CYBERCRIME LECTURE

9 BEDFORD ROW LONDON WC1R 4AZ

THURSDAY 4TH OCTOBER 2018

ADRIAN AMER

BARRISTER-AT-LAW

MEMBER OF THE CRIMINAL BAR ASSOCIATION

MEMBER OF THE CHARTERED INSTITUTE FOR SECURITIES AND INVESTMENT

ELEMENTS OF CYBERCRIME

Elements mean elements

I have specifically chosen a **General Overview of Cybercrime** in this lecture. I of course do not intend to cover every single aspect of cybercrime in it. For example, in this lecture I will not be covering elements of what cyber security is and how to manage it nor its relationship with financial crime. Those topics can be covered on another day. In any event I would probably need a full day to do that in any meaningful way. However this lecture may be useful to you as an introduction to certain areas of general cybercrime that may also be relevant to you both at work and at home.

GENERAL

1. **Cybercrime is an all encompassing legal topic**. It has the capacity to affect almost every area of the law and society. It crosses over and transverses civil, company, commercial and intellectual property law. Its reach is never ending and continually expanding. The extent of cybercrime is only matched by the ingenuity and creativity of the perpetrator and the lack of awareness of the victim. Its effect is all encompassing and has the ability to affect everyone and all walks of life and much human activity.
2. **There is a craving for a one stop non-shop definition of cybercrime**. There is none. There can be none due to the ingenuity of the perpetrator and lack of awareness of the victim. Cybercrime itself is a continually evolving subject, scenario and phenomenon. **It cannot be pigeon holed in time and place**. Our culture and civilisation has developed to the extent that in some way shape form or other we rely on computers, computerisation, electronic communications in all and various forms and all aspects of digitalisation. Whether it be travelling on the underground, switching on our computer at work, buying our food from the supermarket, using banking facilities, travelling overseas, trading or manufacturing, using national and international trade, making or threatening war, utilising aeronautics, or simply using Facebook, Instagram, Twitter and emails to communicate with each other or others we may wish to reach out to. The computer and electronic technology to achieve all this and more in a civil and peaceful society is no less than mind boggling and extraordinary. The fact that it can still exist in any war torn society or country ravaged by civil war is no less than a miracle.
3. **It is extraordinary because it is happening all around us every minute of the day without us necessarily thinking about it or being aware of it**. It is because of this general lack of awareness

whether it be in specific or general terms that cybercrime occurs and consciously and/or subconsciously, depending on the level of perceived risk by ourselves and institutions such as large and small, national and international, global firms and corporations and financial institutions that cybercrime is perfectly suited to the modern world in which we live. In my view other than using totalitarian methods which of course would be unacceptable to modern western democracies cybercrime can never now be obliterated but only ameliorated. Cybercrime of course is only an extension of criminal activity that has always existed. The difference now is its strength and potential sophistication matched by any user naivity, ignorance, lack of diligence, helplessness which only serves to encourage more cybercrime. For example, the world financial system is daily, by the hour and the minute constantly attacked by cyber criminals. If the true extent of the problem were ever truly revealed by the banks, there would be a loss of confidence in the world financial system and it would collapse in its present form. However, to be fair to the banks, they are extremely aware of the problem and they are doing everything in their power to prevent any major catastrophe as a result of cybercrime. The only greater threat to the financial system may be simple human greed.

4. **Therefore what is cybercrime?** My very simple and perhaps not altogether very useful definition is any intentional or reckless act caused by a perpetrator by means of a computer or computerisation or by way of any electronic means which causes loss, damage or harm to any victim or any potential loss, damage or harm to a victim. Loss, damage or harm isn't necessarily confined to physical, financial, or structural harm. It can be mental, psychological, emotional harm as we see in victims in sex cases in court. Even in fraud cases where financial loss can be great or small, the impact upon the victims can be devastating, especially where the victims are elderly, life savings are stolen, and dreams for the future are destroyed. Fake investing in

pyramid schemes or presumably ecologically sound but non-existent or fake schemes and the like can be devastating to the loser.

