The Criminal Law Reform Now Network

Launched in 2017, and partly funded by an AHRC Network Grant,[1] the mission of the Criminal Law Reform Now Network (CLRNN) is to facilitate collaboration between academics and other legal experts to gather and disseminate comprehensible proposals for criminal law reform to the wider community. We include members of the public and mainstream media as well as legal professionals, police, policymakers and politicians. Our proposals might require legislation but we do not restrict ourselves to such projects. We are also interested in reforms which public bodies such as the Home Office, Police or CPS can bring about by internal policies, as well as reforms which require the support of some of the judiciary, bearing in mind the proper judicial constraints on law making. We are ready to consult with and make recommendations to anyone who has the power to bring about reform.

More information about the CLRNN, including our other reform projects, can be found at our website (www.clrnn.co.uk) and by following us on Twitter @CLRNNetwork. We have also published an edited volume exploring reform proposals.[2]

CLRNN Committee

***Co-Directors*:** Dr John Child, Birmingham Law School (J.J.Child@bham.ac.uk); and Dr Jonathan Rogers, University of Cambridge (jwr53@cam.ac.uk).

Committee: Prof Liz Campbell, Monash University; Mr Simon McKay, Barrister; Mr Paul Jarvis, Barrister; Ms Abigail Bright, Barrister; Mr Raj Chada, Solicitor; and Dr Laura Noszlopy, University of Birmingham.

Contributors to Computer Misuse Act Report

Working with the CLRNN Committee and Project Lead, a range of external contributors have variously offered their expertise in discussing, researching, drafting, and/or editing across the report.

Project Lead: Mr Simon McKay.

External Contributors: Audrey Guinchard, Peter Sommer, Lyndon Harris, Sebastian Walker, Amy Woolfson, Abhilash Nair, Duncan Campbell, David Wall, Richard Clayton, Ian Walden, Michael Turner, Ian Henderson, Aled Evans, Katy-Louise Payne, Katie Maras, Oriola Sallavaci, Andrew Charlesworth, Nicola Searle, Roxana Bratu, Naomi Colvin, Wendy Grossman, Chris Marsden, Robert Kaye, Stavros Demetriou, Ottilia Shaanika, Hans Crombag, Rachel Gimson, Kat Sommer, Krisztina Petreczky, Peter Horsfall, Josh Underwood.

---

[1] Grant Ref: AH/R013160/1.

[2] Child and Duff (eds), *Criminal Law Reform Now: Proposals and Critique* (Hart, 2019).

REFORMING THE COMPUTER MISUSE ACT 1990

CLRNN REPORT

CONTENTS

CHAPTER 1

INTRODUCTION

1.1 PROJECT INTRODUCTION

1.1.1 The 'Computer Misuse Act Project' (CMA Project) was recommended at our first open project meeting in June 2017 by Dr Audrey Guinchard, University of Essex. Of the various topics recommended and discussed at the meeting, the CLRNN Committee selected the CMA Project because we were satisfied on each of our core project criteria:

(1) Substantive Need: It was clear that the Computer Misuse Act 1990 requires significant reform to make it fit for the 21st Century, with problems identified across offences, defences, sentencing and prosecutorial guidance;
(2) Relevant Expertise: We were satisfied that we could build a collaboration of legal experts (across academia, industry and practice) to produce a robust and authoritative report;
(3) Potential Impact: We identified existing calls for reform, as well as a broad willingness from relevant reform institutions to engage with our recommendations.

CLRNN Committee member Mr Simon McKay agreed to lead the project.

1.1.2 The project originated in September 2017. We hosted a symposium event at the University of Sussex which brought together a variety of computer misuse experts to identify and discuss the priorities for the project. This resulted in an open-access Project Framework Document (published on our website), which has provided the

structure for the project and report. Sections of the report were then commissioned to different experts, including collaborative teams, for research and drafting. The CLRNN Committee provided comments on these drafts, before they were more formally workshopped at a Scrutiny Symposium Event at the University of Birmingham in May 2019. This was followed by a further round of expert editing, involving collaborators from across the Network, providing critical reflections on all aspects of the project. The report was later compiled and edited as a single document, allowing for a concluding round of expert review, before being finalised by the Project Lead and CLRNN Committee.

1.1.3 We are pleased to lend our voice to the variety of commentators calling for reform of cyber regulations in general, and the Computer Misuse Act 1990 in particular. In recent months, this includes (but is not limited to) reviews at a European level,[3] at the National level,[4] reviews within the National Crime Agency,[5] as well as campaigns for reform from those within the cyber security industries.[6]

1.1.4 Within this CLRNN report, we bring together a variety of experts to provide an independent assessment of the current law and practice. We highlight problems, and we present concrete and workable options for reform. The report is available in hard copy from Dr John Child (J.J.Child@bham.ac.uk), and electronically (open-access) on our website.

1.2 CMA 1990 HISTORICAL CONTEXT

1.2.1 Public awareness of something called 'computer crime' can be traced back at least as far as the early 1970s. In 1970 a teenager called Jerry Neil Schneider acquired information about the ordering procedures of a US telephone company and used a computer terminal to order equipment which would be dropped off at a place of his choosing and then sold on. The Equity Funding fraud of 1973 involved the computer-aided manufacture of computer records showing 60,000 bogus life-insurance policies that were sold on for reinsurance and which in turn were used to prop up a Ponzi investment scheme; the crime was turned into a TV movie.[7] In 1978 Stanley Rifkin

[3] See, for example, recent work on cross-border policing: https://www.europol.europa.eu/newsroom/news/fs-isac-and-europol-partner-to-combat-cross-border-cybercrime.
[4] See, for example, concerns relating to Brexit: https://www.gov.uk/government/publications/eu-cyber-security-certification-eu-exit-call-for-views.
[5] For updates on their work in this area, see: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved.
[6] See, for example, the work of the NCC Group: https://www.nccgroup.trust/uk/about-us/what-we-do/computer-misuse-act/.
[7] Billion Dollar Bubble (BBC, 1978).

carried out a $10.2 million wire transfer fraud using acquired authentication codes. He flew to Switzerland and converted the money into diamonds. These and similar crimes were frauds. There were also a number of instances of physical attacks on computer hardware, sometimes to generate additional income for those who would have to repair them, sometimes for blackmail and sometimes ideological reasons.[8]

1.2.2 Until 2010 or so, most people referred to 'computer crime', but more recently this has changed to 'cybercrime'. The term 'cyberspace' is usually dated either to the Danish artist Susanne Ussing in the late 1960s or, more frequently, to the novelist William Gibson and his short story *Burning Chrome* (1982) and novel *Neuromancer* (1984). In the UK we had a Metropolitan Police Computer Crime Unit from 1984 onwards, a Police Central eCrime Unit (another briefly popular term) between 2008 and 2012 which was then drawn into the National Cyber Crime Unit, part of the National Crime Agency. Cybercrime includes criminal activity on networks including the Internet where, perhaps, 'computer crime' was limited to activities within computers.

1.2.3 With the arrival of the hobbyist personal computer and the availability of low cost modems it became possible for individuals, particularly teenagers, to routinely access corporate computers with ease. Most of these early activities were recreational and designed to show off prowess rather than to make serious money. By 1984 the phenomenon was sufficiently well established for Hollywood to create the successful movie *WarGames*, a movie that prompted Ronald Regan to ask his military advisors if it really was that bad.[9]

1.2.4 Although the concept of malware[10] is almost as old as computing itself, and the notion of self-replicating malware – the essence of what a computer virus is – appears in academic literature in the late 1950s / early 1960s, the actual use of the term 'computer virus' is usually attributed to Fred Cohen in 1983. By 1986 the earliest form of well-distributed viruses, *Brain*, gained general publicity and in 1988 the proto-Internet was infected by the *Morris Worm*. Trojans, malware which allows covert remote access to devices across networks, appeared around the same time.

