Fields **Associates**
Litigation Consultants

Did your Client Really Create that File?

Only a few years ago solicitors and barristers representing individuals accused of having indecent images stored on their computer's hard drives would advise their clients to plead guilty irrespective of their client's protestations. To some, this will come as no surprise. A significant portion of the population would assume that any kind of digital file, whether an image, word document or other type of file could not be found in a device's storage media unless it had been created or downloaded by an end user – most likely the device's owner.

It could be argued that the accused was not responsible for the presence of the data and that, as alluded to previously, it had been created by another individual who had access to the device in question. This is perfectly plausible, of course, but it is still extremely difficult to prove. But did you know that it is possible that illegal data could have found its way onto the relevant storage media without the intervention of either the device's owner or, indeed, anyone else with access to the device – at least not directly.

When an individual uses the internet, they are, if the correct security software is not installed on their device, susceptible to any number of viruses. Some of these viruses, known as Trojan horses or Trojans, can, if they infect the device in question, result in files appearing in a system without the user's knowledge.
Consider, for example, whether you've ever been told that you need to download a certain file before you can view a webpage, or if you've ever received a spam email from someone who you know and whose email address was in your address book. The former is a clear example of how a Trojan horse virus can find its way onto someone's hard drive whilst the latter shows the ease with which they can be circulated.

In some if not many instances Trojan horse viruses can be relatively innocuous. Many hackers utilise them solely to annoy end users by turning web pages upside down, affecting mouse movements or playing sounds repetitively. Some, however, utilise them in order to gather sensitive data such as passwords and debit/credit card information. Others afford hackers remote use of the infected device effectively turning its hard drive into a proxy storage device within which nefarious individuals could store any number of illegal images or other incriminating documents. All whilst the mechanism's owner is oblivious to the fact that illegal material is regularly being downloaded to their hard drive.

Quite literally any computer can become infected by a Trojan horse and the vast majority of people will have files that they have neither downloaded nor created lurking somewhere in their computer's hard drives. Fortunately, these files will rarely be incriminating and a relatively small number of people will face charges as a result of them. Those that do, however, will be hard pressed to explain their presence.

Sometimes files can appear in hard drives without the involvement of hackers, though. When you visit a website, the image files present on

the page are stored in the device's temporary internet file. Now, imagine if you were to visit a site by accident – or were redirected to one – which contained illegal images. These images would be stored in your temporary internet folder until you removed them and, as this could potentially serve as proof of the fact that you created indecent images, you could then be prosecuted under the Protection of Children Act 1978.
If either set of circumstances outlined above applied then an accused would not be guilty of downloading – and therefore creating – an indecent image as they would not have knowingly either viewed and/or downloaded such an image. In spite of this, many of these individuals would (and perhaps still will) be advised to plead guilty by their representatives.
On a final note, it must be added that there are numerous other reasons why an incriminating file may be present on any form of storage media without the appellant's knowledge, and under no circumstances should an individual that finds themselves accused of possessing illegal data be advised to plead guilty before significant investigations into the relevant media have been undertaken.