UNIVERSITY
of DERBY

Derby Law School

Faculty of Law

Independent Studies

2020/2021

Bachelor of Laws LLB (HONS)

Name: Curtis Rouse.

Student Number: 100476261.

Supervisor: Taiwo Oriola.

Module Code: 6LA998.

Title: "An examination of the legislation and case law surrounding computer hacking with suggestions for reform."

Contents

Abstract:

This Dissertation will primarily focus on the effectiveness of legislation and will examine the case law surrounding computer hacking with suggestions for reform. I will also detail the methodology of computer hacking, because to analyse the law in the context of computer hacking, one must understand how it is done. Without such understanding it is not viable to analyse the law and suggest reforms due to the lack of knowledge on how an individual may hack a computer.

I will examine the key legislation which relates to computer hacking and the extent of how effective it is as a deterrent. The key legislation is the Computer Misuse Act 1990 (as amended). This Act is the primary legislation around Cybercrime. It was the first legislation concerning cybercrime and has served as a landmark piece of Law because it was the first time Parliament acknowledged and subsequently tried to control the immense power that computers hold by punishing people for using computers in undesirable ways. This legislation is related to the decision made in the landmark case of *R v Gold & Schifreen*[1]. I will also analyse the case law around computer hacking.

Finally, this paper will make suggestions for new laws (should they be needed), if existing laws should be revised and any new areas that need attention.

Introduction:

Before defining computer hacking, it is important to have an accurate definition of what constitutes a computer. A computer was defined by Lord Hoffman in *DPP v McKeown and Jones*[2] as "*a device for storing, processing and retrieving information*".[3] based on the definition, it includes smartphone, tablet and games console can all be defined in the same way as a traditional desktop computer/laptop.

[1] (1988) 1 AC 1063 (HL).

[2] [1997] 2 Cr App R 155 HL.

[3] IBID.

Computer hacking is the process in which an individual gains *"unauthorised access to computer material, unauthorised access with intent to commit a further offence and/or unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer"*.[4]

Computer Hacking has become very problematic in modern society because we are extremely computer dependent. This has resulted in the most powerful pieces of technology Humanity has so far made being widely available at anybody's fingertips. Due to this widely available, easily accessible power, some individuals/groups have taken it upon themselves to make Computers act in undesirable ways. There are many reasons why individuals partake in Computer Hacking, be that for money, power, reputation or simply boredom. But one consistency is that there is a level of harm/damage caused to the recipient of such hacking, this has led to Computer Hacking becoming a criminal offence, as per the Computer Misuse Act 1990.

It should also be noted that not all computer hackers are performing illegal actions. Governments, corporate entities, and other individuals commonly hire hackers to legally hack into their systems to identify exploits and other issues. This is known as ethical hacking or white hat hacking.[5] However, this paper will not focus on ethical hacking, and will instead focus on the illegal hacking, performed by black-hat hackers, also known as *"bad hackers"*.[6]

[4] Computer Misuse Act 1990.

[5] *"White hat hackers are deemed to be the good guys, working with organizations to strengthen the security of a system."* Sanchit Nanda 'World of White Hat Hackers' (2019) International Journal of Scientific & Engineering Research, Volume 10, Issue 5 285, 286.

[6] *"A bad hacker is a person who typically would breaks into computer systems for malicious reasons ranging from acts of vandalism, theft of sensitive information, to acts of terrorisms."* Taiwo Orialo, 'Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities' (2011) 28 J. Marshall J. Computer & Info. L. 451, 479.

Chapter 1: Methodology of Computer Hacking:

Whilst there is no step-by-step methodological process to Computer Hacking, there is a usual pattern hackers tend to follow to breach a system and make it behave in undesirable ways.

Firstly, and most importantly is the operating system. Computer Hackers commonly rely upon the Linux operating system because it is open-source, meaning the original code is released to the public and can be changed by anyone. This results in Linux being chosen over more well-known operating systems such as Windows because Windows is not open source. The nature of open-source means that individuals can make powerful computer programs from the source code which allows them to be harder to detect and trace by authorities in comparison to those using a windows-based operating system.

Once the hacker is on the desired operating system with the precautions in place to protect themselves from being exposed, they begin to perform the hack. Hacking is commonly comprised of several steps. Whilst no set rules exist on how to perform a hack; the following steps are the widely accepted steps to perform a computer hack.

The first step when performing a computer hack is to use a technique called *"reconnaissance."*[7] which is the process of collecting as much information as possible about a target system before performing an attack. Information such as (but not limited to) employee email addresses, IP

[7] Juneja Gurpreet K, 'Ethical Hacking: A technique to enhance information security' (2013), volume 2, International Journal of Innovative Research in Science, Engineering and Technology 7575, 7576.

address,[8] whois records,[9] DNS information,[10] are actively collected through social engineering and Google search. When a hacker is performing reconnaissance, they spend as little time interacting with the target system to avoid being detected.

After information has been gathered by the hacker on the target system via reconnaissance, the hacker uses this general information to begin finding more precise information on the target. This is known as *"scanning"*.[11] It is done through more complex techniques to gather more precise information. For example, a hacker will often perform a port scan to see which ports are live in a system. A hacker will also attempt to discover the operating system of the target and will also perform a ping sweep which allows the hacker to see a range of IP addresses that map to any live hosts. Scanning allows the hacker to acquire more in-depth

[8] *"An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network."* Kaspersky 'what is an IP address – definition and explanation' (definitions, November 17th, 2020) < https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address > accessed 20/04/2021.

[9] *"A Whois record contains all of the contact information associated with the person, group, or company that registers a particular domain name. Typically, each Whois record will contain information such as the name and contact information of the Registrant (who owns the domain), the name and contact information of the registrar Registrar (the organization or commercial entity that registered the domain name), the registration dates, the name servers, the most recent update, and the expiration date. Whois records may also provide the administrative and technical contact information (which is often, but not always, the registrant)."* Domaintools 'What is Whois Information and Why is it Valuable?' (Support, September 19th, 2017) < https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable > Accessed 20/04/2021.

