Augmenting reality—avoiding criminal liability

20/10/2016

IP & IT analysis: As part of our augmented reality (AR) series, Ian Whitehurst, barrister at 6 Pump Court and 7 Harrington Street, considers some of the potential criminal law issues surrounding the development of AR.

What is AR?

AR has been defined as 'a real time direct or indirect view of a physical real world environment that has been enhanced/augmented by adding virtual computer generated information to it'. AR is related to the more generalised concept of mediated reality where a computer can modify or even diminish a view of reality.

In plain English, the best way to think about what AR is comes through considering an example of the technology. The recent Pokemon Go app has been a massive success and it uses AR in an ingenious way—when a Pokemon is nearby, players can hold their mobile telephones up and the screen shows their physical surroundings (through the camera) but with a Pokemon overlaid and often dancing around in the 'real world'.

How can or will AR be deployed?

The uses in theory are limitless ranging from advertising, to film to medicine and even deployment by the military. From a criminal law perspective, the immediate uses are in relation to facial recognition of suspects believed to be involved in criminal activity.

Facial recognition software is developing to such an extent that a person can potentially now simply hold their mobile telephone up and be informed, in real time, who they are looking at, where they are from and what their job is. This will raise considerable issues surrounding the existing case law contained in the Police and Criminal Evidence Act 1984 relating to the stop and seizure of suspects and their subsequent formal identification.

Can the use of AR technology directed at a specific individual (to track, record) attract criminal liability?

If AR is being used by a private individual or corporation to track the location of an individual or record their actions and behaviour and obtain access to confidential information relating to them, it is arguable that they are committing criminal offences.

By using AR in the manner described above, they are doing so without the consent of the individual and are clearly breaching their right to privacy. It would be open to the individual to report them to the police for offences in relation to public order and/or harassment. Furthermore, dependent upon what data is collected and how, the activities might also be a criminal offence under section 55 of the Data Protection Act 1998.

In relation to state authorities deploying this technology against individuals suspected of being involved in criminal activities, it would be necessary to amend the existing statutory regime. The Regulation of Investigatory Powers Act 2000 is in place to facilitate covert surveillance to expressly cover the deployment of AR against individuals/organised crime groups suspected of being involved in criminal activity.

What are the issues around 'digital assault' eg, the hacking of software programmes and using AR to induce seizures and to scare the user of the software?

Using AR in this form would seem unfortunately to be the next step in cyber criminality or cyber terrorism being deployed by various individuals or organisations once the technology and its accessibility catches up with their criminal intent and enterprises.

At present, under English law an assault is committed when a person intentionally or recklessly causes another to apprehend the immediate infliction of unlawful force.

Inducing a physical reaction triggered through AR or some other computer application may very well fall foul of the law as constituting an assault.

In order to combat the specific nature and method of delivery of the assault as well as jurisdictional issues surrounding its commissions (these threats could be aimed at someone in the UK but delivered by someone in the US via a server in the EU), it is likely to be vital that specific new legislation is drafted to address these issues which will manifest themselves in the near future.

The government has to stop being reactive in this field of practice—the interface between technology and crime—and start to plan and consider the ways to stop AR being used for criminal purposes on a pro-active level.

Could using VR headsets in trials at court to project a digital 3D version of a crime scene assist lawyers and jurors in making decisions and are there any drawbacks to employing technology in these settings?

The use of VR headsets for jurors and all parties to the criminal trial process seems potentially to be the next step in ensuring effective case management and presentation. The courts, for example, have long been assisted with the use of CCTV footage in relation to the capturing of criminal acts. This seems the next logical technological step.

However, the key concern is that, by relying upon AR, all parties must be sure that the technology has not inadvertently modified or diminished the reality to such an extent that it impacts in a prejudicial manner on the jury and affects their ability to make a decision based on their own common sense and experiences of the real world.

An over reliance on technology could not only undermine a juror's decision but the very basis of the jury system itself.

What are the trends for the future?

An increasing amount of our lives is now played out on or through a computer and the amount of data held about ourselves is rapidly building. Data is never absolutely 'secure' but there are degrees of security and risk.

When 'lost' data ends up in the wrong hands, it can be coupled with AR technology to allow a person to make quick decisions based on information passing across their field of vision (via a handset or mobile telephone), therefore maximising their criminal gain.

How this will develop is difficult to predict. However, criminals may be able to scan customers waiting at ATMs to determine whether they have enough money in their accounts to be worthwhile to rob. Also, criminals may access GPS material from police units in order to avoid capture and plan a quick escape route from the scene of a crime.

Finally, it may be well lead to criminality being punished and dealt with on the street and in the communities where it has taken place by police officers using AR to transmit the commission of crimes straight into the courtroom for a judge to determine culpability and punishment and for the police to enforce the sentence.

Ian is a barrister specialising in serious organised crime, fraud, regulatory law and cyber crime.

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor