**Social media in court: your tweets could be used as evidence against you**

June 22, 2018 12.22pm BST

As we increasingly use social media platforms such as Facebook, Twitter, Instagram and WhatsApp to communicate with each other, many of us are unaware of the ways in which our posts might later resurface – and get us into trouble with the law.

There are numerous examples of social media being used as evidence in the criminal justice system, leading to convictions and sometimes prison sentences. Peter Nunn from Bristol, England, was imprisoned in 2014 after MP Stella Creasy and feminist Caroline Criado-Perez were subjected to a string of abuse on Twitter. And after the London riots of 2011, two men were imprisoned for incitement after posting messages on Facebook inviting those who read them to meet the next day and wreak havoc in their local town. Police were able to trace the messages back to the defendants, leading to successful prosecutions.

Messages and media on WhatsApp, Snapchat and the like, have been used in evidence to show that defendants have committed offences, such as selling drugs, possession of firearms (as in the case of R v Noble and Johnson, where WhatsApp messages from a girlfriend of a defendant were admitted into evidence as they suggested that he had a firearm), harassment , or serious assaults.

In 2015, Portsmouth Magistrates’ Court heard that Alan Wilson of Hilsea had sent his ex-partner 143 abusive messages via WhatsApp. These were used in evidence against him.

It is important to realise that where social media messages are retrieved and show that a criminal offence has occurred they can either be cited as direct evidence of a crime being committed, or as circumstantial evidence – for example, a fingerprint identified from a photo of a man’s palm on a WhatsApp message helped convict a drug dealer in April 2018. Even where messages contain elements of hearsay, it is open for the court to decide whether to admit such messages at trial.

***Not criminal, but defamatory?***

Even where criminal consequences do not follow, lurking behind the scenes is the possible threat of defamation cases. In 2017 Monroe v Hopkins – a libel action brought by writer and food blogger Jack Monroe against the Daily Mail columnist Katie Hopkins – Mr Justice Warby, sitting in the High Court, warned that even where “a person can have a low opinion of another … the other’s reputation can still be harmed by a fresh defamatory allegation”.

The judge stressed that it also remains the “responsibility of the litigant to retain and preserve material that may become disclosable”. The judge also warned about the responsibilities that the claimant’s solicitor has in taking reasonable steps to make sure that their client understands this responsibility and carries it out. In other words it’s important not to delete potentially defamatory threads and to take screenshots of messages for possible use as evidence.

***Encryption and recovery***

Among other communication platforms, WhatsApp has in recent years implemented end-to-end encryption for messages. This ensures the messages are unreadable as they are transmitted via myriad private and public networks en route to the intended recipients. They are encrypted before they leave the source device and decrypted only once they reach their destination. While this should protect the messages in the event they are intercepted, messages may still be retrievable by using various forensic recovery methods.

Forensic recovery has featured in large-scale drug cases, indecent images and terrorism offences among others. Where devices are encrypted and passwords or keys are not provided, suspects may be served with a disclosure notice under Section 49 of the Regulatory of Investigatory Powers Act 2000. Failure to reveal such passwords attracts a criminal penalty.

In the absence of the key or password, there may still be a way to break into communications devices. The San Bernardino shootings in 2015 led the FBI to seek a court order against Apple to assist them in their efforts to unlock a deceased terrorist’s iPhone. In the event, the FBI withdrew their application after a third-party firm was reported to have broken into the handset on their behalf.

It is important to realise that once a message on social media is posted or sent, there is little or nothing the author can do to prevent it becoming part of the public record – whether that is due to its addition to a freely available and/or widely viewed social media profile, or because the receiving party, or the police, have produced it as evidence of wrongdoing. Months and even years later, when people have moved on with their lives, these can and do resurface with a wide range of consequences.

And it’s important to remember that the technology of today that is used to encrypt and protect our communications, may be no match for the technology of next week, month or decade, which might be used to defeat that protection, revealing past thoughts and opinions to the world.