1.2.5 In the United Kingdom in 1983, a live broadcast BBC show devoted to education in micro computing was subjected to an on-air attack or hack which had not been

[8] Discussed in Cornwall, *DataTheft* (London, 1987) Chapter 9.
[9] Kaplan, *Dark Territory: The Secret History of Cyber War* (Simon & Schuster, 2017).
[10] Malware is the general term for computer code designed to have a bad effect by either deleting or corrupting contents or preventing normal working. It can be designed simply to operate on one computer to which it has been installed or it can be the subject of automated distribution as in worms and viruses (these two terms overlap). A Trojan is a program which creates a covert backdoor to a computer accessible over a network including the Internet; the victimised computer can then be subject to extraction of its contents and/or remote control.

planned by its producers. The following year the pioneering public information access service run by British Telecom called *Prestel* was hacked and a demonstration email facility set up for the Duke of Edinburgh was compromised.

Legal Regulation

1.2.6 In 1984 the Scottish Law Commission (SLC) began a Report into the criminal aspects of 'computer crime', produced an Interim Report in 1986 and a final version the following year.[11] The SLC originally identified eight categories of computer crime: (1) erasure or falsification of data or programs so as to obtain a pecuniary or other advantage (2) obtaining unauthorised access to a computer (3) eavesdropping on a computer (4) taking of information without physical removal (5) unauthorised borrowing of computer discs or tapes (6) making unauthorised use of computer time or facilities (7) malicious or reckless corruption or erasure of data or programs (8) denial of access to authorised users.

1.2.7 The English Law Commission produced a Working Paper on *Computer Misuse* in 1988,[12] and a full Report with recommendations in October 1989.[13] In April 1989 a Conservative MP, Emma Nicholson,[14] presented to Parliament a Private Member's Bill designated 'anti-hacking' which was primarily aimed at stimulating public appetite for legislation.

1.2.8 By 1985 two of the men involved in the Prestel hack, Steve Gold and Robert Schifreen, had been identified. There was something of a debate about how they could be charged. Their actions were not for monetary gain so there was no fraud, neither was there any physical damage. There was the possibility of charging for diverting electricity,[15] presumably the additional amount of electricity used by the Prestel equipment, but this seemed far-fetched. In the end the authorities opted for the Forgery and Counterfeiting Act 1981. The case ended up in the House of Lords, then the highest point of appeal.[16] In the Court of Appeal, Lane LCJ said: 'The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a

[11] Scottish Law Commission, *Report on Computer Crime* (Law Com No 106, 1987).
[12] Working Paper No 110.
[13] Law Commission, *Computer* Misuse (Law Com No 186, 1989). Hereafter LC 186.
[14] Ms Nicholson briefly joined the Liberal Democratic Party and then rejoined the Conservatives and now sits in the House of Lords.
[15] Theft Act 1968, s13.
[16] *Gold and Schifreen* [1988] 2 WLR 984, on appeal from CACD [1987] QB 1116.

criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts.'[17]

1.2.9 Both the Scottish and English Law Commissions asked themselves what was meant by 'computer crime' and analysed the existing available offences. In the end they concluded that 'computer fraud' insofar as there was an absence of clear offences should be treated within a revision of the law of frauds as opposed to concentrating on the computer element. They could also have referred to criminal offences under, for example, section 107 of the Copyright Designs and Patents Act 1988 to address the various forms of piracy – software, video, audio and still images. Such offences are usefully referred to as 'computer-enabled crimes'. This left the issue of unauthorised access and usage of computers,[18] and it is this element that appears in the Computer Misuse Act 1990 (CMA 1990). Such offences are usefully referred to as 'cybercrimes'.

1.2.10 The decision to limit the CMA 1990 to pure cybercrimes has had a lasting impact on the number of charges made each year using that specific legislation.[19] There are many situations in which the substantive criminal act is, for example, extortion or fraud where an important element in the *modus operandi* involved evidence sufficient to add CMA charges, but where prosecutors see little point in doing so as it would make little difference to the penalties a court was likely to impose and might, indeed, simply lengthen a trial. Such overlapping and/or related offences are discussed below at **1.4**.

The Computer Misuse Act 1990

1.2.11 In its original formulation the CMA 1990 covered three substantive offences:

- Unauthorised access to computer material (section 1).
- Unauthorised access with intent to commit or facilitate commission of further offences (section 2).
- Unauthorised modification of computer material (section 3).

1.2.12 Several other decisions were made in framing the legislation. First, there would be no definition of 'computer' because it was recognised that technological forecasting was difficult.[20] Second, that jurisdiction would be worldwide and not limited to activities that were manifestly within the geographic boundaries of the United Kingdom.[21]

[17] [1987] Q.B. 1116, 1124, quoted again in the House of Lords at 1071.
[18] LC 186, Parts II and III.
[19] See Appendix B.
[20] LC 186, para 3.39.
[21] LC 186, para 4.1.

1.2.13 It did not take long for those having to work with the new provisions to realise that section 3, in particular, was inadequate. It had been designed with computer malware in mind – worms, viruses and Trojans. But what it failed to capture was the situation where a computer is compromised because it has been overwhelmed with unwanted traffic – usually referred to as 'denial of service' (DoS). When that happens there is no unauthorised modification. The first attempt at reform was made in 2002 in the House of Lords by the Earl of Northesk.[22] Further attempts were made in the Commons in 2004, 2005 and 2006. Finally section 36 of the Police and Justice Act 2006 provided substantial reform, substituting the original provision with a new, more expansive offence in the following terms:

> (1) A person is guilty of an offence if—
>
> (a) he does any unauthorised act in relation to a computer;
>
> (b) at the time when he does the act he knows that it is unauthorised; and
>
> (c) either subsection (2) or subsection (3) below applies.
>
> (2) This subsection applies if the person intends by doing the act—
>
> (a) to impair the operation of any computer;
>
> (b) to prevent or hinder access to any program or data held in any computer;
>
> (c) to impair the operation of any such program or the reliability of any such data; or
>
> (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

1.2.14 The same Act increased penalties for conviction under section 1 of the CMA 1990 from six months to 12 months,[23] and also introduced a new section, section 3A, relating to the making, supplying or obtaining of articles for computer misuse offences.[24] There were further minor clarifications of the original 1990 Act.[25]

Recent Amendments

1.2.15 By 2015 there was increasing concern over the prospects of cyber-terrorism or other large-scale cyber-attacks, in other words, attacks which relied on computers rather than the physical activity of troops, aircraft and ships. Typical techniques would

[22] Computer Misuse (Amendment) Bill 2002.
[23] Police and Justice Act 2009, s35.
[24] Police and Justice Act 2009, s37.
[25] Police and Justice Act 2009, s33 and 61.

involve large-scale DoS attacks on computers which are an important component of a nation's critical infrastructure involving the provision of internet services, electric power, food delivery, fuel availability, health services, and so on. Alternatively these computers could be infected with particular strains of malware, known as ransomware, similar to the later 2017 Wannacry virus which affected the NHS.[26] Attacks could also be directed towards hardware or cyber physical systems, as happened with the 2010 Stuxnet virus which hit Iranian facilities producing nuclear fuel.[27] Estonia had suffered a large-scale attack in 2007.[28] The legislative response to this in the UK was the introduction of offences that reflected the potential for such activity to cause 'serious damage'. Section 41 of the Serious Crime Act 2015 introduced the new section 3ZA CMA 1990, 'unauthorised acts causing, or creating risk of, serious damage'.

1.2.16 There was a further change in the same Act that dealt with 'savings' for law enforcement,[29] which are considered below at **1.4**.

1.3 PROBLEMS WITH THE CURRENT LAW

1.3.1 We discuss the full variety of problems within the CMA 1990 across the chapters of this report. However, it is useful at this stage to introduce some of the most important. Essentially, the role of the CMA 1990, like any criminal statute, is to accurately target and criminalise wrongful conduct; ensuring that legitimate and beneficial conduct (including research, enforcement and reasonable expression) is protected in the public interest. We do not believe that the current law achieves this aim. Rather, overbroad offences (and a lack of defences) serve to criminalise or supress conduct in a manner that few if any would defend.