[10] *"The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources."* Cloudfare 'what is DNS?' (DNS learning objectives, March 30th, 2019) < https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/ > Accessed 20/04/2021.

[11] Juneja Gurpreet K, 'Ethical Hacking: A technique to enhance information security' (2013), volume 2, International Journal of Innovative Research in Science, Engineering and Technology 7575, 7576.

information about the system which means they are more likely to discover exploitable vulnerabilities within the system.

Upon acquiring the above-mentioned information via the previously mentioned techniques, a hacker will next perform the action of *"enumeration"*.[12] This is done by closely examining the information gathered and allows the hacker to determine the usefulness of the information. The types of information enumerated by hackers are the network resources, DNS information, the user's ID, machine names, auditing, and service settings, routing tables (data stored in the router/host network) and Simple Network Management Protocol (to gather information about any devices connected to the network). Enumeration provides the hacker with the most critical information and upon a successful enumeration of information, they can proceed to system hacking.

"Gaining access"[13] is the next step. The hacker will use the gathered information from the previous steps to gain unauthorised access to the computer to make it behave in an undesirable way, be that impairing the system's ability to function which can result in a shutdown, resulting in stealing valuable information stored on the system such as (but not limited to) credit card details, national insurance numbers and other sensitive, personal information. A hacker will usually target valuable information like this when performing a system hack because they can get some form of monetary gain by selling the illegally obtained

[12] *"Enumeration is defined as the process of extracting usernames, machine names, network resources, shares and services from a system. In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target."* GreyCampus 'Enumeration and its Types' (Ethical Hacking, September 27th 2020) < https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types#:~:text=Enumeration%20is%20defined%20as%20the,and%20services%20from%20a%20system.&text=The%20gathered%20information%20is%20used,in%20the%20System%20gaining%20phase> Accessed 22/01/2021.

[13] Juneja Gurpreet K, 'Ethical Hacking: A technique to enhance information security' (2013), volume 2, International Journal of Innovative Research in Science, Engineering and Technology 7575, 7576.

information on the dark web on illicit marketplaces (darknet market.[14]). In past times, such illicit marketplaces would have included, but are not limited to the silk road, and the dream market. Similar marketplaces still exist, but now they are more private and less known due to law enforcement taking down the above-mentioned sites.

After a successful system hack, the hacker will proceed to escalate their privileges. There are two ways in which this can be done. The first is known as horizontal privilege escalation.[15] This allows the intruder to use the same permissions gained from the initial hack. For example, a hacker may access protected resources using a normal user account.

When a hacker gains access to a system, they will not have administrator privileges. The next step is to gain these privileges. This is done via the second method of privilege escalation; it is known as vertical privilege escalation.[16] This allows the hacker to move away from a low privileged account to a high privileged account such as an administrator, meaning they have more control over the system which consequently allows them to access protected information and other critical information to which low privileged accounts do not have access to.

[14] *"Darknet markets are dark web black markets that offer illicit goods for sale, often using cryptocurrencies as a method of payment. Although some products for sale are legal, illicit goods such as drugs, stolen information, and weapons are common items in these markets."* Jake Frankenfield, 'Cryptocurrency' (Investopedia, Darknet Market, 1st February 2021) < https://www.investopedia.com/terms/d/darknet-market-cryptomarket.asp > Accessed 03/02/2021.

[15] *"When a malicious user attempts to access resources and functions that belong to peer users, who have similar access permissions."* GreyCampus 'Privilage Escalation' (Ethical Hacking, 18th September 2020) < https://www.greycampus.com/opencampus/ethical-hacking/privilege-escalation > Accessed 22/01/2021.

[16] IBID.

When the hacker has completed their desired tasks, they will perform the next step of *"covering their tracks"*.[17] This process involves the hacker removing any evidence of their presence within the system. To do this, hackers will clear the user logs, the event logs, and the command history. A hacker will cover their tracks to hide the system breach because the ideal outcome is that the owner of the system is not aware of the hacker's presence, or that a breach even has occurred. However, should the owner become aware of a breach, there is no evidence of who hacked the systems because the hacker has removed the logs and command history, therefore covering their tracks.

If the hacker has not yet been detected, and if they have adequate time, upon successfully covering their tracks, they will place 'backdoors' into the system. A backdoor[18] means the hacker can re-enter the system anytime they please and do so undetected. This will allow the hacker to steal personal and financial information or even install malicious software into the system.

This chapter provides important context because, before examining the legislation and case law around computer hacking with reform suggestions, it is important to first understand what hacking is, and how it is done.

[17] Juneja Gurpreet K, 'Ethical Hacking: A technique to enhance information security' (2013), volume 2, International Journal of Innovative Research in Science, Engineering and Technology 7575, 7576.

[18] *"A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application."* Malwarebytes 'backdoor computing attacks' (Backdoor Computing Attacks 28th April 2019) < https://www.malwarebytes.com/backdoor/ > Accessed 22/01/2021.

Chapter 2: The current legislation surrounding computer hacking and the extent to which it is effective as a deterrent.

The primary UK legislation surrounding offences and/or attacks against computers is the Computer Misuse Act 1990. This legislation was created in response to the case of *R v Gold & Schifreen*[19] and the subsequent suggestions put forward by the Law Commission to create three offences of computer misuse; those being *"Unauthorised access to a computer, unauthorised access to a computer with intent to commit or facilitate the commission of a serious crime and unauthorised modification of computer material"*.[20]. This chapter will therefore focus on analysing this legislation by examining how effective it is as a deterrent.

