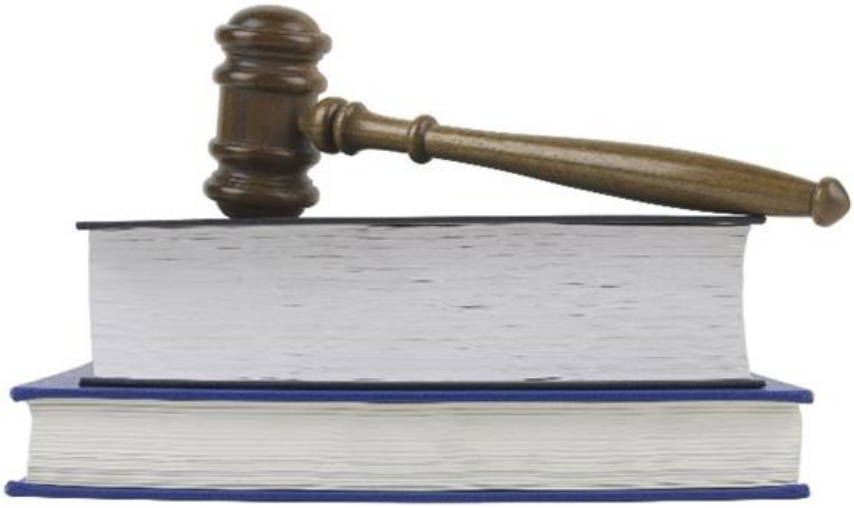
Article by **Andrew Willan, Associate in Dispute Resolution at Payne Hicks Beach** first published online by Writers Online on 29 October 2019 and reproduced with kind permission
https://www.writers-online.co.uk/how-to-write/the-law-for-writers-save-your-work/

WRITERS ONLINE *Helping you become a better writer*

Andrew Willan,
Associate Dispute Resolution

The law for writers - save your work



Protecting your intellectual property isn't all about rights - what are your legal safeguards against outright theft?

As the world has gone online, it has presented a raft of new opportunities for criminals looking to exploit weaknesses in cyber security. They prey on technological faults, human weakness and operate in the knowledge that under-resourced law enforcement authorities are struggling to keep up with the increasingly sophisticated world of cybercrime. The scale of the task can be measured by recent statistics that demonstrate that approximately half of all property crime now takes place online.

Bands such as Radiohead have seen hours of previously unreleased music stolen and used in an attempt to blackmail them. Most recently, it has been reported that Margaret Atwood was the victim of (apparently unsuccessful) attempts by cyber criminals to steal the manuscript for her latest novel, *The Testaments*. This article looks at the legal options available to those who find themselves on the receiving end of unlawful attempts to steal their intellectual property.

One of the most obvious difficulties in civil claims involving cybercrime is that, save for the most bungling criminals, tracking down the identities of those responsible will invariably be problematic.

There are however steps that can be taken to help to identify wrongdoers. Often the most effective steps is to seek from the Courts what is known as a “Norwich Pharmacal” order after the House of Lords case of Norwich Pharmacal v Commissioners of Customs & Excise [1974] UKHL 6. Where, for example, you have

been able to obtain an IP address or other information that may potentially lead to the identification of the individual, this can be an effective means of compelling ISPs (the companies that provide access to the internet) to disclose the identity of users to enable action to be brought against those responsible. Indeed, the process of seeking to expose the identity of a hacker and the threat of the liabilities they may face as a result can be an effective way of warning the hacker off from continuing their unlawful activities.

However, it may often be the case that the individuals have been sufficiently careful to obscure their identity. What, therefore, are the options if it remains impossible to identify those responsible? Ordinarily, an injunction (which, in essence, is an order requiring the defendant to take, or refrain from taking certain steps) is granted only against a named defendant. However, there are circumstances in which a claimant may seek an injunction against unidentified defendants, described in this jurisdiction as “Persons Unknown”.