5. On Monday September 17th 2018 The Times reported '' **Blackmail threat over web use in 'sextortion' scam** by Mark Bridge Technology Correspondent. Email scammers based overseas have extorted hundreds and thousands of pounds in bitcoins by claiming to have evidence of victims' pornography use after quoting their passwords. The scam is part of a wider trend for 'sextortion' and webcam blackmail, with 1,304 cases reported to the police last year, up from 428 in 2015. Police say that the numbers represent the '' tip of the iceberg'', as many victims do not come forward. At least five suicides in Britain have been linked to the crime.
6. Banbreach, a security firm, identified hundreds of **bitcoin wallets** associated with the latest variant of the scam, with total takings above £382,000. Suman Kar, its chief executive, told the Motherboard website that the money was siphoned with ''very little effort''. In some sex extortion scams hackers do obtain webcam footage of victims, but experts said this was not the case in the recent, widely circulated version. **The criminals appear plausible because they quote personal details, falsely implying they have gained access to the victim's computer**.
7. **The passwords or numbers** were obtained by other criminals in data breaches of companies such as Linked-In and purchased by the scammers on the **dark web**. A typical email begins by quoting a current or old password or mobile number of the recipient. The criminals claim to have obtained webcam footage of the victim and access to their email and Facebook contacts. They threaten to send the footage to these contacts if the victim does not send a payment of hundreds of pounds in bitcoins to an account in one day.

8. This month **an inquest** heard that a 56 year old man drowned in a river after being targeted by online blackmailers thought to be based in Iran. The man from Leominster in Herefordshire was found dead days after he received an anonymous email demanding a bitcoin ransom. It was not stated in court whether the scam was sex extortion specifically and the police did not comment on the matter.
9. Detective Constable Theresa Wood of West Mercia Police said 'the man had been sent an email from an unknown person who made a **demand for some money over the internet in bitcoin**. The email stated if he didn't comply and make this payment everybody in his phone contacts would find what he had been using the internet for'. Ms Wood added after the inquest which returned an open verdict, the victim's phone was not found to contain any inappropriate comment.
10. Detective Chief Inspector Rik Klair of West Mercia Police said ''**Cybercrime**, including **cyber-enabled blackmail and sextortion**, can cause a huge amount of distress to both the victims and their loved ones. If you do become a victim of cybercrime there are people that can help. It's very important that you do not suffer in silence. Do not pay any money and contact police'',''.

11. **Note the very real and key words in this tragic cybercrime incident**:

BLACKMAIL/THREAT/WEB/SEXTORTION/SCAM/EMAILS/SCAMMERS/EXTORTED/BITCOINS/PORNOGRAPHY/PASSWORDS/TIP OF ICEBERG/VICTIMS/SUICIDES/SIPHONED/HACKERS/WEBCAM/PERSONAL DETAILS/FALSELY IMPLYING/ACCESS/CRIMINALS/DATA BREACHES/LINKED-IN/DARKWEB/MOBILE NUMBER/FACEBOOK/CONTACTS/PAYMENT/INQUEST/TARGETED/ONLINE/ANONYMOUS/RANSOM/UNKNOWN

PERSON/DEMAND/MONEY/INTERNET/CYBERCRIME/CYBER-ENABLED/ CRIME/DISTRESS/LOVED ONES etc .

One only needs a cursory glance at these words to understand and realise that many if not most of those words and phrases apply to most if not all cybercrimes covering all aspects of society and all human activity. It is not purely and soley criminal in its scope.

12. **Some characteristics of cybercrime**, notwithstanding any particular definition are the **scale, accessibility, anonymity**, **portability, transferability and global reach** : **Clough (2010**). Technological advancement and progress can also be considered another characteristic of cybercrime. It is the basis or platform upon which all cybercrime is committed. Cybercrime is not confined to just individuals though; large corporations and companies of any size can be as equally if not more culpable, particular with regards to invasion of privacy. Note with interest the recent Facebook transgressions and its connection with Cambridge Analytica, a firm not based in Cambridge of course but firmly in the heart of London. All these breaches, whether small or large have demonstrable consequences under the **Data Protection Act 2018 and associated General Data Protection Regulations** as well in associated company and financial regulations.

13. **Numerous statutes cover the legal jursidiction of cybercrime**:

    1. **The Computer Misuse Act 1990** covering unauthorised access to computer materials (**section 1**); unauthorised access with intent to commit or facilitate commission of further offences (**section 2**); unauthorised acts with intent or recklessness to impair operation of computer (**section 3**); making, supplying or obtaining articles for use in an offence (**section 3A**).
    2. **Data Protection Act 2018 and GDPR**
    3. **Misconduct in a Public Office: common law**
    4. **Investigatory Powers Act 2016**

5. **Fraud Act 2006**

6. **The Sexual offences Act 2003.**

The majority of cybercrime and cybercrime related offences that appear in the criminal courts are of course the **Fraud and Sexual Offences Acts**. It remains to be seen whether the **Information Commission Office** will step up their present prosecutorial regime or whether it will maintain an educative and penal approach. Large security data breaches of course will be pursued if not for no other reason to demonstrate to industry and the public at large the seriousness of the breaches. It goes without saying, the earlier the breaches are reported, the more lenient the ICO will be. That can potentially translate into a saving of hundreds of thousands if not millions of pounds in penalties.