As previously stated, the case of *DPP v McKeown and Jones*[21] defined what a computer is. The reason a computer was not defined within the Computer Misuse Act is to allow for technological development. The level of technological competence displayed by Parliament is something to emphasise because it demonstrates that Parliament understood how computers needed to be regulated, but it also demonstrated their ability to accurately predict the direction society was moving in; a rapidly adapting one which is heavily dependent on computers and where technology advances at such a pace that new systems and types of computers (i.e., smartphones and tablets) are available for access by the general public. If Parliament did not choose this action, it would mean the statue would have to be amended every few years to keep up with the rapid advancement of technology, but this is not a plausible solution because it is time consuming, expensive and the law is slow to adapt. Therefore, meaning Parliament's insight into the power of computing is something to be commended. This consequently means the Computer Misuse Act is an effective deterrent (generally speaking) because it has a wide array of applications and can be applied to recent technology due to the lack of a clear definition of a computer within the act.

[19] (1988) 1 AC 1063 (HL).
[20] The Law Commission, Computer Misuse (Law Com No 186, 1989) para 5.2.
[21] [1997] 2 Cr App R 155 HL.

Section 1, subsection 1 of the Computer Misuse Act states an individual is guilty of an offence if s/he *"causes a computer to perform any function with intent to secure access to any program or data held in any computer (or to enable any such access to be secured), the access he intends to secure (or to enable to be secured,) is unauthorised; and he knows at the time when he causes the computer to perform the function that is the case."*[22] This section acts as an effective deterrent because irrespective of if access is obtained or not, an individual will still be liable. This, therefore, discourages an individual from attempting to obtain unauthorised access to a computer because they will still be punished, even if they fail to gain access which consequently means the effectiveness as a deterrent is high. However, despite the high deterrence provided by subsection 1, individuals/entities still choose to act in a way that breaches subsection 1 and are not at all deterred because they fully understand they are committing a crime yet still go ahead with it anyway, but nothing in the law will ever have a 100% deterrence.

Subsection 2 states *"The intent a person has to have to commit an offence under this section need not be directed..."*[23] However, there is no mention of recklessness within section 2 meaning people who are experimenting with scripts, web browsers and other software's may accidentally find backdoor access, they lacked the intent mentioned in subsection 2, but their actions are nevertheless reckless. However, the lack of recklessness within subsection 2 means its effectiveness as a deterrent is to a lesser extent because it does not discourage people from experimenting with software and/or scripts/web browsers meaning people who lack the intent, but perform a hack are let off on the basis that they lack pure intention. However, if the act specified recklessness as well as intent the extent to which it acts as a deterrent would be enhanced.

Furthermore, the recklessness argument holds validity because although section 2 states *"need not be directed"* implying the element of recklessness exists, it is not explicit in stating that recklessness must be present and that is problematic because based on the wording of subsection 2, all a person need do is intend to hack, but not have a specific target to satisfy the

[22] Section 1 (1) Computer Misuse Act 1990.
[23] Section 1 (2) Computer Misuse Act 1990.

"not directed" criteria presented. This lack of recklessness is arguably a shortcoming of section 2.

Subsection 3 states a guilty person on a summary conviction shall be subjected to imprisonment of *"12 months, or a fine not exceeding the statutory maximum or both".*[24] and an indictable conviction shall be subjected to imprisonment of *"2 years, or a fine or both"*.[25] The extent to which subsection 3 acts as a deterrent is high because it covers both summary and indictable offences which can be committed with a computer meaning all grounds are covered in terms of the seriousness of the offences committed. Furthermore, it is likely to deter individuals from computer hacking if they know they may face prison/a fine or both for their actions meaning the extent to which subsection 3 acts as an effective deterrent is high.

Section 2 deals with those who intend to commit or facilitate the commission of further offences, thereby developing section 1 for repeat offenders and/or people who are committing other offences at the same time. The principles of section 1 apply here in terms of intent and the offence committed. However, the sentencing under section 2 offences is slightly different to section 1; the summary offence sentencing remains the same, however, the sentencing for an indictable offence differentiates in that section 2 will allow those convicted under it to be imprisoned for a term of *"no longer than 5 years, a fine, or both"*.[26] This harsher sentencing structure for indictable offences under section 2 means the extent to which it acts as an effective deterrent is high because 5 years is a substantial amount of an induvial lifetime and because it carries a heavier sentence, it also discourages individuals from facilitating later offences/committing other offences alongside.

Section 3 deals with the impairment of a computer from performing its desired functions, be that intentionally or recklessly. The impairment of a computer can have dangerous and potentially deadly consequences. To be charged under section 3 an individual must either recklessly or intentionally *"impair the operation of any computer; prevent or hinder access to any program or*

[24] Section 1 (3) Computer Misuse Act 1990.
[25] IBID.
[26] Section 2 Computer Misuse Act 1990.

data held in any computer; to impair the operation of any such program or the reliability of any such data; to enable any of the things mentioned in paragraphs (a) to (c) above to be done."[27] Although a reckless element is mentioned in this section, it is not properly applicable to section 1 because that involves computer material and you do not have to impair a computer to access the materials it holds.

Should an individual be found guilty under Section 3, if they are guilty of a summary offence, they will face the same punishment listed in both sections 1&2. However, if an individual is guilty of an indictable offence under this section, they shall face a term of imprisonment *"not exceeding 10 years, a fine or both"*.[28]. The extent to which this is an effective deterrent is high because a term of 10 years is a huge portion of an individual's life, and this sentence is justified because the impairment of a computer could result in the death of someone, or a huge pecuniary loss. Therefore, meaning the harsh sentence is likely to deter people from committing such an offence meaning the extent of effectiveness is high.

Section 3ZA deals with those whose goals are to impact the national security of the nation by dealing with *"unauthorised acts causing or creating a risk of serious damage"*.[29]. This section differs from the others because the sentence this offence carries is life imprisonment, and this sentencing is fitting for the crime because anyone who is in breach of section 3ZA is potentially a risk to national security, the economy or human life, therefore requiring the maximum possible sentence to deter people from committing such offences. Given these crimes are not often reported, it is logical to assume that this deterrent is highly effective consequently meaning the extent to which this section is effective is high.

