non-automated processing where the personal data forms part of a filing system or is intended to form part of a filing system; see Article 2(1), GDPR (and Article 4(6) in relation to filing systems).

9 Article 6(1)(f), GDPR.

10 Article 9(2)(f), GDPR.

11 Article 82(1) GDPR.

12 Sections 170(1) and 196, DPA 2018.

under the prior data protection legislation; senior personnel of the firm, as well as the private investigators themselves, were also convicted.

It is important to note that the individual being investigated may be able to request disclosure of material collected and stored on him or her, by making a subject access request of the appointing party or the private investigator[13]; in our experience, fraudsters often do so to try and put the Claimant on the defensive as to any legal or regulatory breaches they may have been concerned in.

Regulatory considerations

Firms regulated by the FCA should have regard to their obligations in the FCA Handbook. The FCA has paid particular attention to the use of private investigators in the insurance industry, but its guidance as to the applicable principles has wider application. In particular, a firm should approach the appointment of a private investigator as it would any other delegated or outsourced activity. This will include conducting appropriate due diligence of the service provider and ensuring that the arrangement allows the firm to monitor and control its operational risk exposure relating to the appointment of the private investigator.[14] A firm will also need to ensure that the private investigator acts with integrity (Principle 1) and, where a firm is investigating its own customers, it should have regard to Principle 6, treating customers fairly.

Firms should also ensure that they have adequate procedures in place to prevent bribery (Section 7, Bribery Act 2010), given the risk that disreputable private investigators could resort to bribery to obtain confidential information.

Directors may also be at risk of being disqualified where their conduct, or the conduct they authorise, is illegal or falls below expected standards of commercial morality. Similarly, lawyers may be in breach of professional conduct rules where they are complicit in misleading, dishonest or deceitful conduct on the part of private investigators.[15]

Admissibility of evidence in court proceedings

In civil proceedings in England and Wales, there is no absolute rule against the admissibility of evidence obtained unlawfully (save in certain narrow circumstances).[16] However, under CPR 32.1(2) the court has a discretion to exclude evidence and will generally weigh the public interest in discouraging the unlawful conduct by which the evidence was obtained and the public interest in establishing the truth in the proceedings.[17] Therefore, there is a risk that a court will exclude evidence that has been obtained unlawfully, potentially jeopardising the proceedings.

---

13 See, for example, *Gurieva & Anor v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB).

14 See FCA Factsheet 031, https://www.fca.org.uk/publication/other/factsheet-031.pdf and the 2016 and the FCA's guidance on outsourcing claim activities to private investigators, https://www.fca.org.uk/firms/outsourcing-claim-activities-private-investigators.

15 See, in England, the SRA Code of Conduct for Solicitors, paragraph 1.4 and the New York Bar Association's rules of professional conduct which instruct lawyers to "[not] *engage in any conduct involving dishonesty, fraud, deceit, or misrepresentation*".

16 See, for example, Section 56 of the Investigatory Powers Act 2016, pursuant to which certain unlawfully intercepted communications will be inadmissible when they have been collected by a defined list of state authorities.

17 See the leading Court of Appeal case of *Jones v University of Warwick* [2003] EWCA Civ 151, in which the court permitted the use of video evidence obtained by the defendant's enquiry agent who had obtained access to the claimant's home by posing as a market researcher. The court held that the conduct of the

Privilege

Legal advice privilege will not normally apply to communications with a third party, such as a private investigator. However, confidential communications with the investigator may be protected by litigation privilege if litigation is reasonably in contemplation and the communications are made for the sole or dominant purpose of conducting that litigation. Thought should therefore be given to whether the activities of the private investigator could be said to assist in an identifiable future claim and whether it is appropriate to specify this purpose in the terms of appointment of the investigator. It should also be noted that material gathered by the investigator, which was not originally privileged, will not become privileged simply because it has been collected by them for the purposes of the litigation.

Critically, though, the English courts have been willing to set aside privilege in communications with a private investigator and in their reports where the investigator broke the law or acted unethically – relying on the principle that there is no privilege in iniquity. So, if your investigator behaves improperly in gathering information for litigation, do not assume that your communications with him/her will be protected from disclosure. That disclosure could put an otherwise meritorious claimant on the back foot.

Global Contacts

London	10 Gresham Street, London EC2V 7JD	
Tom Canning	tcanning@milbank.com	+44-20-7615-3047
William Charles	wcharles@milbank.com	+44-20-7615-3076
Charles Evans	cevans@milbank.com	+44-20-7615-3090
Julian Stait	jstait@milbank.com	+44-20-7615-3005
Mona Vaswani	mvaswani@milbank.com	+44-20-7615-3002
New York	55 Hudson Yards, New York, NY 10001-2163	
Wayne M. Aaron	waaron@milbank.com	+1-212-530-5284
Antonia M. Apps	aapps@milbank.com	+1-212-530-5357
Thomas A. Arena	tarena@milbank.com	+1-212-530-5828
George S. Canellos *Global Head of Litigation*	gcanellos@milbank.com	+1-212-530-5792
James G. Cavoli	jcavoli@milbank.com	+1-212-530-5172
Scott A. Edelman *Firm Chairman*	sedelman@milbank.com	+1-212-530-5149
Adam Fee	afee@milbank.com	+1-212-530-5101
Christopher J. Gaspar	cgaspar@milbank.com	+1-212-530-5019
David R. Gelfand	dgelfand@milbank.com	+1-212-530-5520
Katherine R. Goldstein	kgoldstein@milbank.com	+1-212-530-5138
Robert C. Hora	rhora@milbank.com	+1-212-530-5170
Alexander Lees	alees@milbank.com	+1-212-530-5161
Grant Mainland	gmainland@milbank.com	+1-212-530-5251
Atara Miller	amiller@milbank.com	+1-212-530-5421
Sean M. Murphy	smurphy@milbank.com	+1-212-530-5688
Daniel Perry *Practice Group Leader*	dperry@milbank.com	+1-212-530-5083
Tawfiq S. Rangwala	trangwala@milbank.com	+1-212-530-5587
Stacey J. Rappaport	srappaport@milbank.com	+1-212-530-5347
Fiona A. Schaeffer	fschaeffer@milbank.com	+1-212-530-5651
Jed M. Schwartz	jschwartz@milbank.com	+1-212-530-5283
Alan J. Stone	astone@milbank.com	+1-212-530-5285
Errol B. Taylor	etaylor@milbank.com	+1-212-530-5545
Washington, DC	International Square Building, 1850 K Street, NW, Suite 1100, Washington, DC 20006	
David S. Cohen	dcohen2@milbank.com	+1-202-835-7517

Andrew M. Leblanc	aleblanc@milbank.com	+1-202-835-7574
Michael D. Nolan	mnolan@milbank.com	+1-202-835-7524
Aaron L. Renenger	arenenger@milbank.com	+1-202-835-7505
Los Angeles | 2029 Century Park East, 33rd Floor Los Angeles, CA 90067-3019		
Robert J. Liubicic	rliubicic@milbank.com	+1-424-386-4525
Jerry L. Marks	jmarks@milbank.com	+1-424-386-4550
Mark C. Scarsi	mscarsi@milbank.com	+1-424-386-4580

Litigation & Arbitration Group

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any of the members of our global Litigation & Arbitration Group.