In 2003, JK Rowling brought legal proceedings after copies of the fifth instalment of the Harry Potter series were taken away from the printers without authority and offered to the press at varying prices. The author successfully applied for an injunction preventing unauthorised publication of the book. The order she obtained extended to “Persons Unknown” defined as “the person or persons who have offered the publishers of the *Sun*, the *Daily Mail*, and the *Daily Mirror* newspapers a copy of the book *Harry Potter and the Order of the Phoenix* by JK Rowling or any part thereof and the person or persons who has or have physical possession of a copy of the said book or any part thereof”.

A person falling within this description could be found liable for contempt of court if he or she acted inconsistently with it. Likewise, any other person who, knowing of the order, assists in its breach may also be found liable for contempt of court. In appropriate circumstances, an even more wide-ranging order may be obtained “contra mundum”, that is against the “whole world”. This, in theory, would potentially place anybody who contravened the court order in breach of it and accordingly in contempt of court. Whilst this is the sort of sanction that might just make those directly involved think twice, it would also potentially make the wider public (including the press or any consumer looking to get their hands on the unlawfully obtained material) wary of their position.

It does beg the question though – how do you bring it to the attention of these “Persons Unknown”? The courts will require claimants to use their best endeavours to effect service of their claim and any order on the primary wrongdoers. Even social media has in the past been accepted to be an appropriate means of effecting service.

Where the theft of intellectual property has occurred outside your control, possibly on the computer system of a third party such as a publisher or record label, you may need to consider your rights under the relevant data protection legislation. In circumstances where your personal data (which is defined broadly as any information by which you are identifiable) has been unlawfully disclosed as a result of a data breach, you may be entitled to notification of information including the nature of the breach, the likely consequences of the breach and what is being done to mitigate against the adverse consequences of the breach. This information may be vital in terms of seeking to limit the potential damage. Depending on the

seriousness of the incident, you may in certain circumstances also be entitled to compensation.

Aside from the options available to a victim through the civil courts, there are also a number of practical steps they may wish to consider. One of the first ports of call will often be a report to the police. In the case of hacking or other data breaches, the wrongdoer may well have committed an offence under the Computer Misuse Act 1990. Amongst other matters, this legislation provides that it is an offence to cause "a computer to perform any function with intent to secure access to any program or data held in any computer the person is not authorised to access".

The involvement of law enforcement authorities may be important in cases where the unlawful activity has been conducted from abroad. The ability of law enforcement authorities to investigate and obtain evidence of cybercrime in other jurisdictions through mutual legal assistance channels can be particularly valuable where the enforcement of any civil order in a foreign jurisdiction is likely to be problematic. However, the UK police have faced much criticism for being ill-equipped and under-resourced to deal with sophisticated cybercrime perpetrated on a global level. Likewise, the Information Commissioner's Office is under resourced and overburdened with complaints about data misuse.

Or if you prefer to take matters into your own hands, there is the precedent set by Radiohead who were recently hacked by an unnamed person who reportedly asked for a $150,000 ransom to return the recordings they had stolen. Instead of agreeing to the hacker's demands and in order to take the wind from their sails, Radiohead instead took the innovative approach of releasing the material to the public and donating any profits to the climate activists, Extinction Rebellion.

The best way of warding off any attempt to steal intellectual property is to maintain adequate cyber security such as installing up-to-date anti-virus software and firewalls and using secure WiFi and stronger passwords.

However, in a world that is increasingly rife with online crime that is reaching new levels of sophistication (often out-stripping the capacity of law enforcement authorities), the question of how to protect intellectual property, and how to limit the damage when something goes awry, has never been more acute.

Andrew Willan is an Associate in the Media & Privacy team at Payne Hicks Beach

10 New Square, Lincoln's Inn, London WC2A 3QG
DX 40 London/Chancery Lane
Tel: 020 7465 4300 Fax: 020 7465 4400 www.phb.co.uk