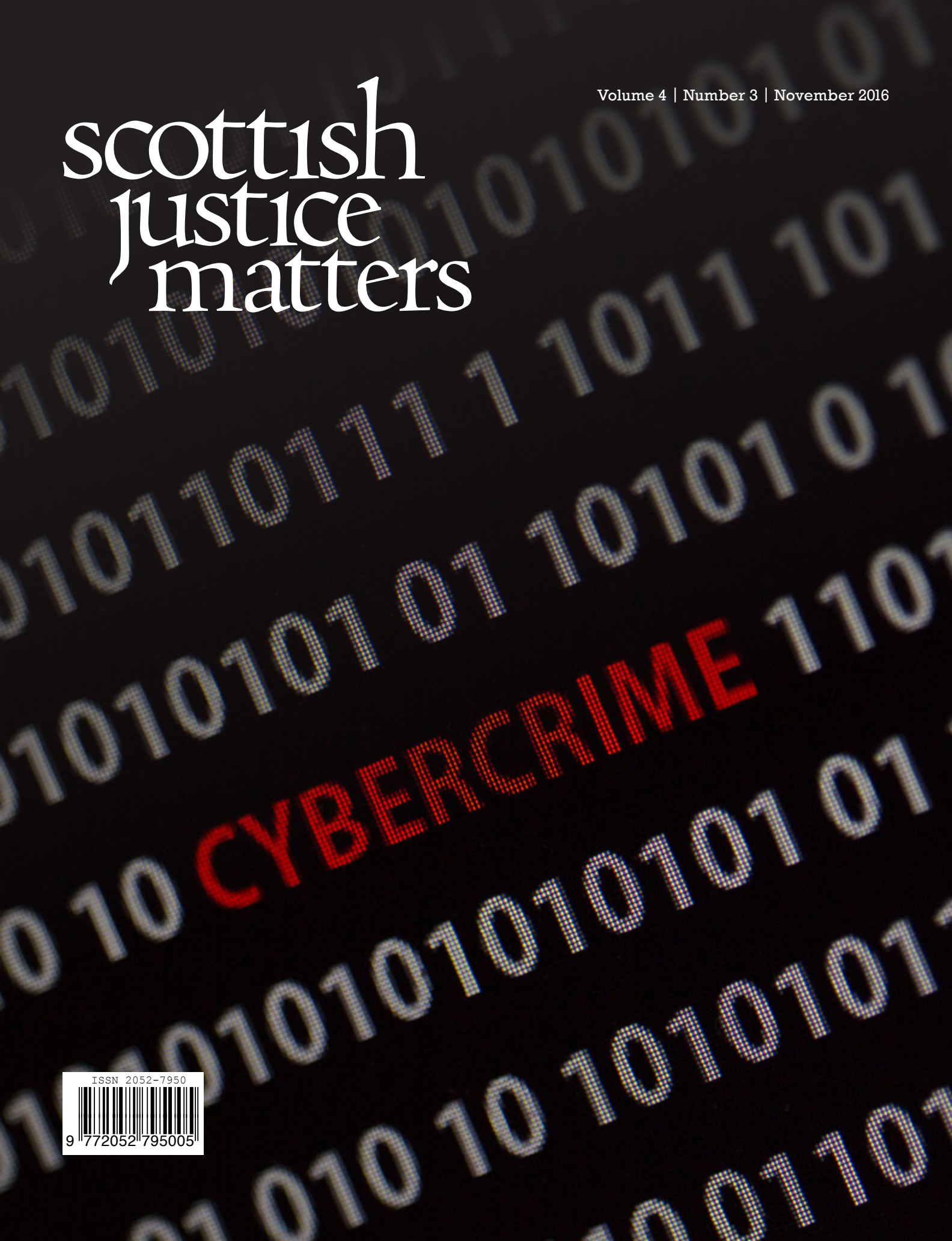
Volume 4 | Number 3 | November 2016

scottish justice matters



ISSN 2052-7950

PROSECUTING IN THE SOCIAL MEDIA SOCIETY

Scot Dignan introduces some of the issues faced by prosecutors when new media is involved

THERE ARE over four million 'likes' on Facebook every minute and 350 billion photos are uploaded daily, contributed by the 32 million of us in the UK who participate in this social-media phenomenon. Technology has changed the way we interact with each other and with our community; it has permeated every aspect of our social experience to the extent that we can easily state we live in a social-media society. Unfortunately as our society develops, as our technologies exponentially progress, there are those that would use these developments for ill: crime it seems has kept pace. In this article I discuss some of the issues that as a Procurator Fiscal Depute, prosecuting in the public interest, I am confronted with when prosecuting cybercrime and cyber-assisted crime in Scotland.

What do I mean by cybercrime and cyber-assisted crime? Cybercrime I would categorize as those cases in which the use of technology is central to the criminal act, for example downloading indecent images of children (prohibited under s52 of the Civic Government (Scotland) Act 1982). Cyber-assisted crime I would categorize as those cases in which the technology forms a part of the overall criminal act, but is not central to the commission of the offence: for example, if an accused acted in a threating and abusive manner towards an individual by shouting, swearing and then sending them an abusive and alarming Facebook post (prohibited under s38 of the Criminal Justice and Licensing (Scotland) Act 2010). Whether the technology requires to form part of a criminal prosecution will depend on the nature of the offence and the evidential value of the information retrieved.

Let us be clear however, with 70% of the adult population walking around with a Smartphone in their pocket, prosecutors are not seeking to seize and examine devices in every case, or even every cyber-assisted case, only those cases in which there would be strong evidential merit to do so. The decision to instruct seizure and examination is a difficult one and it is not one I as a prosecutor take lightly. It can cause economic and emotional upset. Often witnesses and victims of crime do not realise that by bringing a cybercrime or cyber-assisted crime to the attention of the police, it may be essential for police to seize their device as well as that of the accused for forensic examination and for trial, which can be a significant period of time in some cases (see also Sinclair, page 9).