[27] Section 3 Computer Misuse Act 1990.

[28] IBID.

[29] Section 3ZA Computer Misuse Act 1990.

Finally, section 3A deals with people who are involved in the *"making, supplying or obtaining of articles for use"*.[30] I.e., malicious software (also known as malware[31]) Such as computer viruses,[32] Worms,[33] Trojan horses,[34] and lesser-known malware such as spyware,[35]Ransomware,[36] and adware.[37] The sentencing structure for this is identical to that of section 1 which does bring into

[30] Section 3A Computer Misuse Act 1990.

[31] *"Malware is an abbreviated term meaning malicious software. This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner. There are various types of malware including spyware, keyloggers, true viruses, worms, or any type of malicious code that infiltrates a computer."* (Symantec, Norton 360 knowledge base version 22.20.5.39, 26 October 2020).

[32] *"A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document."* (Symantec, Norton 360 knowledge base version 22.20.5.39, 26 October 2020).

[33] *"A computer worm is a type of malicious software that travels through network connections all over the world to find its targets."* (Symantec, Norton 360 knowledge base version 22.20.5.39, 26 October 2020).

[34] *"A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network."* (Symantec, Norton 360 knowledge base version 22.20.5.39, 26 October 2020).

[35] *"Spyware is a blanket term given to software that gathers information about your computer and the things you do on it and sends that information over the Internet to a third party. Sometimes spyware asks for your consent first. More commonly, it installs itself on your computer without you knowing and runs in the background, secretly collecting data, sending you targeted adverts or meddling with your computer set-up."* Symantec, Norton 'What is Spyware?' (Norton Blog, 7th September 2015) < https://uk.norton.com/norton-blog/2015/08/what_is_spyware_.html > Accessed 20/04/2021.

[36] *"Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. This class of malware is a criminal moneymaking scheme that can be installed through deceptive links in an email message, instant message or website. It has the ability to lock a computer screen or encrypt important, predetermined files with a password."* Kaspersky 'What is Ransomware?' (Definitions, 3rd April 2019) < https://www.kaspersky.com/resource-center/definitions/what-is-ransomware > Accessed 20/04/2021.

[37] *"Adware, or advertising supported software, is software that displays unwanted advertisements on your computer. Adware programs will tend to serve you pop-up ads, can change your browser's homepage, add spyware and just bombard your device with advertisements. Adware is a more succinct name for potentially unwanted programs. It's not quite a virus and it may not be as obviously malicious as a lot of other problematic code floating around on the Interne... it could also cause long-term issues for your device."* Symantec, Norton

question its effectiveness as a deterrent because the sentences that can be passed down are light in comparison to the societal impact an offender may have with such software. This means an individual could provide someone with the ability to infect a large amount of the population with malware and steal valuable, sensitive information and the max sentence they can receive for distributing such harmful software is 2 years and a fine. The cost/benefit analysis for a computer hacker would dictate that the risk is worth taking because the sentence is so low. This, therefore, means the extent for Section 3A acting as a deterrent is low.

The extent to which the Computer Misuse Act is an effective deterrent is high because it makes it clear what actions will breach the Act whilst also subsequently providing a clear outline of what will happen to the individual based on the seriousness of the offence they commit. It also deals with individuals who make and distribute malware and those who seek to attack the national infrastructure meaning all the outcomes and the performing of a computer hack is covered. Furthermore, the lack of a definition for a computer allows the law to develop quickly alongside technology therefore making its effectiveness high. However, section 3A's sentencing is light considering the impact of things such as malware can have, meaning the extent to which section 3A is effective as a deterrent is low.

There are more sections within the Computer Misuse Act (CMA), however, the ones covered above are the most important and whilst the CMA is the main legislation surrounding computer hacking and all offences under the Act can be prosecuted if there is a link to the domestic authority. It should be noted that it does have links to other legislation such as the Data Protection Act 2018 because computers are involved in the storing, transmission and receiving of data. Another legislation with close links to the above-mentioned Act is the Investigatory Powers Act 2016.

'What is adware?' (Emerging threats, 20th April 2019) < https://us.norton.com/internetsecurity-emerging-threats-what-is-grayware-adware-and-madware.html > Accessed 20/04/2021.

Chapter 3: An analysis of the case law on computer hacking.

The landmark case in computer hacking is *R v Gold & Schifreen (1988).*[38] Before this case, there was no legislation for which a computer hacker could be charged under. A direct consequence of this case is the Computer Misuse Act 1990. It was passed to counter and charge hackers. This is supported by Lord Brandon, who stated *"the appellants' conduct amounted... to dishonestly gaining access to the relevant Prestel data bank... That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts."*[39] The outcome of this case is positive because it demonstrated a huge gap in the Law that needed to be fixed by Parliament and that it was beyond the Court's power to charge it as an offence based on legislation that existed before 1990.

The Computer Misuse Act (CMA) has caused uncertainty for what constitutes *"unauthorised access"* because section 17(5) of the CMA was vague. Therefore, case law is required to develop this area of Law. One of the early cases which dealt with this issue is *DPP v Bignell*, which held *"...an unauthorised purpose, does not constitute the offence of unlawful access."*[40]. This ruling was handed down because the officers in question gained the information in question for their own purposes, not police purposes, which is not authorised. Their acts were deemed to be legal. However, this leaves a glaring hole in the law because it meant employees could freely take computer data that they had no purpose in taking, but because they had authorised access to the computer, it was not an illegal act. This is problematic because it does not deter disgruntled employees from stealing data from their employer. However, the House of Lords dealt with this issue in the *R v Bow Magistrates* case by ruling *"Their Lordship made it clear that an employee would only be guilty of an offence if the employer clearly defined the limits of the employee's authority to access a program or data."*[41]This ruling came after an employee made a computer access data; she knew she was not allowed to access. In retrospect, this should be an open and

[38] 1 AC 1063 (HL).

[39] IBID.

[40] (QBD) 1998 1 Cr App.

[41] R v Bow Street Magistrates' Court and Allison (AP) Ex parte Government of the United States of America [Allison] [2002] 2 AC 216.

closed case. However, because the employee had no defined limits, it means her act was not illegal, which seems unjust, because applying common sense to the facts, it is clear she is guilty of a section 1 because she intended to access data without proper authorisation. The ruling handed down now means the hole in the Law created by Bignell is now corrected because no longer can an employee take data, call it an unauthorised purpose and be free of consequence meaning better security for employers because the Law now protects them from rogue employees stealing their data consequence-free.

The case of *DPP v Lennon*[42] exposed another gap in the law with its initial ruling because the defendants performed a denial of service (DOS) attack against a mail server of his former employer. The initial ruling held this was not in breach of the CMA. This ruling is surprising, because as Stefan Fafinski pointed in his commentary; *"The deliberate and informed act of bringing down computer systems under a barrage of e-mail, or indeed any other manifestation of a denial-of-service attack, instinctively feels like the sort of behaviour that should fall within the criminal law particularly when it results in loss..."*.[43] However, this decision was reversed upon appeal with LJ Keene ruling *"in my judgement he does not consent to receive emails in a quantity and at a speed which is likely to overwhelm the server. Such consent is not to be implied from the fact the server has an open as opposed to a restricted configuration"*.[44]. This ruling closed the gap in the law concerning DOS attacks and therefore closed an area which the Legislature failed to cover within the CMA. However, judicial intervention to determine the mischief of the legislature with the CMA is not ideal, because the legislature should not allow for such glaring issues in the Law to develop.

[42] [2006] EWHC 1201 (Admin).

[43] Stefan Fafinski, 'Computer misuse: Denial of service attacks' (2006) 70, Journal of Criminal Law 474, 476.

[44] IBID.

The decision handed down by Lord Woolf in the *Zezev and Yarimaka*[45] case was relied upon in the Lennon case. Lord Woolf held *"If a person caused a computer to record that information came from A when it came from B, that manifestly affected the reliability of that information for the purposes of s.3 Computer Misuse Act 1990."*[46] the *Lennon* ruling followed this judgement because the same principles apply to the Lennon case; by performing the DOS attack, the defendant *"affected the reliability of that information"*.[47] because the information within the servers (genuine emails) could not perform reliably in the sense that it could not be sent/received by the intended parties. Therefore, impacting the reliability of the information.

The CMA has a major floor, because *"there are no specific sentencing guidelines relating to offences under the CMA".*[48] This is problematic because it makes the Court's job of passing sentences more difficult. However, *R v Oliver Baker*[49] was the first in a series of cases that provided some form of structure to sentencing after a former employee hacked into the Welsh Assembly's account, read sensitive emails, and made fake pay and display tickets. These offences were in breach of S1 CMA resulting in a four-month sentence. Furthermore, *R v Crosskey (Gareth)*[50] added more structure by omitting the idea of a suspended sentence for a computer hacker who illegally accessed a minor celebrity's social media, emails and attempted to sell the obtained information. This case built on *R v Oliver Baker.*[51] because it denied a suspended sentence, and whilst such a sentence is a plausible option, it is less likely to be utilised by the Courts after this ruling because far graver crimes can be committed via computer hacking and the offence committed in Crosskey is relatively minor in comparison to the graver crimes.

[45] Zezev and Yarimaka v Governor of HM Prison Brixton and another (QBD) 2002 EWHC 589.
[46] IBID.
[47] DPP v Lennon [2006] EWHC 1201 (Admin).
[48] Jacqueline Zoest 'Current sentencing trends for data protection and data 'theft' offences' (2015) Lexis Nexus 1, 2.
[49] (2011) EWCA 928.
[50] [2012] EWCA Crim 1645.
[51] (2011) EWCA 928.

This duo of cases provided a baseline of guidance to what sentences should be handed down concerning specific offences. Something which the CMA fails to do, but as already pointed out, the CMA does have sentencing guidelines in terms of the minimum and maximum time for a breach of each section. However, the specifics are something which case law has been forced to develop and this was intentionally done because the Act itself has been left vague, so it has a wide scope of application to Computer-related offences meaning Parliament do not have to continually update the Act, removing potential offences that could fall outside the scope of the Act if it were too specific.

However, there has been no guidance on how the Courts should handle a case where the defendant has intent but is not malicious. This changed with *R v Glen Mangham (Glen Steven)*[52]after the defendant stole intellectual property from a Facebook employees' email and stored it on a hard drive. There was no ill intent, only to demonstrate vulnerabilities. Justice Cranton therefore held *"the serious crime prevention order cannot stand... and substitute 4 months for 8 months on each account."*[53] This case demonstrated that a lack of intent will not excuse the commission of a crime and will be punished accordingly. However, cooperation with the authorities can act as a mitigating factor for the sentence. Thus, clarifying what will happen to offenders who lack intent. This ruling applies to individuals who act in the capacity of a *"white hat hacker."* [54] (See introduction), but unlike white hat hackers, such individuals are not given consent to hack and are not employed by the company in question (Facebook in this case), to do so and will face legal consequences.

Despite the ruling from *R v Glen Mangham (Glen Steven)*[55] , in the case of *R v Martin (Lewys Stephen)*[56] the defendant launched a DOS attack on Oxford University, this was blocked, but the attack migrated to other sites. However, the intent was to show off and not gain anything financially. The Court consequently held that the Glen Mangham case *"should not be considered*

[52] (2012) EWCA Crim 973.
[53] IBID.
[54] Sanchit Nanda 'World of White Hat Hackers' (2019) International Journal of Scientific & Engineering Research, Volume 10, Issue 5 285, 286.
[55] (2012) EWCA Crim 973.
[56] (2013) EWCA Crim 1420.

as a benchmark for the sentence in such cases, which were likely to attract sentences measured in years rather than months."[57] and dismissed the defendants appeal that the sentence was too long. This case did, however, confirm an idea from *Glen Mangham* which was the type of intent did not matter or have a bearing in the sentence received, basic intent is only needed. This is confirmed because in both cases there was no malicious intent; in the Glen Mangham case, the intent was to expose vulnerabilities with no maliciousness intended. This was demonstrated by the fact the defendant *"...had not attempted to pass on or sell any information."*[58], and in the previously mentioned Martin case, the intent was *"motivated by youthful bravado rather than financial gain."*[59]. Therefore, confirming the type of intent does not have any relevance to the sentence handed down.

Chapter 4: Suggestion for reform.

The Computer Misuse Act 1990 is the Primary legislation concerning computer hacking. Consequently, it will be the focus of this section on reform.

The way traditional crimes such as theft, murder etc. won't change in how they can be committed because the general principles have stood the test of time. However, computer hacking is a modern crime that exists because of technological advancements within society. It, therefore, means how computer hacking crimes are committed can change over time as technology advances and changes.

One way in which the Computer Misuse Act 1990 can be reformed would be changing section 1, specifically in agreement to the CLRNN's (Criminal Law Reform Now Network) suggestion for *"the current offence definition, if retained, should be reduced to a summary only offence; or if current sentencing is maintained, the offence should be narrowed by specifying required harms*

[57] IBID.
[58] R v Glen Mangham (Glen Steven) (2012) EWCA Crim 973.
[59] R v Martin (Lewys Stephen) (2013) EWCA Crim 1420.

beyond simple unauthorised access."[60]. The reason for this suggestion is because the current layout of section 1 is overly complicated, and the sentence it carries is too wide because the damage caused by a breach of section 1 is theoretically limitless in scope, so who is to say what constitutes a summary offence and an indictable offence in the context of section 1. Therefore, the most appropriate action is to make section 1 a summary offence and have an indictable offence under a separate section/subsection with clear definitions of such offences in the context of computer misuse.

Another suggestion for reform would be to alter section 3za of the Computer Misuse Act to require an intention to *"cause serious damage of a material kind."*[61]. Currently, recklessness is sufficient to cause a breach of this section. However, recklessness provides the possibility for accidents to occur and in such cases, people shouldn't be charged with an offence. Individuals should only be charged if they have the intent to cause a criminal offence. An example of a reckless action not being charged is that of Sanmey Ved.[62] where he brought the google domain after seeing it on sale for 12 dollars and it consequently allowed him to access internal emails from google and the webmaster controls. However, Sanmey never used such controls to cause damage and instead reported the issue to Google. Sanmey was not charged for recklessness despite the risk to national security and the economy because Google has access to a nearly incomprehensible amount of personal data, which, if leaked could damage national security as well as the economy. In the UK, Sanmey could be charged despite not doing anything wrong, which is unfair prosecution. Therefore, reform is needed because if intention is required, it gives the option for people think twice before proceeding with any action to breach section 3za whereas currently, recklessness doesn't allow such afterthoughts to occur meaning if someone is reckless, like Sanmey, they are in breach of the law anyway so they may as well continue with

[60] CLRNN 'reforming the Computer Misuse Act 1990' (2020) Criminal Law Reform Network 1, 137.

[61] Section 3za (1) (d) Computer Misuse Act 1990.

[62] Devan Joseph and Biz Carson 'This guy bought 'Google.com' from Google for one minute' (business insider, Tech, 1st October 2015) < https://www.businessinsider.com/this-guy-bought-googlecom-from-google-for-one-minute-2015-9?r=US&IR=T > Accessed 28/02/2021.

their actions. Therefore, if section 3za is amended to only require intent, people aren't going to be unfairly prosecuted.

In addition, section 3A needs to be reformed (in agreement with the CLRNN's suggestion), section 3A *"should be narrowed, to apply only where a defendant intends to pursue a criminal endeavour."*[63] because as it currently stands, section 3A is too wide in its application. For example, if person A were to supply such articles (as mentioned in section 3A) through a legitimate business, with no intention of helping person B commit a criminal offence, person A would still be liable for person B's transgressions. Despite person A providing such articles for legitimate use, as Peter Sommer points out, *"there is no explicit defence of legitimate use."*[64] meaning person A would be liable under section 3A.

Another example would be the *"white hat hacker."*[65]. The role of whom is to test the security of companies (penetration testing). However, nothing can stop an individual posing as a white hat and obtaining such an article from an unknowing software developer who is not aware of the criminal intent such an individual possesses and under section 3A, the software developer would be held liable. This is demonstrative of why section 3A should be reformed to only require intent.

Finally, another suggestion is the introduction of a new section that holds corporate entities responsible for inadequate security on their computer systems and/or servers. It should amount to grossly negligent behaviour/conduct because it makes computer hacking much easier to perform and puts many people's private, personal information at risk (see the example of Equifax hack[66]). To only blame the hacker in such situations feels like an oversight from the law, because but for the security systems being up-to-date and secure, the hackers

[63] CLRNN 'reforming the Computer Misuse Act 1990' (2020) Criminal Law Reform Network 1, 137.

[64] Peter Sommer, 'criminalising hacking tools' (2006) 3 digital investigations 1, 6.

[65] Sanchit Nanda 'World of White Hat Hackers' (2019) International Journal of Scientific & Engineering Research, Volume 10, Issue 5 285, 286.

[66] Mckay Smith & Garrett Mulrain 'Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform' Journal of National Security Law & Policy (2018) Volume 9 549.

would not have gained access as easily, if at all. Therefore, having the potential to save millions of people's private information and data. Equifax did the equivalent of leaving their door unlocked and open, ready for a thief to take their valuables. To say a corporate entity shouldn’t also be held liable is to absolve them of liability when protecting customers data because they can use the hacker as a scapegoat. Whilst, yes, the hacker breached the law and should be held accountable, it is also paramount for the Law to hold the companies accountable for their weak security systems. Holding companies accountable would cause a reason for systems to be upgraded owing to the fact they would now be deterred from not upgrading system security, consequently meaning the people win, and the Law can hold those accountable who do not value security over personal information.

However, despite the previously discussed shortcomings of the Computer Misuse Act, it is important to note that it is still a legally sound piece of legislation because it keeps up with the development of new technologies. This comes because of having no definition of a computer, and the act itself being vague in terms of its application to technology. This means before a new technology becomes mainstream (such as Neuralink[67]), it's already illegal to hack and manipulate it, meaning another consequence of this Act being intentionally vague is that it could inadvertently save the lives of those who choose to have technology augmented into their bodies, such as Neuralink. Therefore, making the Computer Misuse Act a mostly legally sound legislation, despite the many shortcomings it may present.

However, just as Stefan Fafinski pointed out in 2006, *“it is clear that this is an area which will undoubtably undergo a transformation potentially as significant as the transformation in technology over the past 16 years”*.[68] This statement still stands 15 years later, because technology is always changing and advancing at a rapid pace, meaning this area will have to

[67] Elon Musk & Neuralink ’an integrated brain-machine platform with thousands of channels’ (2019) BioRxiv the preprint server for Biology.

[68] Stefan Fafinski ‘Access denied: Computer misuse in the era of technological change’ (2006) 70, Journal of Criminal Law 424, 442.

undergo transformation because if changes in technology are inevitable, then changes to the Law must also be inevitable.

Chapter 5: Conclusion

The primary focus of this dissertation was to examine the current case law and legislation surrounding computer hacking with suggestions for reform whilst also explaining the methodology for computer hacking.

The methodology behind computer hacking was included because, to discuss the topic area in the context of current legislation, case law and reform suggestions, one must first have somewhat of an understanding of how an individual can perform a computer hack.

This dissertation's purpose was to analyse the relevant case law and legislation in the context of computer hacking to determine if any reform is needed, as chapter 4 pointed out, some degree of reform is needed concerning the Computer Misuse Act, specifically sections 1,3za, 3a and the inclusion of a new section to the Act. The reason such suggestions exist is that the Computer Misuse Act is starting to become outdated due to the rapid advancement in technology and the subsequent change in societal norms which follow. However, because the Act does not include a specific definition of what constitutes as a Computer (this has however been developed through case law, see chapter 3), the consequence is the act is easier to update because legislators will not have to confine any amendments/new sections to an old definition.

As already stated, the main points for reform are sections 1,3za and 3a as well as a new section. The changes to the already existing sections are recommended on the basis that they are largely outdated because the act itself was passed in response to the *R v Gold & Schifreen*[69]. For example, section 1 is too complex and too far-reaching, providing a theoretically limitless scope resulting in hardship when deciding if an offence is indictable or not. Section 3za only requires someone to be reckless, but as demonstrated by Sanmay Ved, the reckless requirement is unfair, and this section should only require intent. Finally, section 3a should be narrowed to

[69] (1988) 1 AC 1063 (HL).

only include intent to partake in criminal conduct because innocent people who provide software for legal penetration testing can be misled into providing a hacker with software and have no idea that said software is being used illegally, but the provider is still held accountable, which is unfair because they have zero intent to partake in criminal conduct.

The reason behind the recommendation of a new section to the Computer Misuse Act is to allow corporations to be held liable for not providing customers with an adequate level of security with regards to their personal and private data. Currently, there is nothing under the Computer Misuse Act which would hold corporations liable for data breaches like that of the Equifax hack.[70] This should be reformed so corporations are encouraged to provide up-to-date protection for their customers data. A counter argument would be to use the Data Protection Act 2018. However, this Act is concerned with the processing of data and protecting in the context of processing and not the security of the data itself. To obtain such data, a hacker would have to misuse a computer to bypass any security around the data, which is why this new section should be placed within the Computer Misuse Act.

This area of study has made an impact by pointing out the shortcomings of the Computer Misuse Act and providing suggestions to make the Act more robust, in order adequately protect the population.

[70] Mckay Smith & Garrett Mulrain 'Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform' Journal of National Security Law & Policy (2018) Volume 9 549.

Bibliography

Table of Cases:

DPP v. Bignell, (QBD) 1998 1 Cr App.

R v Crosskey (Gareth) [2012] EWCA Crim 1645.

R v Bow Street Magistrates' Court and Allison (AP) Ex parte Government of the United States of America [Allison] [2002] 2 AC 216.

R v Glen Mangham (Glen Steven) (2012) EWCA Crim 973.

R v Gold & Schifreen (1988) 1 AC 1063 (HL).

DPP v Lennon [2006] EWHC 1201 (Admin).

R v Martin (Lewys Stephen) (2013) EWCA Crim 1420.

DPP v McKeown and Jones [1997] 2 Cr App R 155 HL.

R v Oliver Baker (2011) EWCA 928.

Yarimaka v Governor of HM Prison Brixton and another (QBD) 2002 EWHC 589.

Table of Legislation:

Computer Misuse Act 1990.

Criminal Damage Act 1971.

Data Protection Act 2018.

Forgery and Counterfeiting Act 1981.

Investigatory Powers Act 2016

Serious Crime Act 2015.

Bibliography:

Books

Clough, J. ‘principles of cybercrime’ (2nd edition, Cambridge University Press, 2010).

Gillespie A, ‘Cybercrime key issues and debates’ (2nd edition, Routledge, 2019).

Barker D and Robinson P, ‘artificial intelligence and the law. Cybercrime and criminal liability’ (1st edition, Routledge, 2020).

Wall, D. ‘cybercrime’ (1st edition, Cambridge: Polity Press, 2007).