Authorisation I

1.3.2 Authorisation or lack thereof is at the heart of the CMA 1990 and also the area where a number of digital professionals who believe their motives to be entirely ethical see themselves nevertheless as vulnerable to criminal charges. The word 'unauthorised' appears in sections 1, 2 and 3 of the CMA 1990. Section 17(8) provides an interpretation:

[26] Smart, *Lessons learned review of the WannaCry Ransomware Cyber Attack* (2018).
[27] Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon* (2014).
[28] McGuinness, *How a cyber attack transformed Estonia* (BBC Online, 2017).
[29] Serious Crime Act 2015, s44.

17(8) An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)—

(a) is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and

(b) does not have consent to the act from any such person.

1.3.3 The only exception is given to law enforcement and the security and intelligence agencies and appears in section 10:

10. Sections 1 to 3A have effect without prejudice to the operation—

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required; …

and nothing designed to indicate a withholding of consent to access to any program or data from persons as enforcement officers shall have effect to make access unauthorised for the purposes of any of those sections.

1.3.4 The 'powers of inspection, search and seizure' can be, among others, under Part 2 of the Police and Criminal Evidence Act 1984, and under Part 5 of the Investigatory Powers Act 2016, 'Equipment Interference'.

1.3.5 This can leave those who believe that their computer-related investigations and activities improve cyber security and are ethical at the mercy of decisions made by the Crown Prosecution Service. We discuss this in **Chapter 4**.

Authorisation II: Restrictions on the activities of investigators

1.3.6 Looking first at the position of non-law-enforcement investigations: these may be carried out by employees of a victim organisation or external experts brought in to assist after some form of incident. For many IT systems the boundaries may not be obvious. No longer is it the case that all processing takes place in computers that are obviously solely in the control of an organisation that is experiencing an incident. Some processing might be handled in computer facilities owned by others – under an outsourcing contract or within a cloud (cloud services are really out-sourcing facilities on a very large scale). Such arrangements may be used to manage large databases and other forms of complex processing such as artificial intelligence. In addition an organisation's computer facilities are often dependent on data which is provided by

others. Customers use a web interface to input orders or make queries; or, as in e-commerce, one company and its computer systems create computer links to other companies with which it has a partnership or supplier relationship.

1.3.7 In addition, corporate computer systems may open links to specialist contractors so that they can provide needed services such as consultancy. Organisations may also use data feeds for commodities pricing, weather forecasts, and so on. There could be links in banking, credit checking and other financial services. Many large organisations also allow their employees to link their privately-owned devices such as personal computers, laptops and smartphones to the corporate system; this is referred to as BYOD – Bring Your Own Device – with the aim of improving productivity as the employee works away from his/her desk and outside formal business hours. But it is not clear whether that organisation is then authorised to have access to the 'private' aspects of the employee's device.

1.3.8 A yet further 'boundary' problem may occur where email and email archiving takes place or where back-up facilities are out-sourced – one reason for doing so may be in the context of disaster recovery planning so that if an organisation suffers from a flood, fire or bomb, essential data is preserved. In fact, back-up data may be an important source for a forensic investigator.

1.3.9 The problem for the investigator is that an organisation can only authorise investigations into its own systems, but the source of a problem may be in the data it is receiving from outside or the external processing upon which it relies.[30] The investigator will be under pressure to identify the source of a problem and to solve it, but where the cause is potentially external there will also be the countervailing concern that there is no authorisation to investigate beyond a certain point. The investigator – and the organisation that commissions the investigation – must then look at the precise contractual relationship with the external systems. And when examined, contracts may lack sufficient detail because the circumstances were not anticipated.

1.3.10 Some actions to stop an external cause of system interference such as 'hacking back' – deliberately and consciously attacking a third-party computer – are clearly

[30] Boundary and interpretation issues of this kind are common. Just as it is difficult to identify who is 'responsible' for a system, we may also question whether 'ownership' of system implies a) systems in my physical location / vicinity b) systems that have been purchased outright c) systems that have been rented or leased? Similar consideration apply to 'data' – does this cover a) data an organisation generates b) data an organisation licenses or c) data an organisation ingests from open/publicly available sources?

prohibited; but many lesser actions, however well intentioned, may be illegal as well. The test in the CMA 1990 is that an accused must know of the lack of authorisation before an offence is committed – section 1(1)(b) and (c) and section 3(1)(b) and (c) – but the fear is that whatever an accused says in court, his suspicions about the legality of the action may be interpreted as knowledge.[31]

1.3.11 Under current law, the only safe route would be for the investigator to say that the police need to be brought in so that their powers under section 10 CMA can be used. But there will be many instances in which the police will feel that the incident being investigated does not point to obvious criminality or, if it does, that they need to concentrate their scarce resources where the harm is on a larger scale. This approach also precludes proactive investigation or threat intelligence collection activities.

Authorisation III: Restrictions on the activities of penetration testers

1.3.12 The problem of identifying the precise boundaries of a computer system also applies to penetration testers, also referred to as 'white hat hackers' or 'ethical hackers'. Such is the complexity of many computer systems that it is impossible to achieve security simply by using robust development techniques and testing. The value of the penetration tester is that they work from outside and use a battery of techniques similar to those that might be deployed by a hostile hacker. Penetration testers nearly always operate under pre-agreed rules of engagement; the tests they run are designed to be finite in nature and with specific technical aims such as identifying out-of-date programs; plainly neither the penetration tester nor the organisation employing them want to destroy the organisation's computer systems.

1.3.13 Penetration testing has been an established feature of cyber security for at least 15 years. There is a formal accreditation scheme - CREST - and the UK government provides a service manual.[32]

1.3.14 But the external computer links referred to above are likely to be an important source of insecurity. How are penetration testers to identify the boundaries of their authority and still deliver to their customer what is being sought – re-assurance about levels of security?

[31] Discussed in Sommer, 'Computer Misuse Prosecutions' (2006) *Journal of the Society of Computers and Law*.
[32] *Vulnerability and penetration testing* (Online at gov.uk, last updated in 2017).

Authorisation IV: Restrictions on the activities of academic and commercial researchers

1.3.15 Another area of critical importance to cyber security is the work of researchers who identify and investigate new threats that could apply to large numbers of computer users. The term normally used for this activity is 'threat intelligence'. Whereas many generic threats are extremely well-known – viruses, Trojans, compromises of websites, etc – the security professional whose job is to advise and implement security for their employers needs to know of new specific threats so that preventative and evasive action can be taken. Threat intelligence can be carried out by commercial companies,[33] but also by academic groups.[34] There are also variations in method.[35]

1.3.16 One reason why threats emerge is because 'bad actors' have identified weaknesses in widely used operating systems and software. Once identified the weaknesses can be turned into 'exploits'. From time to time new forms of malware also appear – these can include new mechanisms to enable data to be destroyed or computers taken over, and new methods to conceal the ways in which the malware is installed onto a 'target' computer. Another concern of threat intelligence is new forms of social engineering. In social engineering the aim is not so much to use a technical method as to find ways of deceiving a legitimate user into installing rogue software or otherwise providing information to outsiders which would enable them to take control of a system – this may be as simple as a misleading phone call or the request to click on a link in an email or on a website. 'Ransomware', where an organisation is told that their computer is already infected with a program that will encrypt its contents beyond any form of recovery unless a ransom fee is paid, will feature both technical and social engineering means. In all these instances the cyber security and threat professional can help design specific technical methods to block or thwart hostile actors from using the exploits; in the case of social engineering threats it may be necessary to send out specific warnings to members of staff in potential victim organisations about the precise form the attack might take, or indeed building the warning into any staff education process that is in place.

[33] Including, for example, the NCC Group; FireEye; and others.

[34] Including, for example, https://citizenlab.ca/; https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/space-and-technology/cyber-risk-outlook-2019/; https://www.cam.ac.uk/Malicious-AI-Report.

[35] It can be useful to distinguish security research (identifying vulnerabilities in systems that require fixing to avoid exploits by bad actors) and threat intelligence research (identifying bad actors, and their tactics, techniques and procedures – which IP domains they use, which malware they develop, which targets they have, in order to warn potential victims, and enable (automated) protection mechanisms to include criminals' signatures to more effectively defend against them). Both make significant contributions to broader public policy cyber security objectives (eg improving cyber resilience, and tackling cybercrime).