14. **Cyberterrorism and cyberwarfare and hacktivism** and the use of the internet by terrorists is a cheap and easy way to reach a large audience and in quick time. Lets also not forget emails, texts, Whats App, Snapchat and all manner of social media networks in the commission of these offences. Propaganda, fundraising, disseminating information, secure communications, gathering intelligence are all methods that are used in order to facilitate such cybercrimes. Main legislation in this area are the **Terrorism Acts 2000 and 2006. Section 5 Terrorism Act 2006** criminalises preparatory acts. Where a person 'engages in any conduct' in preparation for giving effect to the committing of acts of terrorism or assisting another to commit such acts an offence is committed (**section 5 (1**). **Section 56 Terrorism Act 2000** could include websites linked to terrorist organisations where a person 'directs at any level the activities of an organisation which is concerned in the acts of terrorism'. This would include raising finance or creating or maintaining a website for the purposes of terrorism.

15. The Ubiquity of Fraud

Types of online fraud are never ending: most develop quite simply with the most harmful of effects: where a relationship is developed between scammer and victim, filling in of an on-line employment application, obligation to pay a fee in advance, subscribing to a particular web site, ringing a particular number at cost, **phishing, spear phishing, pharming and spoofing**, auction frauds, charity frauds, Ponzi schemes, get rich quick schemes, romance frauds and the list goes on and on. If any type of human behaviour can be deceived online there will surely be a fraudulent activity to benefit from it. Often benefitting from an appeal to the emotions, greed, loneliness, fear, embarrassment and shame. Ignorance and naivity, lack of time to act and investigate, and little due diligence all have their part to play. **The Fraud Act 2006** is a powerful tool in the combating of cybercrime. Unfortunately for political, social, financial and economic reasons it is only a drop in the ocean when compared to the amount of cybercrime committed. The bottom line is that few cybercriminals are caught, and less are prosecuted due to the cost of prosecuting them. However, at least there is the prospect that such a good legal tool exists and will be continued to be used given the sufficiency of time, money and political will. Convictions can be obtained for fraud by false representation (**section 2**), failure to disclose information (**section 3**), fraud by abuse of position (**section 4**), obtaining services dishonestly (**section 11**); **conspiracy to defraud** at common law: **R v Wellman [2007] EWCA Crim 2874**: five individuals undertook a complicated fraud where they hacked into servers operated by various companies to identify personal information about employees; **R v Jabeth and Babatunde [2014] EWCA Crim 476:** The appellants and others from around the world sent a series of emails purporting to be from a bank where a number of victims responded with their bank details. Phishing at its highest level. Conspiracy offences are useful in cyber fraud cases as the internet allows for criminals to operate all over the world to work with each other.

16. Other ''Property Issues'' to consider

Tangible and intangible property, virtual property, the acquiring of rights, commercial worth, intellectual property, piracy are also subject matters which are worthy of consideration in relation to cybercrime. Highly sophisticated digitalisation exists and can mask and copy any original, copy or reproduction of any material. The computer hardware, software, programs and games industry, the music industry and the entertainment industry and their copyright can also be the subject of cybercrime and at very considerable cost to themselves. The primary act relating to these topics is the **Copyright, Designs and Patent Act 1998**.

17. Vicious, malicious and nasty crimes

All crimes are vicious, malicious and nasty. That goes without saying. However the following crimes in a cybercrime context are particularly so because they are so personal and cause, along with sexual crimes, extreme personal distress.

1. Hate sites and hate speech in practice are generally covered by racial hatred offences, religious hatred offences, sexual orientation hatred and communication offences. Many offences are covered in **Part 3A Public Order Act 1986** which was inserted by the **Racial and Religious Hatred Act 2006**.
2. It is heartening to note that where in the **USA** which has traditionally adopted the approach that **hate speech** is generally protected under the **First Amendment**, in Europe **Article 17 of the ECHR** prevents an individual from using a Convention right in such a way as to deny the rights and freedoms of others. Therefore in Europe and at present in the UK (lets see what happens after **BREXIT**) it is not possible to rely on a human rights arguments where the purpose of hate speech is to increase prejudice against others.

3. **Self harm sites such as suicide websites, self-injury websites**, **eating disorder websites** will often be characterised by derogatory language and personification. Eating disorders EDs become so personified that many sites and people with it will talk about it as though it were a person. **Aneroxia** is shortened to Ana on the internet, **Bulimia** is shortened to Mia. Often on the internet people with an ED refer to Ana and Mia not only in the feminine but as a personality. Those who do not 'fit in' will often have derogatory language used against them. A **'wannarexic'** is somebody who is accused of being a **'wannabe aneroxic**'. They are normally treated with disdain. Insults and hostility can flow insidiously from these and all sites which have a capacity and tendency to bully which leads in some cases to over-reactions on the part of the recipient. Many of these sites are harmful or potentially harmful and they can be a particular potent source of cyber bullying. **Psychiatric, psychological, emotional as well as physical issues** come into play here and are highly complex as well as potentially dangerous. **Section 127 Communications Act 2003** criminalises the sending of obscene , indecent, grossly offensive or menacing communication. In **DPP v Collins [2006] 1WLR 3**08 Sedley LJ said ''what is offensive has to be judged …by considering the reaction of reasonable people…by the standards of an open and just multicultural society''. It seems the content of these sites will be judged according to the Act and the prevailing reasonable norms of the day, taking also into account the **Human Rights Act 1988**.

18. Sex, sex and more sex

1. **Some of us prosecute and defend all manner of sex cases**. They are demanding, challenging, exhausting and emotional cases.

2. **Cybercrime sex cases are no different and are often even more challenging due to the amount of material one has to deal with and the never ending disclosure problems that exist with the onslaught of social media websites, mobile phone evidence, texting**, **sexting, emails, sexemails, and the internet generally**.

3. Adult pornography, obscene publications, extreme pornography, revenge porn, child pornography, photo-based material, the possession and taking and making and distributing of child pornography, virtual child pornography, computer manipulated and generated images and all offences under the **Sexual offences Act 2003** ranging from rape and assault offences, offences where the victim is a child, indecent images of children, exploitation offences and other sexual offences under the Act may have an element of cybercrime attached to them in part and/or in full. The penalties are extensively covered by the **Sentencing Council Sexual Offences Definitive Guideline** and the guideline is used extensively in court. **Sentencing children and young people: Definitive guideline to be used from June 2017**: contains overarching principles which must be considered when sentencing children. These are highly complex provisions which only the most dedicated and competent of lawyers will be qualified to do whether prosecuting and defending. Children and young persons are at the same time most competent in using computers and yet most in danger from them. They may unwittingly become victims because of their computer use, or unwittingly without realising the consequences become perpetrators of sexual cybercrime.

19. Cyber-harrassment, cyber-bullying, cyberstalking

In many ways these cybercrimes are parallel forms of behaviour. Bullying and harassment include **flaming** (the posting of provocative or abusive posts), **malware** (the deliberate sending of a virus or other software in an attempt to cause damage to a computer or otherwise or signing someone up to spam so that their email is clogged up etc), **outing** (the posting or misuse of

personal information). They are often combined and committed across **all forms of communication. Twitter and Facebook are infamous for flaming.** The term 'troll' now has a very different meaning to the original Norwegian folklore legend. Trolls in cybercrime can be very threatening and very frightening and harmful to recipients.

20. **Cyberstalking** can be nothing short of insidious. Communication with the victim can be both passive and aggressive as well as passive-aggressive. A perpetrator can publish information about the victim, the victim's computer can be targeted, and the victim can be placed under surveillance including cyber-surveillance. There can also be impersonation of the victim, disclosure of further embarrassing personal information (true or not), and the posting of false information. Repeated and unwarranted messages which include or lead up to including abusive messages may originally have been innocuous or innocent but take a life on of their own in time becoming nasty, malicious and vindictive.

21. **Surveillance** can take two forms: **firstly** where technology is used to gain information about the victim and those connected to the internet; **secondly** the use of technology to monitor the victim's activities. Bugs, GPS information, webcams, tracking software can all be used in cybercrime.

22. **Offensive comments** are covered by **Section 127 Communications Act 2003** and **Section 1 Malicious Communications Act 1988**. Please note there is an **express mens rea** requirement in the 1988 Act, where on the face of it there is **no express mens rea** requirement on the face of the 2003 Act.

23. **Harrassment** is covered by the **Protection from Harassment Act 1997** amended by the **Protections of Freedoms Act 2012** which was introduced to cover the offence of **stalking**.

24. **Grooming or solicitation of children** can of course happen online both in this country and overseas. **Section 15** of the Sexual Offences Act 2003 covers this activity. Section 10 of the Sexual

Offences Act 2003 deals with causing or inciting a child to engage in sexual activity. **Section 12** of the Sexual Offences Act 2003 criminalises causing a child to watch a sexual act. **Section 14** of the Sexual Offences Act 2003 is designed to tackle grooming: it tackles the arranging or facilitating of **anything** that would involve the commission of an offence by someone anywhere in the world. There is no need for a physical meeting as in Section 15 and therefore can involve **online encounters.**

Adrian Amer

4.10.18.