An affair to remember--cyber crime implications of the Ashley Madison hack

02/09/2015

Crime analysis: In the wake of the Ashley Madison hacking affair, Matthew Richardson, a barrister at Henderson Chambers, considers the criminal law implications and looks at how computer crime legislation is developing to deal with these types of issues.

What offence have the hackers committed by capturing and releasing account details associated with the Ashley Madison site?

It is clear that, given the business model of Ashley Madison, privacy is key to their clientele. It is safe to assume that the massive breach of data that occurred recently was not an authorised use of the Ashley Madison system.

The most obvious offences committed by the Ashley Madison hackers are offences under the Computer Misuse Act 1990, ss 1-3 (CMA 1990). These offences primarily concern the unauthorised access to a computer system although they differ slightly in their scope.

Section 1

CMA 1990, s 1 creates the statutory offence of unauthorised access to a computer system. The actus reus of the offence under CMA 1990, s 1 is substantiated by causing a computer to perform 'any function' in order to secure access to it. In practice, therefore, the actus reus can be substantiated by relatively innocuous acts. The interpretive provisions under CMA 1990, s 17 provide that 'A person secures access to any program or data held in a computer if by causing a computer to perform any function he' uses the data, copies it from one medium to another or outputs it.

A person convicted of the CMA 1990, s 1 offence could expect two years at Her Majesty's Pleasure on indictment--there are currently sentencing guidelines for this offence but it is likely that, given the scope and damage caused, this would be at the higher end of the scale.

Section 2

CMA 1990, s 2 (unauthorised access with intent to commit or facilitate further offences) is the cyber equivalent of 'going equipped'. The offence is basically the same as the CMA 1990, s 1 offence but with the additional mental element of intention to commit further offences.

It is likely that this offence was not a single breach event and planning and previous access is likely to have been involved--therefore, CMA 1990, s 2 is likely to be engaged. This offence carries a maximum sentence of five years in jail. There are no guidelines but this offence is likely to be at the top end.

Section 3

CMA 1990, s 3 (unauthorised acts with intent to impair, or recklessness as to the impairment, of a computer) is, as it sounds, an offence which adds in the additional mental element of impairing the function of a computer system. It is clear that the Ashley Madison hack caused significant impairment of the system and it is likely it is still broken. This offence carries with it a far more severe penalty of ten years in jail.

It has long been argued by many senior law enforcement and legal commentators, including Adrian Leppard, commissioner of the City of London Police, that offences like the Ashley Madison hack should be considered as terrorism offences under the Terrorism Acts 2000 and 2006 (TA 2000 and TA 2006). The elements of the offence are such that they would probably fall under the ambit of TA 2006.

TA 2000, s 1 creates an offence of terrorism in which a person interferes with or disrupts an electronic system for the purposes of intimidating a section of the public for the advancement of a political, religious or ideological cause. In the case of Ashley Madison it could be argued that these provisions are met as the perpetrator has publicly sought to shame and intimidate these people into halting their use of the site, as they believe that extramarital affairs are wrong.

Additionally, there are offences under the Protection from Harassment Act 1997 and fraud offences--not to mention potential offences relating to the deaths of those people who have killed themselves since their names were exposed.

What are the challenges in identifying hackers?

The hackers themselves, given the sophistication of the hack, are likely to be very capable and will have taken many steps to hide their identities. This will mean using multiple proxy servers in multiple, unhelpful, jurisdictions, using hijacked, zombie computers or 'botnets' and doing everything they can to avoid being caught.

Given the level of planning that goes into a hack like this, the hackers will have had to use bots (zombie computers) and there will have been some record of this hack and multiple people will know about it.

It is unlikely to have been a state-sponsored attack and so the perpetrators may be identifiable not by the hack itself but by the preparatory steps, and dissemination of the hacked material.

If found to be located outside of the jurisdiction, could prosecuting authorities of different jurisdictions work together to bring a case against the hacker(s)?

There has of late been much more co-ordination between cyber crime forces in the UK and abroad. A number of treaties and conventions govern the policing of cross border crime and world leading cyber crime detection and monitoring like that of the City of London Police is exported to other jurisdictions through a series of training programs.

If the perpetrators are found to be in a jurisdiction that is friendly or signatory to a convention or treaty to extradite them, it is possible that they will be brought to justice. If they are in a country like Korea, Syria, Iran or other unfriendly country, they will likely escape justice.

Could individuals who have signed up to the site face criminal prosecutions in any jurisdictions?

Not in most jurisdictions, but it is possible that they may find themselves on the wrong end of a divorce settlement.

Have there been any examples of successful prosecution of hackers?

The law and detection method are still catching up with the online criminals, but slowly and surely the number of prosecutions of these kinds of cases is on the rise. As courts, lawyers and police start to understand these types of crimes more there will be more and more prosecutions. It is possible that the lack of understanding within the police, Crown Prosecution Service (CPS) and judiciary have allowed hackers who should have been prosecuted and convicted to walk away.

How is the criminal law developing in this area?

Given the seriousness of the hack and that several people have reportedly taken their lives as a result, it is possible that the hackers could be the first to face the brand new offence under CMA 1990, s 3ZA (unauthorised acts causing, or creating risk of, serious damage) which was added by the Serious Crime Act 2015 in May 2015.

A person is guilty of an offence if:

- the person does any unauthorised act in relation to a computer
- at the time of doing the act the person knows that it is unauthorised
- the act causes, or creates a significant risk of, serious damage of a material kind, and
- the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused

Damage is of a 'material kind' if it is damage to human welfare, the environment, the economy of any country or the national security of any country.

Serious damage to human welfare can be:

- loss to human life
- human illness or injury
- disruption of a supply of money, food, water, energy or fuel
- disruption of a system of communication
- disruption of facilities for transport, or
- disruption of services relating to health

This is an indictable only offence and can result in up to 14 years in jail.

The new offence created has not yet been prosecuted and, given that the other new offence in CMA 1990, s 3A (inserted by the Police and Justice Act 2006), has only been prosecuted once, it is possible that the lack of understanding of the CPS and police in this field has led to an offence which is often breached but rarely prosecuted.

Legislators seem to be keeping up with the times in the creation and definition of these offences and one hopes that the enforcement side of the equation can keep up too.

Interviewed by Alex Heshmaty.

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