1.3.17 The findings of threat intelligence are also used by companies that produce cyber security software; a typical commercial anti-virus software product as used by organisations and individuals alike will update its list of threats to be detected and ameliorated on a daily basis.[36]

1.3.18 A practical problem is whether 'scanning the Internet', looking for sources of potential disruption, involves accessing or interfering with the computers being scanned. Digging a little more deeply, is there a difference in law between asking a computer to identify itself and interrogating further to see what facilities it offers? As before, how does one locate the boundary? One of the main tools used is called Zmap.[37]

1.3.19 The research may also extend to identifying the people responsible for the new exploits. These may be individuals, organised crime groups, ideologically motivated groups, or nation states. A classic research method involves using a 'honeypot', a computer specially set up to appear to be enticing to a hostile actor; a hidden feature of the honeypot is to try and identify the computer sources of an attack and to capture as much code as possible so that the code can be examined to see if there are similarities in terms of style with the work of known hostile hacking groups.[38]

1.3.20 If a strict interpretation of section 17 of the CMA 1990 is taken then the only computers that can be examined are those in the control of organisations and individuals in a position to grant 'authorisation'. Any probing of a remote computer which might be the source of an attack could only be carried out by law enforcement using their section 10 powers. Researchers using a honeypot could, provided that they set up the honeypot in the first place, look at the impact of attacks on the honeypot computer but would be very limited in probing the source of those attacks. This restricts the ability of security researchers to identify threats and pass vital information to public enforcement bodies.

1.3.21 The public policy issue, therefore, is that under current law only law enforcement and the National Cyber Security Centre (NCSC), which is part of GCHQ and inherits its powers under section 10 of the CMA 1990, Part 5 of the Investigatory Powers Act 2016 and section 3 Intelligence Services Act 1994, appear to be the only UK bodies that can carry out threat intelligence beyond a corporate boundary. This places a significant limit on the resources available to identify threats and also on the range of threats investigated; law enforcement will concentrate on events likely to have criminal

[36] For example, Norton 360, Avast, BitDefender, McAfee, etc.
[37] Other tools are Shodan and Censys, all of which are based in/registered in the US because the port scanning required as part of the tools/service is another grey area in English law.
[38] See, for example, the Honeynet Project: https://www.honeynet.org/project.

outcomes, NCSC's central remit is state security. The current legal framework therefore runs in direct opposition to repeatedly stated national policy of partnership working across public and private sector, effectively preventing industry from deploying its technical capabilities in the pursuit of national cyber security objectives.[39]

Section 3A: Making, Supplying or obtaining Articles for under s1, 3, and 3ZA

1.3.22 The aim of section 3A was to find an additional means of punishing hostile attackers by looking at the tools that they use. The main problem in drafting the legislation was that code and tools used by hackers are either identical to or very similar to code and tools used legitimately by computer and network systems administrators and by penetration testers.

1.3.23 Probing and testing code used by penetration testers is often freely available via websites such as www.darknet.org which, despite its sinister name, dates back to the year 2000, long before the arrival of the hidden or dark web and 'onion' websites.[40] But there is nothing that can be done to prevent such code being used for criminal purposes.

1.3.24 The main types of code that do not have any legitimate purpose include those used for creating and managing botnets (as used in DDoS attacks) and harvesting software which will scan a computer for specific items such as banking and credit cards credentials, Social Security numbers and other data which can be later exploited in frauds. The primary route by which bad codes and tailored services such as botnets-for-hire are distributed is the hidden or dark web.

1.3.25 'Articles' can include items that are not code, of course. Typical examples include credentials for access to banking websites, credit card pin numbers, and similar. These

[39] The 2016-2021 National Cyber Security Strategy makes repeated reference to the role of the private sector in tackling cybercrime and reducing cyber vulnerabilities in UK infrastructure. Elsewhere, the 2018 Serious and Organised Crime Strategy identifies cybercrime as a significant threat to UK prosperity, and commits to a holistic approach that will equip '(…) the private sector (…) to play their part in a single collective endeavour to rid our society of the harms of serious and organised crime.'

[40] In addition to the regular, easily accessible sites on the world wide web and which can be found via the use of search engines such as Google and Bing there are others which are referred to as being on the 'dark web'. These require specialist knowledge and in some instances specialist software in order to be accessed. One sub-set of this is accessed via an encrypted browser and connection; they are known as 'onion' sites after the specialist browser called The Onion Router (TOR).

will have been collected via phishing and then sold in blocks on rogue websites on the dark web.

Corporate Liability

1.3.26 The construction of sections 1, 2 and 3 of the CMA 1990 all begin with the words: 'A person is guilty of an offence if'. The question then is whether 'person' is limited to a single human being or can be extended, subject of course to the availability of evidence, to the actions of a corporate entity.

1.3.27 As far as we know, to date there has been no attempted prosecution of a corporate entity in a computer misuse offence. Schedule 1 of the Interpretation Act 1978 provides that 'person' includes a body of persons corporate and unincorporated. The consequence of this, as section 5 of the 1978 Act makes plain, is that where the word 'person' appears in an Act of Parliament, unless the contrary intention appears, that word should be construed as including a company, a corporation (which will include a limited liability partnership) or an unincorporated association. It follows that the use of the word 'person' in the offence-creating provisions of the CMA 1990 could include a legal person, as opposed to a 'natural person'.

1.3.28 Later in this report (**Chapter 2**) we examine the problems of demonstrating a mental element, such as 'intent', in the actions of a corporate body. There are also potential issues if an organisation is to be found responsible for the actions of its employees as an accessory or through vicarious liability.

Jurisdiction

1.3.29 The CMA 1990 deals with jurisdiction in sections 4-9. Although there have been a number of amendments particularly in the Police And Justice Act 2006 and the Serious Crime Act 2015, the original text of the 1990 Act identified that computer or cybercrime traverses territorial boundaries. Matters of concern include:

- The position of an individual in the UK accessing or attacking a computer in another country A;
- the position of an individual in the UK offering for sale malicious code, compromised access codes and credentials on a website based in another country B which is then used to attack computers et cetera in yet further countries;

- the position of a UK citizen operating from another country C accessing or attacking a computer in yet further overseas countries;
- the position of a UK citizen operating from another country C offering for sale malicious code, compromised access codes and credentials, botnets-as-a-service-for-hire on a website based in yet another country which is then used to attack computers et cetera in yet further countries;
- the position of a non-UK citizen operating from the UK and attacking a computer based in the UK;
- the position of a non-UK citizen operating from a third party country but attacking a computer based in the UK;
- situations where cloud facilities are attacked and the cloud provider has several different data centres, places where data is stored and processed, in a variety of locations and is unable to say at any one time where any specific item of data is being held.

1.3.30 The relevant sections of the CMA 1990 begin by asserting that it is irrelevant for the purposes of any offence whether the accused was actually in the UK provided that there is what is referred to as a 'significant link' with the UK.[41] If an accused person is outside the UK he must be a citizen of the UK and any offence charged must be an offence under the law of the country in which it is said to have occurred.[42] Section 6 of the CMA 1990 deals with conspiracies and attempts.

1.3.31 There are a number of examples demonstrating computer offences as genuinely international in nature and reach. Daniel Kaye's services as a hacker-for-hire were taken up by a senior official at Cellcom, a Liberian mobile phone provider, to attack its main rival, Lonestar MTN. He deployed a Distributed Denial of Service attack. Lonestar's customers were badly affected, and collateral damage was caused in Germany because the DDoS code was not uniquely focused on Lonestar's equipment. Kaye pleaded guilty in Germany but his UK defence team investigated whether the UK courts had jurisdiction as the DDoS attack was mounted from his then home in Cyprus and his attack had no impact on UK computers. In the end they concluded that Kaye, who had dual British and Israeli citizenship, was subject to UK jurisdiction; he pleaded guilty, and he was jailed for two years and eight months.[43]

1.3.32 Sections 6 and 7 of the CMA 1990 deal with inchoate offences – conspiracy and attempts.

[41] CMA 1990, s4.
[42] CMA 1990, s5.
[43] Rahim, 'British man jailed for hacking Liberia thought to be the first to take entire nation offline' (*Independent Online*, 2019).

1.3.33 Although the scope of the law seems comprehensive there can be difficulties in terms of presenting evidence. Not only may it be necessary to adduce evidence of the activities of individuals in overseas jurisdictions and evidence that computers were accessed or attacked, but in some circumstances there may be doubt about the equivalence of cybercrime offences in the UK and overseas territories. Although an increasing number of countries have signed the Treaty of Budapest (the Cybercrime Convention), not all signatories have yet aligned their legislation and there are still countries that have almost no cybercrime-related offences.

1.3.34 All of the problems discussed in this section appear across this report, directing our recommendations on offences (**Chapter 2**), defences (**Chapter 3**), prosecutorial guidance (**Chapter 4**), sentencing (**Chapter 5**) and civil provisions (**Chapter 6**). What is needed is a full re-evaluation of the current law, and we provide that in this comprehensive report.

1.4 RELATIONSHIP WITH OTHER OFFENCES

1.4.1 There are a number of other items on the statute book, the effects of which need to be considered when reviewing the operation of the CMA 1990.

Fraud Act 2006

1.4.2 The Fraud Act 2006 (FA 2006) was designed to simplify and clarify previous attempts at defining 'fraud'. The previous law had a large number of specific fraud offences, defined with reference to different types of consequence. A number of these had appeared in Theft Acts in 1968 and 1978, and had been criticised in a Law Commission report in 2002.[44] Often the confusion and overlap meant that prosecutors concentrated on the common law of conspiracy to defraud as opposed to negotiating their way to finding evidence to support the more specific offences. One particular area of criticism was that it appeared to be impossible to deceive a computer, the essence of deception being that a human being was deceived. The Law Commission recommended a single offence of fraud with three main ways by which the crime could be committed – by way of false representation (Section 2), failing to disclose information (Section 3) and abuse of position (Section 4).

[44] Law Commission, *Fraud* (LC No 276, 2002).

1.4.3 Many 'cybercrime' incidents are in fact frauds and prosecutors often prefer to base charges on fraud, which they regard as the essence of the activities, rather than computer misuse even though unauthorised access and/or impairment provided an important element in the accused's modus operandi. In practical terms, the addition of computer misuse counts to an indictment may make no difference to the overall punishment in the event of a guilty finding; all that happens is that the trial lasts longer.

1.4.4 But there are two features newly introduced in the FA 2006 which have a direct bearing on the CMA 1990. Section 6 concerns possession of articles for use in fraud, and section 7 deals with making or supplying articles for use in fraud. Section 8(1)(b) says: '"article" includes any program or data held in electronic form.'

1.4.5 This overlaps with section 3A of the CMA 1990: making, supplying or obtaining articles for use in offence under section 1 or 3.

1.4.6 From a prosecutor's point of view, pursuing a charge under section 3A of the CMA 1990 appears to require proof that the articles could be used for an offence under sections 1 or 3. By using sections 6 or 7 of the Fraud Act 2006 the proof has to be that the tools could be used to commit a fraud. The CPS provides the following advice in its charging guidance for computer misuse:

> Prosecutors may wish to consider whether the 'article' might be intended for use in fraud and consider whether there is an offence contrary to section 7 and / or section 6 of the Fraud Act 2006. An offence of making or supplying articles for use in fraud contrary to section 7 punishable by a maximum of 10 years imprisonment. An offence of possession of articles for use of in fraud contrary to section 6 is punishable by a maximum of 5 year's imprisonment.

1.4.7 The offences can be used in situations such as: cloned bank cards, apparatus for collecting the data and manufacturing of cloned bank cards, collections of fraudulently obtained bank accounts credentials, equipment for acquiring data from contactless cards, keystroke monitoring software, Trojan backdoors and similar for acquiring credentials (including attempts at 'phishing', booby-trapped web pages, etc) and many others. Indeed, the use of a specialist hardware device (a remote controlled KVM) mentioned above was prosecuted under the Fraud Act as opposed to the 1990 Act.[45]

[45] Leydon, 'UK bank heist-by-KVM gang sent down for 24 years after nicking £1.2m' (*The Register Online*, 2014).

Data Protection Acts 1998 and 2018

1.4.8 The Data Protection Act 1998 (DPA 1998) created a number of criminal offences that could have a cyber dimension. For example, under section 55(1), it is an offence to 'knowingly or recklessly obtain, disclose or procure the disclosure of personal information without the consent of the data controller.'

1.4.9 The main target of the section was so-called 'pretext calls', which typically involve someone assuming the identity of a person entitled to request and obtain information. But it can also include the use of 'phishing' emails and fake websites – which could also attract charges under both the CMA 1990 and sections 6 and 7 of the FA 2006.

1.4.10 If a person had obtained personal information illegally, section 53(3) made it a criminal offence to offer or to sell personal information. Section 55(4) and section 55(5) created offences of selling and offering to sell personal data and included advertisements to that effect.

1.4.11 The main purpose of the Data Protection Act 2018 (DPA 2018) was to provide statutory support for the UK's adoption of the general data protection regulation, GDPR.

1.4.12 This is now reproduced with some strengthening in section 170 DPA 2018:

(1) It is an offence for a person knowingly or recklessly—

(a) to obtain or disclose personal data without the consent of the controller,

(b) to procure the disclosure of personal data to another person without the consent of the controller, or

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

(4) It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under subsection (1) was committed.

(5) It is an offence for a person to offer to sell personal data if the person—

(a) has obtained the data in circumstances in which an offence under subsection (1) was committed, or

(b) subsequently obtains the data in such circumstances.

1.4.13 There are defences to section 170(1) if the procurement, etc was 'for the purposes of preventing and detecting crime' and 'in the public interest' – section 170(2); and 'reasonable belief' that the information had been obtained legally and 'with a view to the publication by a person of any journalistic, academic, artistic or literary material', and 'in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.' – section 170(3). Section 170(1)(c) adds to the DPA 1998 to cover the position where someone acquires personal data lawfully but then retains it without the consent of the data controller.

1.4.14 As with the DPA 1998, the illegal activities under section 170 could also attract charges under both the CMA 1990 and section 6 and 7 of the FA 2006. However DPA offences are, of course, limited to personal data.

Investigatory Powers Act 2016

1.4.15 The purpose of the Investigatory Powers Act 2016 (IPA 2016) was to update the earlier Regulation of Investigatory Powers Act 2000 and other Acts. One trigger was the Snowden whistleblowing revelations about the activities of the electronic spying agencies GCHQ and NSA. Another was the uncovering of surprising legal interpretations of other laws as a result of actions in front of the Investigatory Powers Tribunal (IPT) by the NGO Privacy International and others.[46] There had also been a series of reports by Parliament's Intelligence and Security Committee (ISC).[47]

1.4.16 The main new feature relevant to discussion of the CMA was the introduction of the concept of 'equipment interference'. Up to that point equipment interference, in effect licensed 'hacking', was dealt with as 'property interference'. As we have seen, police powers derived from section 10 of the CMA 1990 and the powers of the intelligence agencies came from section 5 of the Intelligence Services Act 1994. In addition there was section 94 Telecommunications Act 1984, which empowered the Secretary of State to give directions 'of a general character' to telecommunications

[46] For example, *Privacy International and Greennet & Others v (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters*, IPT 14/85/CH 14/120-126/CH.
[47] For example, *Privacy and Security: A modern and transparent legal framework* (HC 105); *Report on the draft Investigatory Powers Bill* (HC 795).

companies 'in the interests of national security or relations with the government of a country or territory outside the United Kingdom'.

1.4.17 The main detail is in Part 5 of the IPA 2016. Section 101 describes the scope – a warrant may be aimed or 'targeted' – either at specific equipment or at specific individuals or organisations:

(1) A targeted equipment interference warrant may relate to any one or more of the following matters—
  (a) equipment belonging to, used by or in the possession of a particular person or organisation;
  (b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
  (c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;
  (d) equipment in a particular location;
  (e) equipment in more than one location, where the interference is for the purpose of a single investigation or operation;
  (f) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description;
  (g) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information;
  (h) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment.

(2) A targeted examination warrant may relate to any one or more of the following matters—
  (a) a particular person or organisation;
  (b) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
  (c) more than one person or organisation, where the conduct authorised by the warrant is for the purpose of a single investigation or operation;
  (d) the testing, maintenance or development of capabilities relating to the selection of protected material for examination;
  (e) the training of persons who carry out, or are likely to carry out, the selection of such material for examination.

1.4.18 Equipment interference warrants for the use of the intelligence agencies must be issued under the personal signature of a minister (sections 102-105). Law

enforcement warrants are issued by police chief constables and their equivalents in other agencies (section 106). Both types of warrant are subject to approval by Judicial Commissioners (section 108). The test throughout is 'whether the warrant is necessary' and 'whether the conduct which would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct'. The role of the Investigatory Powers Commissioner and other Judicial Commissioners is covered in Part 8, Chapter 1.

1.4.19 Section 126 requires individuals and companies in receipt of a targeted equipment interference warrant to provide assistance in giving effect to the warrant. Section 128 does the same for telecommunications companies. There is also a duty not to make unauthorised disclosures (section 132), in effect imposing secrecy on the operations.

1.4.20 Part 6 of the IPA 2016 covers 'bulk warrants' and Part 6, Chapter 3 refers to bulk equipment interference warrants. The case for bulk warrants in general was the subject of a Report by the Independent Reviewer of Terrorism Legislation, David Anderson QC in 2016.[48]

1.4.21 Part 9 gives two more powers to the Secretary of State: section 252 provides for the issuing of a National Security Notice to a telecommunications operator to 'provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively' and section 253 covers Technical Capability Notices which can order any 'operator' to have the capability to provide facilities to support, among other things, the means of equipment interference. The issuing of such notices is subject to approval by Judicial Commissioners (section 254).

1.4.22 Much more detail is covered in a Code of Practice,[49] which describes what is involved in equipment interference:

> Equipment interference describes a range of techniques used by the equipment interference authorities that may be used to obtain communications, equipment data or other information from equipment. Equipment interference can be carried out either remotely or by physically interacting with the equipment.
>
> Equipment interference operations vary in complexity. At the lower end of the complexity scale, an equipment interference authority may covertly download data from a subject's mobile device when it is left unattended, or an equipment interference authority may use someone's login credentials to gain access to data held on a computer. More complex equipment interference operations may

[48] Anderson, 'Report of the Bulk Powers Review' (Cm 9326, 2016).
[49] Home Office, *Equipment Interference: Code of Practice* (2018).

involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device.

1.4.23 Paragraphs 3.6 to 3.9 refer to the interaction with the CMA 1990. Many of the actions involved in equipment interference would normally be offences under sections 1, 2, 3, 3ZA, and 3A, but where an equipment interference authority has obtained an appropriate authorisation no offence is committed. This is on the basis of the protections – 'savings' – in section 10 of the CMA 1990 and section 5 of the ISA 1994. Activities by law enforcement officers and members of the intelligence and security services outside the scope of warrants would of course be offences under the CMA 1990.

Terrorist offences

1.4.24 There are a limited number of situations involving terrorism which could be tried under section 3ZA Computer Misuse Act. The test applied is that a person is guilty if an act causes 'serious damage of a material kind or is reckless as to whether such damage is caused'. Damage of the material kind is further defined as damage to human welfare, damage to the environment, damage to the economy of any country, or damage the national security of any country (section 3ZA(2)) and damage to human welfare applies if it causes loss to human life, human illness or injury, disruption of the supply of money, food, water, energy or fuel, disruption of the system of communication, disruption facilities for transport, or disruption of services relating to health (section 3ZA(3)).

1.4.25 The potentially overlapping terrorist offences could include 'possession of an article for terrorist purposes' under section 57 of the Terrorism Act 2000. This might involve the possession of software and hardware capable of mounting a large-scale malware or DDoS attack but would presumably also need some indication of deployment for terrorist purposes. Section 6 of the Terrorism Act 2006 'providing or receiving instruction or training for terrorism' might cover instruction in the use of cyber weaponry. Section 2 of the same Act 'dissemination of terrorist publications' could also be applied to an instruction manual for cyber attacks.

1.4.26 All of the recommendations for reform made in this CLRNN report are mindful of the necessary interaction and overlap between offences and defences within these (and other) offence regimes.

1.5 PROBLEMS OF ENFORCEMENT AND DATA

1.5.1 This CLRNN report focuses on recommended changes to the substantive criminal law, alongside guidance to prosecutors and sentencing courts. However, it is useful to set these recommendations in a context of under enforcement and problematic data. This context is important because it highlights the absurdity of current overly-broad legal regulations, deterring legitimate research and cybercrime defence whilst failing to hold criminals to account. Commenting in 2019, cybersecurity press highlight the 'the lack of prosecution tools available continues to mean a low risk for criminals and shortage of justice for their victims'; and similar cyber blogs that 'Cybercrime has become accepted as a low-risk, potentially high-reward activity for organised criminals. If they act professionally, they can make substantial sums of money with very little chance of being caught.'

1.5.2 A context of under enforcement is also important in highlighting potential future dangers. For example, we see all political parties united in promises to increase the policing and prosecution of cybercrime, and yet if the legal regulation is not reformed to narrow upon appropriate targets, increased enforcement will be inefficient (ie, taking time to discern legitimate targets in the public interest) and/or potentially over-criminalising in its effects.

1.5.3 Every stage of the enforcement process requires attention:

Stages of Enforcement	**Problem Recognition**
Reporting: More concerns have been voiced about the current crime reporting regime than any other aspect. We summarise a typical experience of the Action Fraud/NFIB reporting process: 1. A member of the public or a business believes that they have been the victim of a cybercrime attack and contacts the police; 2. Police tell the victim that the victim's experience of cybercrime is a potential fraud or a civil matter and that they can't help;	Which? 'Some crime reports made by scam victims are never being read by actual police staff.' The Register 'Action Fraud is only passing 2% of cases to cops.' 'The Register 'Only a small proportion of reports made to Action Fraud are ever looked at by real police workers' Graham Cluley 'If the [ONS] figures are correct, only 2% of computer misuse crimes are passed on to the actual police who could investigate them.' '[Action Fraud] staff tricked victims into thinking their cases will be investigated when most are never looked at again.... Action Fraud helpline is largely for show. That opinion is

3. Police tell the victim that they need to contact Action Fraud to report their cybercrime offence; 4. Victim submits details to Action Fraud by phone or website; 5. Action Fraud reports are assessed by artificial intelligence algorithms to filter out reports that may be relevant to ongoing fraud investigations for further investigation and/or for intelligence. It is not clear whether *any* non-fraud cybercrime offences are referred for investigation. Victim support is not provided; 6. When prompted by the victim, Action Fraud tells the victim that their report has been reviewed and that the police have decided there is insufficient evidence to investigate or that it is a civil matter or that the police do not have the resources to investigate	growing more popular, as proven by the creation of a parody Twitter account for Action Fraud (called, appropriately, @InactionFraudUK.)' This is Money '[Action Fraud] doesn't provide police with information they need to decide whether investigations should go ahead in order to better protect the public.' ZDNet '9,000 cybercrime reports filed by UK citizens have sat inside a police database without being investigated after security software mistakenly identified them as containing malicious code and placed them in quarantine. All the quarantined reports came from Action Fraud' Trustpilot rates Action Fraud as One Star on the basis of 94% bad ratings in 250 Reviews.
Evidential: There is no public guidance on what evidence should be secured to enable the police to investigate a particular type of offence, and how.	There appears to be no means of submitting evidential material with an Action Fraud report.
Public Investigation: Police forces are under-funded and are under-equipped to deal with the increasing range and number of cybercrime offences. As a result the police forensic investigators have permanent backlogs of work and forensic investigations take too long. CMA 1990 offences are not prioritised in forensic investigations.	The Daily Swig 'Police in the UK lack the tools to prosecute cybercriminals' RPC 'The low levels of prosecutions in this area is partly a result of police not having the resource to tackle the full extent of the problem as cybercrime has become increasingly widespread and complex.'
Prosecution: CMA 1990 is underused in cybercrime prosecutions. However CMA is regularly used to prosecute police officers and staff who have exceeded the limit of their authority to access a police computer system.	RPC 'the number of prosecutions still represents less than 1% of reported cybercrimes in the UK.' Naomi Colvin 'There aren't that many CMA prosecutions per year and if you have a look at

	who actually gets prosecuted at least a third of them tend to be police officers'

1.5.4 With regard to the statistical data, discussed further at **Appendix B**, the problems include a lack of recording and (even when recorded) a lack of standardisation. Our review of the available sources of statistics has led us to the conclusion that It is largely impossible to cross-reference and reconcile the various sources due to the lack of agreement of terms between them.[50] As Mike Fenton, CEO of Redscan, has recently commented: 'The fact that the statistics include just 20,000 offences reported against businesses to the National Fraud Intelligence Bureau by Action Fraud shows that the data is deeply flawed. Until the reporting of computer misuse crime improves, data like this should be taken with a large pinch of salt.' A lack of reliable data causes problems for all reform and enforcement agencies.

1.5.5 What is needed is agreement between all the relevant parties to standardise the definition of terms parties use throughout the life-cycle of a CMA 1990 incident, so that each individual reported incident can be tracked through the reporting system, intelligence system, triage, police investigation(s), charging decision, court records, trial and sentencing using shared references for cross-reference, intelligence-gathering and statistical analysis.

1.6 SUMMARY

1.6.1 This CLRNN report joins a variety of commentators calling for reform of cyber regulations in general, and the CMA 1990 in particular. These include reviews at European and national level, including within the UK's National Crime Agency, and campaigns for reform from those within the cyber security industry. It comes at a time when a general political re-think is taking place about the legal environment required to improve law enforcement capabilities to tackle serious and organised crime, and to enable public and private sectors to work in partnership to protect the British public, economy and critical infrastructure from harm by cyber criminals and hostile nation states.

1.6.2 As it stands, the Computer Misuse Act 1990 is not fit for purpose to tackle current policing and national security challenges. The piecemeal amendment of the legislation over the last 30 years has led to a regime with significant anomalies. International

[50] For example, there is no way to easily extract the name of a defendant from the case details recorded in the CMA ToC and compare it with the relevant court records or to check that the same prosecution is included in a MoJ Outcome subtotal for a particular period. As a result, all the sources of statistics lack credibility.

comparisons show that offences in the CMA 1990 are significantly broader and less specific than within comparator jurisdictions, and out of line with international treaty commitments. The CMA 1990 also contains no specific defences to any of the offences; surprising because statutory defences exist in respect of a number of offences that are similar in rationale and even substantively overlapping. While the Crown Prosecution Service undertakes a public interest test ahead of decisions to prosecute, current guidance on computer misuse offence is severely limited; and guidance to courts at sentencing is entirely absent.

1.6.3 Problems with the current law particularly affect those whose ethically motivated computer-related investigations and activities seek to improve cyber security, such as non-law enforcement investigators, penetration testers and academic and commercial security and threat intelligence researchers.

1.6.4 The only way to remedy the obvious and fundamental deficiencies present in the CMA 1990 is through primary legislative reform of core offences (and the creation of new defences); combined with bespoke guidance for prosecutors and sentencing courts. Across the chapters that follow, this report makes several recommendations on the reforms that are needed to create a legislative regime that is fit for purpose – allowing ethically motivated cyber defenders, security researchers and journalists to pursue their work with greater legal certainty, while improving the ability of the state to identify, prosecute and punish those acting against the public interest.

CHAPTER 2

OFFENCES

2.1. INTRODUCTION

2.1.1 Nowadays the phenomenon of hacking is well-known,[51] and one of the great challenges of cybercrime law is timely adaptation to the myriad ways in which hackers operate. The aim of this chapter is to consider the extent to which the offences in the CMA 1990 are adequate in light of the increased sophistication of cybercriminals and the methods they employ to access or disrupt computers and computer systems.

2.1.2 After outlining the CMA offences, we will consider the UK's international commitments under the Council of Europe Convention on Cybercrime and the Directive 2013/40/EU. The comparison with international law and other national laws will provide a valuable perspective on the UK's legislative choices, pointing towards areas of reform. We will conclude with a summary of recommendations.

2.2 CURRENT OFFENCES IN ENGLAND AND WALES

2.2.1 The CMA 1990 initially criminalised two types of conduct: (i) the unauthorised accessing of computer material, either in a simple form (section 1) or in an aggravated form (section 2), and (ii) the unauthorised modification of computer material (section 3).

[51] See Yar, *Cybercrime and Society* (2nd, edn, Sage Publications, 2013), Ch 2.

Unauthorised Access Offences

2.2.2 Section 1 is an either-way offence that carries a maximum sentence on indictment of 2 years' imprisonment. The elements of the offence are:

(a) A person causes a computer to perform any function with intent to secure access to any programme or data held in any computer, or to enable any such access to be secured;
(b) The access that person intends to secure, or to enable to be secured, is unauthorised;
(c) That person knows at the time when he causes the computer to perform the function that that is the case.

2.2.3 Within England and Wales, the defendant must act with intent to secure access to any programme or data held in any computer, or in Scotland only since 2006, the intention to enable any such access to be secured. As per section 1(2), intention needs not be directed at any particular program or data, a program or data of any particular kind or a program or data held in any particular computer.

2.2.4 Section 17(2) CMA describes 'access' by reference to alterations or erasure, copying, or moving data (uploading, downloading), using it or producing output, such as displaying on a screen or printing it.[52] There is certainly merit in maintaining unauthorised access as a separate offence from that of data and system interference. In the UK, section 1, combined with section 17(2)(b), does not necessarily constitute data interference (section 3 CMA). For example, when the original file being copied remains intact, because the copying is unlikely to hinder the functioning of a computer or alter the reliability of the data.[53] The CMA definition of 'access' can be understood as the actions revealing that the access has been obtained, and that intrusion occurred. In addition, mere access can at times simultaneously damage the information system. However, the fact that 'mere' access is sufficient, without the requirement of associated harms, makes the section 1 offence particularly broad.

2.2.5 The offence in section 2 is also an either-way offence that carries a maximum sentence on indictment of 5 years' imprisonment. A person is guilty of the section 2 offence if he commits an offence under section 1 with intent (a) to commit an offence to which

[52] See Walden, *Computer Crimes and Digital Investigations* (OUP, 2015), para 3.262. To the best of our knowledge, how the offence potentially overlaps with the offences of system and data interference under section 3 CMA, and why this definition has been adopted, have not been articulated.
[53] With the assumption that the copying aims at preserving the data, and thus does not affect its reliability.

section 2 applies, or (b) to facilitate the commission of such an offence (whether by himself or by any other person).

2.2.6 The offences to which section 2 applies are (a) those offences for which the sentence is fixed by law (so, for example, murder) or (b) those offences for which a person of 21 years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years.[54]

2.2.7 For the purposes of section 2, it is immaterial whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion,[55] and a person may be guilty of the section 2 offence even though the facts are such that the commission of the further offence is impossible.[56]

Unauthorised Act Offences

2.2.8 The offence in section 3 is an either-way offence that carries a maximum sentence on indictment of 10 years' imprisonment. The conduct element of the section 3(1) offence occurs if a person does any unauthorised act (or series of acts) in relation to a computer (and for these purposes the doing of an act includes a reference to causing an act to be done) and at the time when the person does the act he knows that it is unauthorised.

2.2.9 The mental element of the offence occurs if the person either intends to, or is reckless as to whether the act will, either permanently or temporarily (a) impair the operation of any computer, (b) prevent or hinder access to any program or data held in any computer, or (c) impair the operation of any such program or the reliability of any such data. In addition, for Scotland, but not for England, Wales and Northern Ireland, the mental element includes (d) enable any of the things mentioned in (a) – (c) to be done.[57] The objective was to facilitate prosecution of individuals whose actions were more akin to those of accomplices than authors, as required in the Council Framework Decision of 2005. The introduction of the assisting and encouraging offences in 2007 led to the repeal of the provision for England and Wales.[58] The intention or recklessness need not relate to any particular computer, any particular program or data, or a program or data of any particular kind.