Did s/he do it?

Once a device is seized, sent off for forensic examination and found to contain relevant information it is up to the prosecutor to determine the evidential weight of that information. In cybercrime and cyber-related crime the fundamental evidential challenge is proving the accused undertook the cyber-activity. Let me illustrate my point with two examples.

(a) Possession of Indecent Images of Children

Police, working on intelligence that indecent images of children have been downloaded at a property, obtain and execute a Sheriff search warrant on that property, and seize a computer. The property is a family home and the computer is seized from the 18-year-old son's bedroom. Forensic examination of the computer uncovers several indecent images of children. The Forensic Examiner in their cyber-report states how many indecent

images were found, which file they were found in and when the image files were created or downloaded. The son is detained, interviewed and makes no comment. How can the prosecution prove that the son was the person who downloaded the images, or even knew they were on his computer?

Ensuring that the cyber jargon is explained and is fully understandable is imperative in these cases

The prosecutors approach is deductive: eliminating the possibility as far as possible that it was someone other than the son who could have downloaded the images. This can involve taking statements from everyone else who resides at the house, and calling them as witnesses, in order to rule them out: ascertaining whether the computer was password protected and establishing who would know the password; inviting inference - it was found in the accused's room, it's not the family computer it's his personal computer, other files found on the computer, school essays, CVs etc., establishing he is the only user. In these types of cases, every detail matters.

Often juries, I suspect, want a definitive answer but the law, unlike the digital world, does not operate in the binary. Prosecutors cannot provide the scientific certainty too often expected in today's CSI society. We, as prosecutors, can only show the jury what was on the computer screen; we cannot show who sat before it. The rest is inferences, some more irresistible than others.

(b) Posting an abusive Facebook message

Bernard and Sandra Abernethy were in a relationship for five years, it ends badly and they are currently going through the courts for custody of their two children. Bernard receives a Facebook post from the account 'Sandra Abernethy', the post appears on his Facebook wall, and it blames him for all the marital problems and then threatens him with physical violence. Bernard calls the police and shows them the message on his smartphone; police seize Bernard's phone. Sandra is detained, interviewed, and states that she has a Facebook account, she accesses it through her own smartphone, and that there is no password on her smartphone. Police seize her smartphone.

In this scenario there is no dispute as to a message being posted on Bernard's wall or that it was posted by the account of Sandra Abernathy. The evidential challenge is proving, that Sandra was the one that posted it. It is not enough to conclude that it was Sandra's account so it had to be Sandra. Sandra's defence could be 'I left the phone on my desk at work and went to the bathroom, it must have been sent then'.

There are certain strands of evidence that the prosecutor can draw upon: that the account is in her name, that the account's profile picture displays a picture of the accused, and that the message contained marital information that would be peculiar to only those in their marriage. Once again when it comes to the identification of the cyber-criminal, detail and inference is key. It becomes even more complex when the accused denies the account: There are as many as 80 million fake Facebook accounts out there.

These two small examples hopefully give the reader an idea of the evidential difficulties facing prosecutors in cybercrime and cyber-assisted crime, and the level of creativity prosecutors must develop to deal with these evidential challenges.

In the public interest?

Once an evidential merit and sufficiency of evidence is established, it still falls to the prosecutor to decide if it is in the public interest to prosecute, to exercise prosecutorial discretion. Cybercrime and cyber-assisted crime cases are creating interesting new decisions for prosecutors, as we as a society decide how we wish to tackle this form of offending. For example, cases involving younger offenders using social media in an inappropriate manner (see Quayle page 17) raise important questions such as, are criminal proceedings in the overall interest of the public and public safety considering the evolving line between an act of immaturity, and an act of criminality? Also, can and should we establish criteria for those cases in which alternatives to prosecution may be more appropriate?

Presenting the evidence

Once the decision is made to take up a prosecution, perhaps one of the most interesting tasks when prosecuting cybercrime and cyber-assisted crime is presenting the evidence. Prosecutors must ensure the trier of fact understands the evidence, whether that is a Sheriff sitting alone or a jury of fifteen members of the public. One cannot take for granted that everyone knows what a USB or hard-drive is, or what Facebook or 'downloading' means. Social media and in particular social media devices, have become such a normalized part of our daily routine for many of us, that we take for granted sometimes that everyone is (a) also participating in this modern phenomenon, and (b) even if they are participating that they understand exactly how it works. The truth is if it works, people don't really care how it works. Ensuring that the cyber jargon is explained and is fully understandable is imperative in these cases.

As a prosecutor cybercrime and cyber-assisted crime is constantly posing new and interesting legal challenges. As a society we must realise that we are responsible for our online actions: what we 'like' on Facebook and how we use technology matters, and when that online action falls to be criminal, individuals must be held accountable. However, practitioners in the legal system must be wary of creating the perception that the technology in our pockets is a 'smoking-gun', ready to be used against us at the flick of a thumb. Fear breeds bad law and bad decisions, as US Supreme Court Justice Brandies famously stated, "Men feared witches and burnt women" *(Whitney v California)*.

Scot Dignan is a Procurator-Fiscal and has recently begun doctoral study at the University of Glasgow

Whitney v California 274 U.S. 357 (1927), pp376

Ofcom, The Communications Market Report, 2016
https://www.ofcom.org.uk/research-and-data/cmr/cmr16

Smith, Kit (2016). Marketing: 47 Facebook 2016 [Brandwatch.com]
https://www.brandwatch.com/2016/05/47-facebook-statistics-2016/