Journals:

CLRNN. ‘Reforming the Computer Misuse Act 1990’ (2020) Criminal Law Reform Network.

Elon Musk & Neuralink ’an integrated brain-machine platform with thousands of channels’ (2019) BioRxiv the preprint server for Biology.

Fafinski, S. ‘Access denied: Computer misuse in the era of technological change’ (2006) 70, Journal of Criminal Law.

Fafinski, S. ‘Computer misuse: Denial of service attacks’ (2006) 70, Journal of Criminal Law.

Gurpreet K, J. ‘Ethical Hacking: A technique to enhance information security’ (2013), volume 2, International Journal of Innovative Research in Science, Engineering and Technology.

Orialo, T. ‘Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities’ (2011) 28 J. Marshall J. Computer & Info. L. 451.

Smith, M & Mulrain G, ‘Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform’ Journal of National Security Law & Policy (2018) Volume 9.

Nanda, S. ’World of White Hat Hackers’ (2019), Volume 10, Issue 5 International Journal of Scientific & Engineering Research.

Sommer, P. ‘criminalising hacking tools’ (2006) 3 digital investigations

The Law Commission. Computer Misuse (Law Com No 186, 1989).

Zoest, J. ‘Current sentencing trends for data protection and data 'theft' offences’ (2015) Lexis Nexus.

Online Articles/Websites:

LexisNexis < https://www.lexisnexis.co.uk/ > Accessed 22/01/2021.

WestLaw < https://legalsolutions.thomsonreuters.co.uk/en/products-services/westlaw-uk.html > Accessed 22/01/2021.

Geek University ‘Hacking methodology ‘(Basic concepts, 9th June 2016) < https://geek-university.com/ccna-security/hacking-methodology/#:~:text=Although%20there%20is%20no%20specific,prior%20to%20performing%20the%20attack. > Accessed 22/01/2021.

GreyCampus ‘Enumeration and its Types’ (Ethical Hacking, 27th September 2020) < https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types#:~:text=Enumeration%20is%20defined%20as%20the,and%20services%20from%20a%20system.&text=The%20gathered%20information%20is%20used,in%20the%20System%20gaining%20phase. > Accessed 22/01/2021.

GreyCampus ‘Privilege Escalation’ (Ethical Hacking, 18th September 2020) < https://www.greycampus.com/opencampus/ethical-hacking/privilege-escalation > Accessed 22/01/2021.

Malwarebytes ‘backdoor computing attacks’ (Backdoor Computing Attacks, 28th April 2019) < https://www.malwarebytes.com/backdoor/ > Accessed 22/01/2021.

Crown Prosecution Service ‘Cybercrime - prosecution guidance’ (Legal Guidance, Cyber/online crime, 26th September 2019) < https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance > Accessed 30/01/2021.

UK General Public Acts ‘Computer Misuse Act 1990’ (1990 c.18, 25th September 2010) < https://www.legislation.gov.uk/ukpga/1990/18/contents > Accessed 30/01/21.

UK General Public Acts ‘Data Protection Act 2018’ (2018 c.12, 23rd May 2018) < https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted > Accessed 30/01/2021.

UK General Public Acts ‘Investigatory Powers Act 2016’ (2016 c.25, 1st December 2016) < https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted > Accessed 03/02/2021.

UK General Public Acts ‘Serious Crime Act 2015’ (2015 c.9, 13th March 2015) < https://www.legislation.gov.uk/ukpga/2015/9/contents/enacted > Accessed 03/02/2021.

UK General Public Acts ‘Criminal Damage Act 1971’ (1971 c.48, 13th October 2010) < https://www.legislation.gov.uk/ukpga/1971/48/contents > Accessed 03/02/2021.

UK General Public Acts ‘Forgery and Counterfeiting Act 1981’ (1981 c.45, 20th January 2011) < https://www.legislation.gov.uk/ukpga/1981/45 > Accessed 03/02/2021.

Jake Frankenfield, ‘Cryptocurrency’ (Investopedia, Darknet Market, 1st February 2021) < https://www.investopedia.com/terms/d/darknet-market-cryptomarket.asp > Accessed 03/02/2021.

CLRNN ‘Reforming the Computer Misuse Act 1990’ (Criminal Law Reform Now Network, publications and reports, 1st July 2020). < http://www.clrnn.co.uk/publications-reports > Accessed 24/02/2021.

Devan Joseph and Biz Carson ‘This guy bought 'Google.com' from Google for one minute’ (business insider, Tech, 1st October 2015) < https://www.businessinsider.com/this-guy-bought-googlecom-from-google-for-one-minute-2015-9?r=US&IR=T > Accessed 28/02/2021.

Alfred NG, ‘How the Equifax hack happened, and what still needs to be done’ (Cnet, Tech 7th September 2018) < https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/ > Accessed 01/03/2021.

Kaspersky ‘what is an IP address – definition and explanation’ (definitions, November 17th, 2020) < https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address > accessed 20/04/2021.

Domaintools ‘What is Whois Information and Why is it Valuable?’ (Support, September 19th, 2017) < https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable > Accessed 20/04/2021.

Cloudfare ’what is DNS?’ (DNS learning objectives, March 30th, 2019) < https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/ > Accessed 20/04/2021.

Symantec, Norton ’What is Spyware?’ (Norton Blog, 7th September 2015) < https://uk.norton.com/norton-blog/2015/08/what_is_spyware_.html > Accessed 20/04/2021.

Kaspersky ’What is Ransomware?’ (Definitions, 3rd April 2019) < https://www.kaspersky.com/resource-center/definitions/what-is-ransomware > Accessed 20/04/2021.

Symantec, Norton ’What is adware?’ (Emerging threats, 20th April 2019) < https://us.norton.com/internetsecurity-emerging-threats-what-is-grayware-adware-and-madware.html > Accessed 20/04/2021.