



**NOTHING TO SEE HERE: IS
SURVEILLANCE DURING LITIGATION
INIQUITOUS CONDUCT OR A
LEGITIMATE INVESTIGATIVE PRACTICE?**

15 DECEMBER 2020

In pop culture at least, solving mysteries has always led investigators to sail close to the wind. A friend and fellow investigator pointed out recently that in one outing Sherlock Holmes stages an accident, lies to witness, is outed as a cocaine addict, daubs himself in fake blood, and tries to steal blackmail material. Modern consulting detectives are more scrupulous, if less likely to be serialised.

However, the recent judgment [Gerrard v ENRC and Diligence](#) has put a spotlight on a discreet area of investigation: surveillance activities in the context of litigation support. If George Herbert (17th century poet) was right and “*the life of spies is to know, not to be known*” then this judgement provides an interesting insight into the modern-day exploits of the second oldest profession.

By way of a quick precis, Mr and Mrs Gerrard brought claims against ENRC and Diligence for breaches of data protection law, misuse of private information, harassment and trespass arising from surveillance activities provided by Diligence. The defendants sought to have these claims struck out, but were unsuccessful in this application. These allegations, like others pertaining to the case, will ultimately be determined at trial, after disclosure.

Some legal commentary has already leaped to suggest this could be the death knell for surveillance in litigation - and that this will give lawyers pause for thought before instructing surveillance. While this may be the case, it is hard to imagine that they will be put off entirely. The details of this particular case notwithstanding, some forms of surveillance can provide intelligence that can materially impact proceedings. Investigators are also unlikely to stop selling these services. It is a lucrative market. A high-level estimate based on Chambers-ranked firms suggests that the total revenue of the UK corporate intelligence market comprises nearly 5% of the revenue of UK dispute resolution law firms.

We may ultimately look back on this case as a cautionary tale more than a turning point, but there are certainly lessons to be learned.

Look for kite marks that justify confidence in conduct. If surveillance is to be conducted lawfully it should be reasonable, proportionate and with the express intention of gathering evidence for use in proceedings. It must have courtroom utility. The costs and risk of challenge need to be assessed against the probative value. If the surveillance is subject to a successful challenge of harassment, it may yet damage your case or reputation if the work was subject to disclosure (or press attention). A well-regulated practice will be aware of how to advise on risks as well as benefits - and will suggest other options if the work is unlikely to yield a genuine benefit.

The risks are much higher than other forms of investigation. Even the best laid plans go awry, and surveillance leaves a greater scope for both accident and human error. Events occur that are outside of a team’s control, they may ‘improvise’ in response, and inadvertently open the door to allegations of “iniquitous conduct”. This could expose a client to liability and threaten litigation privilege. Facts can be checked ‘in the moment’ from a smartphone, lies unravel easily, and increased awareness of countersurveillance can expose devices that were thought hidden, and these can be subject to forensic examination. There is also a heightened risk of disclosure of communications about activities which, as noted above, may or may not fall under legal privilege.

The press love a spy story. It goes without saying that if “prolonged surveillance” is exposed, the interest will extend beyond the courtroom. Anyone inclined to browse the 100-page judgment released will spot the intrigue, and so will the press: London hotels, Caribbean islands, tracking devices, night vision binoculars, alleged sham job interviews. One of the questions raised in these proceedings is whether such conduct constituted harassment. Whatever the outcome, the challenge itself invited the court of public opinion to speculate and debate what might be “genuinely offensive and unacceptable behaviour”.

Misconduct in these areas opens the door to tactical litigation. It was suggested that Mr and Mrs Gerrard may be using the present proceedings as a means of gaining access to certain documents that may be relevant for the main proceedings (for which the harassment claim is something of a side show). Mr and Mrs Gerrard deny this. As the Judge pointed out, this claim had reputedly cost £4million although damages are only £100,000 - sometimes there is a broader agenda at play.

See no evil: reducing risk in the use of surveillance

Surveillance can be considered, but here are three key questions to consider:

1. Are all other investigative tactics exhausted? Very thorough online investigation can sometimes turn up a piece of evidence that moves the needle. OSINT may not have the James Bond connotations (though nice to see it featured in *Killing Eve*), but technical skills and lateral thinking can sometimes get the same answer with far less risk. Using some advanced internet searches, we recently identified the details of a meeting by a group of senior executives and government officials via

the visitor logs of the government body which were on the deep web.

2. Is the surveillance under consideration reasonable, proportionate and justifiable? Before work is undertaken on the project a 'risk committee' should challenge some of the assumptions and practices and look at balancing the competing rights and interests. This ensures any surveillance instructed is clear and purposeful, and avoids 'protracted' surveillance for diminishing returns and higher risks. Don't rely on litigation privilege, which may be challenged in any case.

3. Can you ensure the on-the-ground team will observe the chain of command and follow the brief? Surveillance work often gets subcontracted and instructions are lost along the way. Teams make 'in the moment' decisions that can backfire. It seems Mr Gerrard's suspicions were aroused when two men followed him into an empty restaurant and sat next to him. Even pre-Covid this stood out.

If you are not considering surveillance, but feel you may be a target of it you can consider counter-surveillance measures including bug sweeps of your home, office, or other relevant locations. Keep alert to unusual approaches and conduct open-source investigation into any unknown individuals who are suddenly keen to get to know you.

The case is far from closed. As noted in the judgement, Mr and Mrs Gerrard *may* succeed in demonstrating that the surveillance complained of in this instance constitutes harassment. However, this doesn't mean surveillance cannot be lawfully carried out in other circumstances. Each case will ultimately turn on its own facts. Still, there is no denying that the claim will likely bring to the fore - and into the public eye - many of the issues that have long been 'shop talk' for those of us pushing for greater transparency and debate on investigator conduct