[54] Section 2(2).
[55] Section 2(3).
[56] Section 2(4).
[57] Introduced by the Police and Justice Act 2006, the provision has been repealed in 2008 by the Serious Crime Act 2007 for England and Wales only.
[58] Explanatory Notes to s.61 of the Serious Crime Act 2007, para 225.

2.2.10 The offence in section 3ZA is indictable-only and carries a maximum sentence of 14 years' imprisonment, save where it is committed as a result of an act causing or creating a significant risk of (a) serious damage to human welfare (loss of life or human illness of injury), or (b) serious damage to national security, in which the case maximum sentence is life imprisonment. A person is guilty of an offence under section 3ZA(1) if:

(a) He does any unauthorised act or series of acts, or causes an act to be done, in relation to a computer;
(b) At the time of doing the act the person knows that it is unauthorised;
(c) The act causes, or creates a significant risk of, serious damage of a material kind;
(d) He intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.

2.2.11 Subsections (2) and (3) further define what constitutes damage of a material kind, and subsection (4) provides that it is immaterial whether or not an act causing damage does so directly or is the only or main cause of the damage.

2.2.12 In particular, damage is of a material kind if it involves damage to human welfare in any place, damage to the environment of any place, damage to the economy of any country or damage to the national security of any country. For these purposes an act causes damage to human welfare only if it causes (a) loss to human life, (b) human illness or injury, (c) disruption of a supply of money, food, water, energy or fuel, (d) disruption of a system of communication, (e) disruption of facilities for transport, or (f) disruption of services relating to health.

2.2.13 There is potential for this offence to be interpreted widely. While 'damage' is limited to attacks aimed at critical infrastructures, the conduct in section 3ZA needs only to create a significant risk. The offence can also be attempted, so attempting to create a risk is criminalised. No caselaw exists on section 3ZA so far but, during the rushed drafting of the offence, the impact of its broad scope was raised with regard to whistleblowers.[59] With section 3ZA, a leak – often today made of data held and communicated digitally, thus on computer systems – could constitute 'any act', by definition 'unauthorised', and be argued to 'create a significant risk' of serious 'damage to the national security of any country', not just that of the UK. The scope of the offence is thus dangerously broad, requiring rationalisation and/or new defences (**Chapter 3**).

[59] Taylor, 'Computer users who damage national security could face jail', (*Guardian Online,* 2014). Available at https://www.theguardian.com/law/2014/oct/23/computer-users-damage-national-security-face-jail.

Offences of supply/misuse of tools

2.2.14 Section 3A creates either-way offences, and on indictment the maximum sentence is 2 years' imprisonment. There are three offences in section 3A:

(a) It is an offence contrary to section 3A(1) if a person makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.
(b) It is an offence contrary to section 3A(2) if a person supplies of offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.
(c) It is an offence under section 3A(3) if a person obtains any article, either intending to use it to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA, or with a view to its being supplied for use to commit, or to assist in the commission of, an offender under any of those sections.

An 'article' is defined as including any program, or data held in electronic form.

Territoriality

2.2.15 Sections 4-9 concern the territorial scope of (a) the offences created by the CMA 1990, (b) inchoate forms of those offences, and (c) inchoate offences related to offences under external law that correspond to the offences under sections 1-3. The Law Commission, in its Consultation Paper on the Protection of Official Data,[60] concluded that the territorial ambit of the CMA offences should be a model to reform the Official Secrets Act 1911 and provide broader jurisdiction. An individual outside the UK can commit an offence where a 'significant link' exists as defined in section 5 CMA.

2.3 INTERNATIONAL COMPARISON

2.3.1 Computer misuse offences exist in the domestic legislation of a number of countries both within the EU and outside of it, most notably for the purposes of this report: France, Italy, the Netherlands, Australia, and to a lesser extent, the United States. Sources on comparative law in cybercrime vary in terms of availability and details.

[60] Consultation No 230, 2017.

Following the UN General Assembly's Resolution 65/230 of 21 December 2010, the UN Office on Drugs and Crime published its 2013 *Comprehensive study of the problem of cybercrime*, based on Member States' surveys.[61] Clough's book, *Principles of Cybercrime*,[62] presents in detail four common law jurisdictions: the US, Australia, Canada, and the UK. The EU also released its own report in 2017,[63] and some national reports on the implementation of the Directive are also available.

2.3.2 We present below an overview of the CMA compared to the Convention on Cybercrime and the Directive 2013/40/EU. It will then analyse both international and national legislations mentioned above per offence: unauthorised access, data and system interference, misuse of tools. The following table shows the correspondence between the texts.

Convention on Cybercrime	Directive 2013/40/EU	Computer Misuse Act 1990
Article 1 - Definitions	Article 2	Section 17 on interpretation
Article 2 on illegal access	Article 3 on illegal access to information systems	Section 1 on unauthorised access to computer material Section 2
Article 3 on illegal interception	Article 6 on illegal interception	Investigatory Powers Act 2016
Article 4 on data interference	Article 5 on illegal data interference	Section 3 on unauthorised acts with intent or recklessness as to impairing the operation of a computer Section 3ZA, unauthorised acts causing or creating risk of serious damage
Article 5 on system interference	Article 4 on illegal system interference	Section 3 Section 3ZA
Article 6 on misuse of devices	Article 7 on Tools used for committing offences	Section 3A on misuse of tools

[61] More generally on the UN General Assembly Resolutions on cybercrime, see Schjølberg and Hubbard, 'Harmonising national legal approaches on cybercrime, Background paper' (International Telecommunications Union, 2005).
[62] CUP 2015.
[63] Report from the Commission to the European Parliament and the Council, *assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA* (2017) 474.

Article 11(1) Aiding or abetting Article 11(2) Attempt	Article 8(1) on incitement, aiding and abetting Article 8(2) on attempt	If not in the structure of the CMA offences: Attempt: section 1 Criminal Attempts Act 1981 Secondary liability: section 8 Accessories and Abettors Act 1861
Article 12 – Corporate liability	Article 10 on liability of legal persons	No section in the CMA Case law
Article 13 – Sanctions and measures	Article 9 on penalties, with aggravating circumstances Article 12 on sanctions against legal persons	See respective sections of the CMA

Unauthorised access offences

2.3.3 According to the United Nations Office of Drugs and Crime report (UNODC Report), eleven multilateral instruments require the criminalisation of unauthorised access to computers, among them being the Convention on Cybercrime and the Directive 2013/40/EU.

2.3.4 Article 2 of the Convention requires that 'when committed intentionally, the access to the whole or any part of a computer system without right' should be an offence. The Convention then allows a restriction to the scope of the offence in three different ways: (i) by requiring the infringement of security measures, (ii) intent to either obtain data or to commit another intentional offence, or (iii) that the computer is linked to a network and accessed through another computer. Article 11 of the Convention does not require the criminalisation of attempts to gain illegal access, but requires that there should be accessorial liability where illegal access takes place.

2.3.5 Article 3 of the Directive has a very similar offence definition: 'when committed intentionally, the access without right, to the whole or to any part of an information system'. However, the Directive, in contrast with the previous Council Framework Decision 2005, requires criminalisation only where the offence is 'committed by infringing a security measure'. Thus, an option in the Convention became a constituting element of the offence in the Directive. The Directive adds a further

restriction not present in the Convention: 'at least for cases which are not minor'. Like the Convention, Article 8 of the Directive does not require the criminalisation of attempts but requires the imposition of accessorial liability.

2.3.6 As a threshold for harmonisation, the Convention therefore requires the criminalisation of 'mere unauthorised access', while offering countries the possibility of attaching additional conditions to the base crime. The Directive places the threshold higher, criminalising unauthorised access, but with two additional elements: the infringement of a security measure and the seriousness of the conduct.

2.3.7 At national level, by 2013, 69% of countries had a specific statute to criminalise the offence of unauthorised access; 19% used their general criminal law; 5% used both; and only 7% of countries did not criminalise illegal access.[64]

2.3.8 However, this very low rate of non-criminalisation masks differences as to the elements of the offence, with the criminalisation of 'mere' unauthorised access remaining controversial at both national and international levels.[65] Often identified by analogy to 'cyber trespass', the underlying question is whether it is appropriate to resort to the criminal law to tackle what would be primarily a civil wrong in the physical world.[66] