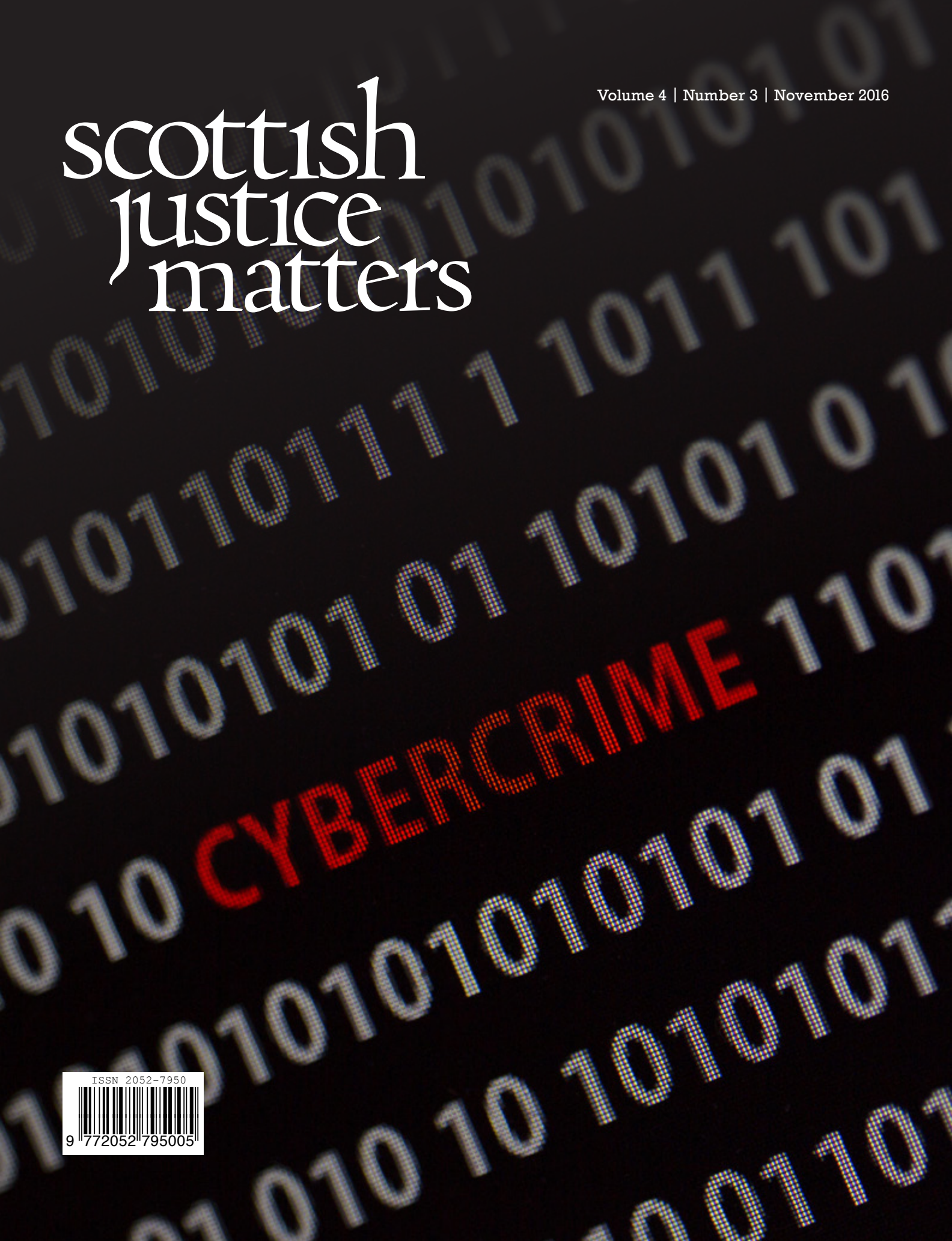
Volume 4 | Number 3 | November 2016

scottish justice matters



ISSN 2052-7950

THE CYBERCRIME PROCESS

A criminal defence perspective by **David Sinclair**

WE ARE a smartphone society. 70% of all adults own one: but that little device in your hand can be tantamount to holding a smoking gun when the police come knocking. In this article, I intend to explore a few of the issues that crop up when suspects are faced with this situation. I am a criminal defence solicitor and practise mainly in the sheriff court. I meet with clients and provide advice when they are detained by the police at the police station. I then consider the strengths and weaknesses of the case against them, advise accordingly and represent their interests at court.

When a person is detained by the police for an offence, a caution is administered by the police warning them that what they say may be noted down. The suspect will be taken in to police custody, they will routinely be searched and any items relevant to the inquiry can be examined for potential sources of evidence. During that detention period, the police may interview the suspect. An interview carried out under caution is an opportunity for the suspect to provide their side of the story should they so wish, but an inviolable right against self-incrimination must be preserved. There is every chance however that a suspect's phone will have all the answers wanted by the police, and potentially more.

As a society we have accepted the 'greater good' over individual privacy argument as it pertains to CCTV. But when detained on suspicion of an offence, what stands between your right to privacy and the state accessing the content of the smartphone? The police have a power to search and examine an accused for evidence. In cases where the police believe there may be physical evidence obtainable from the accused i.e. DNA traces on accused's body, a medical examination by a doctor will be required. An invasion of privacy of this nature requires either the consent of the suspect or warrant granted by a sheriff after applying a test of fairness.

Once the police have your phone can they do what they want with it? Well, we are policed by consent and if you consent to them examining it then yes, they can do what they want as per their statutory function to investigate crime. Your smartphone is capable of alerting police to an

astonishing amount of personal data but as to how much they are interested in it will be proportionate to the nature of the investigation: but that's hardly reassuring for those who find themselves at the wrong end of a false allegation.

Smartphones have their own protection against invasions of privacy - the passcode or lock screen protection. A cursory internet search suggests that around 30% of users do not have a lock on their phone. If the police can obtain access to the phone with a passcode it helps a whole lot but there is however the Regulation of Investigatory Powers Act 2000 at hand when a little more persuasion is needed. S.49 requires a person to disclose the 'key' to the protected information having been given formal notice to do so; failure to do so is an offence that can attract a two year custodial sentence (or five years where it relates to matters of national security). This, in my experience, is a seldom used provision perhaps because it is complicated and unwieldy for run of the mill cases.

The prevalence of cybercrime and digital evidence has increased markedly and so obtaining access to a suspect's phone is invaluable. The recent crime audit from HM Inspectorate of Constabulary in Scotland (2016) acknowledged that criminals are "increasingly exploiting opportunities from the internet to commit crime" and that Police Scotland continues to develop its response to "cyber-related offences". Activities, legitimate or otherwise, that one can undertake with a smartphone is ever increasing given that their capabilities include cameras, diaries, satnavs, address books, notepads all in one. Each would be of interest to a criminal investigation if searched for separately, so, to have it all contained in one device that is most commonly to be found on an accused's person removes a lot of the legwork. The focus of police investigation in to cybercrime and cyber-assisted crime has had to follow suit.

Once a device has been examined, the prosecution will receive a report prepared by the Technical Support Unit of the police which in turn is disclosed to the defence. This report is an edited highlights summary from the device that the reporting officer considers relevant to the case. And therein lies the rub. While I have no doubt that the investigating officer would be nothing but scrupulous in their consideration of what is relevant, my clients can be prone to disagree. This is particularly so when dealing with the all too prevalent domestic allegations where matters are fraught following messy relationship breakups and slanging matches are conducted electronically. In such situations I will instruct my own analysis of the device.

As I work exclusively in cases funded by the Scottish Legal Aid Board (SLAB), I require the prior authorisation from the Board to instruct a suitably qualified expert to carry out such an examination. This will almost always involve the expert travelling to the location where the device is being stored, liaise with the police analysts and extract all of the data on the phone. Mainly, my attention will have been drawn by the client to things that are missing from the Crown report; to attempt to retrieve things that have since been deleted or that may shed perhaps incriminatory actions in a different light. Wading through a full data dump is a laborious process but can reveal the odd nugget here and there. However, this raises the concern that as more cases rely on digital evidence, who has the time or resources to carry out a thorough examination?

The recent case of *JL and El v HMA* case before the Appeal Court showed that the complexities raised by smartphones have not escaped the attention of their Lordships. When two suspects were taken in to custody in respect of an allegation of a serious assault, an iPhone 5 was in the possession of one of the accused. We are told that the detainee gave no consent for the phone to be examined but that an electronic conversation had been recovered from the phone which disclosed incriminatory remarks attributable to both accused.

A detained person is subject to search by virtue of s.14(7)(b) of the Criminal Procedure (Scotland) Act 1995 which states that a constable may "exercise the same powers of search as are available following an arrest" which includes a power to examine. What that examination may entail depends, unsurprisingly, on what is to be examined and the information that it is hoped will be elicited, pretty much carte blanche one might say. But, consider this; is it the contents of the phone in the hands of the police that is being examined or is it the contents of a server located in some data warehouse in California? Alas, that was not ruled on in this case but the door appears to be open for a more rounded argument to be pursued in the future. What the court decided was that the phone is subject to examination as per the rules of detention. Their Lordships have been able to arrive at this position as the grounds of appeal and the facts before the court did not elucidate further on what steps were taken by the police to gain access to the phone, thus the court assumed that all that was undertaken was simply switching the phone on, like one of those 30% unsecured smartphones. That being so, the appeal court decided the case on basis of the previous authority *(Rollo v HMA)* from 1997 where a personal organiser (a Sharp Memo Master 500 for those who may be interested) was the smoking gun.

Other jurisdictions have taken a different tack and have recognised the difference between the static receptacle nature of a personal organiser and the infinitely more versatile and fluid capabilities of a smartphone. The US Supreme Court dealt with a case similar in facts to that above *(Riley v California)* and dismissed out of hand any notion of similarity between such devices stating that it was "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." The Supreme Court ruled such situations would require a judicially determined warrant to overcome the inherent fourth amendment right against unreasonable searches. It is hoped that clarity can be sought regarding the Scottish position soon; that may take the right case with the right set of circumstances for the matter to be revisited. Given the prominent role of digital evidence these days I would anticipate that that might not be far away.

David Sinclair is a public defence solicitor: dsinclair@pdso.org.uk

HMICS (2016) *Crime Audit 2016* http://bit.ly/2dc4wLa

JL and El v HMA [2014] HCJAC 35

Riley v California [2014] 573 US, 17

Rollo v HMA [1997] JC 23