This issue marks the beginning of a new era in our legal coverage. Following the departure of our long-standing columnist, Cytringan, we are pleased to announce that QEB Hollis Whiteman Chambers and Gough Square Chambers will be taking it in turns to fill his shoes. QEB kicks off the first article in our Legal Perspectives section.

DMITRIY SHIRONOSOV / SHUTTERSTOCK.COM

Making more than friends from Facebook

Social networking sites can be a great source of evidence, but there are legal pitfalls, say Adam King and Mark Aldred

The use of evidence from social networking sites, particularly Facebook, is nothing new. But it is not always obvious how to obtain such evidence lawfully. As with any other type of surveillance the provisions of Regulation of Investigatory Powers Act 2000 (RIPA) must be carefully considered.

The first question you might ask is whether you need an authorisation for 'directed surveillance' under s.28. S.26(2), which defines 'directed surveillance' as covert surveillance where *private information* is likely to be obtained.

Now, if you are merely looking at a public profile you may think that you are safe – especially considering Facebook's terms of service, which states that where a user selects the public setting, they are allowing everyone, including non-users, to access and use their information.

But that is merely a contractual term – it does not settle the question whether the information is *private information* as far as RIPA is concerned. In fact, there are circumstances in which you are not *safe*, despite looking only at publicly available information: in the RIPA codes of practice there is no such black and white distinction drawn for offline, real world scenarios – and there is no reason to suppose the rules should be any different online.

An example is given (in paragraph 2.7 of the code for covert surveillance) of a person providing his name and telephone number to a shopkeeper. He may be doing this in a public place, but he is likely to have a reasonable expectation that the information is not being recorded by another person, for another purpose.

In *Wood vs Metropolitan Police* [2009] EWCA Civ 414 the Court of Appeal considered what constitutes private information in the context of Article 8 of the European Convention on Human Rights (ECHR). Their ruling will undoubtedly inform the interpretation of 'private information' in the domestic

context of RIPA. The case involved police taking photographs of arms trade protesters. The court held that the mere taking of the photographs in a public place did not engage Article 8 rights, but that the particular way in which the police subsequently retained and used them did; and, by a majority, that this retention and use was not, in the particular circumstances, proportionate.

Specific content

It is clear from the several recent cases that apply *Wood* that the question whether Article 8 is engaged is highly context specific, (in particular *R (RMC) vs Met Police* [2012] EWHC 1681 (Admin), *Catt vs ACPO* [2012] EWHC 1471 and *Hutcheson vs News Group Newspapers Ltd* [2011] EWCA Civ 808). In Catt, for instance, the fact that the protest organisation with which the claimant was associated was known to have a history of violence and criminality distinguished the case from *Wood* in two ways: that the public would expect the authorities to act as they did, and that the claimant did not have a reasonable expectation of privacy (see paragraph 43). In *Catt*, Article 8 was found not to be engaged.

It seems that publicly available information, whether it's online or on the street, can become 'private information' depending on how the information is stored and for what purpose. If, as a trading standards officer, you were to monitor a suspect's public Facebook profile over a period of time and record the information you found there for later analysis, you may well need an authorisation for directed surveillance – although the extent of your knowledge of the suspect's criminality is likely to be relevant (that is, how speculative the monitoring is), together with other circumstances.

What if the suspect is not so foolish as to leave the information you are looking for publicly available? First you will have to establish for yourself a fake profile, preferably with a large number of fake friends. Then you will have to 'add' the suspect as a friend, and hope he accepts. Do you need to obtain a RIPA authorisation to act as a Covert Human Intelligence Source (CHIS) to do even this?

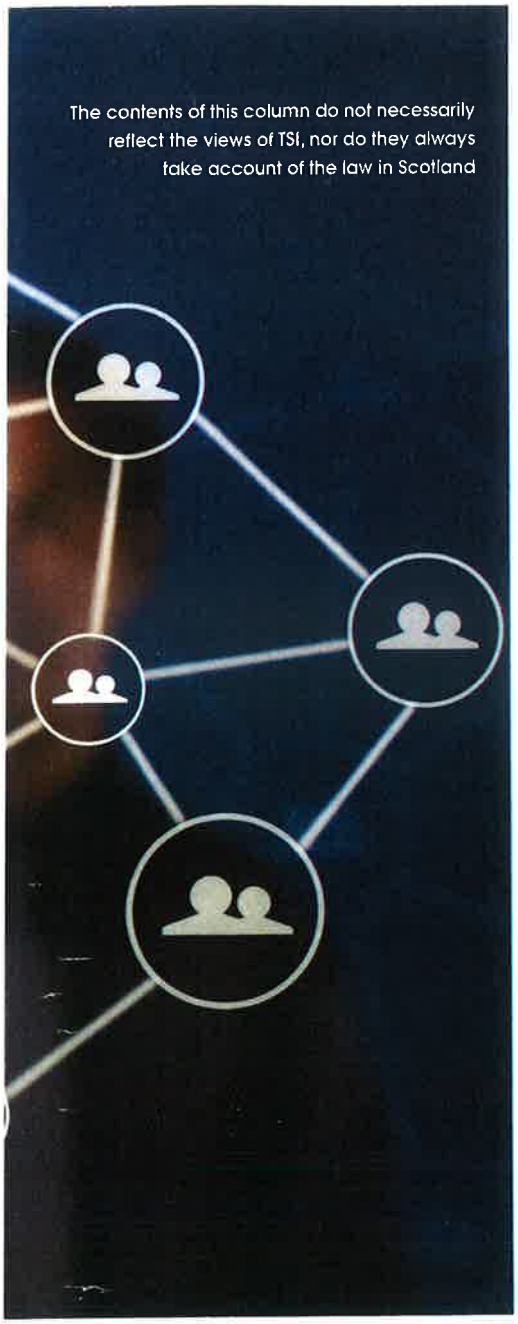
The simple answer is yes. The CHIS Code (para 2.12) draws a distinction between a test-purchase child going into an off-licence attempting to buy alcohol (no authorisation required) and a child going in repeatedly to build up trust before making an attempted purchase (authorisation required). For one thing, this distinction is not well supported by the definitions and detail in s.29 of the Act itself (although the code provides significant reassurance).

> In the RIPA codes of practice there is no such black and white distinction drawn for offline, real world scenarios

But that aside, imagine if, in real life, a shopkeeper had to provide the names and photographs of all his friends to a prospective customer before any sale could take place. This would, you might think, make it a relationship of some substance, and one that requires a CHIS authorisation. And remember, CHIS activity includes anything 'incidental' to the establishing or using of the relationship (s.26(7)). It is hard to conceive of any instance where adding a suspect (or non-suspect) as a friend as part of an investigation would not require a CHIS authorisation.

But would the owners of Facebook be happy with this kind of subterfuge? Paragraph 4.1 of their current terms of service suggests not: *'You will not provide any false personal information... or create an account for anyone other than yourself without permission.'* There is nothing to stop you asking for permission of course. But good luck, as they say, with that.

The contents of this column do not necessarily reflect the views of TSI, nor do they always take account of the law in Scotland



DUSIT / SHUTTERSTOCK.COM

Unauthorised access

But if you choose – as the police frequently do – to ignore this purported prohibition, are you in danger of committing a criminal offence? S1 Computer Misuse Act 1990 made it an offence to deliberately access unauthorised computer material.

The offence is generally aimed at hackers, but it is very broadly drafted, and 'unauthorised' is inadequately defined in the case law. There is an exemption for activity authorised by 'any enactment relating to powers of inspection, search or seizure', but a good argument could be made that RIPA is not such an act. The best course, therefore, is to obtain a RIPA authorisation where possible because, quite apart from anything else, s27 provides protection from civil and criminal liability for anything done in accordance with the authorisation. And this also goes for other criminal offences you might be worried about, such as s55 Data Protection Act 1998 (obtaining personal data without the consent of the data controller).

Note that the protection of s27 only applies where you are acting *in accordance with* the authorisation – it is not a *carte blanche* for all purposes. In s1 RIPA, for instance, the unlawful interception offence will still apply. You will not be prosecuted for reading messages on your suspect's 'wall'[1], but if somehow you obtained his password and then read messages in his inbox, then you could – your RIPA authorisation would not entitle you to do this (fairly obviously).

It should also be remembered that your RIPA authorisation will not permit unnecessary obtaining (much less retaining) of information. So if you keep a file of material from a Facebook Wall which, for instance, consist solely of obviously irrelevant exchanges between a suspect and his family, or between two people entirely unrelated to the investigation, these are best left alone as you will have neither the protection of s27 nor any 'necessary for the prevention or detection of crime' exemption, such as is found in the Data Protection Act.

> With careful consideration at the beginning of an investigation, there is no reason why even the smallest of teams should not feel comfortable gathering evidence from Facebook

Breaching rights

What happens if for some reason you fail to obtain a RIPA authorisation when you should have done? Well, it is not in fact mandatory (see s80): as a public body you are of course under a duty to obtain a RIPA authorisation where one is required, but failure to do so is not an offence, nor would it (without more) give rise to civil liability.

But despite the non-mandatory nature of the regime, where a public body acts without the protection of an authorisation and also breaches a person's ECHR rights, the Investigatory Powers Tribunal (IPT) has the power to issue a fine. Although it is perhaps worth noting that in the first 10 years of its existence there were fewer than 1,200 complaints to the IPT and only 10 of them were upheld – less than one per cent.

And might a failure to obtain authorisation affect the admissibility of the evidence obtained? *R vs Button* [2005] EWCA 516 would suggest not: the Court of Appeal held that the trial judge had not been wrong to decline to exclude under s78 PACE evidence, which had been obtained beyond the scope of the RIPA authorisation that had been granted, and which was therefore in breach of Article 8 of the ECHR.

That said, s78 applications are usually highly dependent on the facts of a particular case and there can be no doubt that failure to obtain, or acting beyond the scope of, a RIPA authorisation will be a clear point in the defendant's favour, and could easily tip the balance towards exclusion in the exercise of the trial judge's famously wide discretion. It would be a mistake to think that RIPA authorisations are irrelevant to the question of admissibility.

As ever, the speed of development of information and communication technology and the human behaviour dependent on it has far exceeded the speed of development of the law, and it could well be argued that RIPA is in need of updating. But until a regulatory framework specifically tailored to our online world is enacted we must work with what we have got.

In my opinion, it would be as great a failing to shy away entirely from investigating through the use of social networking sites, for fear of falling foul of some legal ambiguity or other, as it would be to blunder through willy-nilly on the grounds that probably nothing will go seriously wrong.

With careful consideration at the beginning of an investigation, there is no reason why even the smallest of teams should not feel comfortable gathering evidence from Facebook and other social networking sites.

ABOUT THE AUTHOR: Adam King and Mark Aldred are barristers at QEB Hollis Whiteman Chambers. Contact them at adam.king@qebhw.co.uk and mark.aldred@qebhw.co.uk

[1] See the article, *Social networking sites, RIPA and criminal investigations* by Michael O'Floinn and David Ormerod, Crim. L.R. 766 for a detailed discussion of this point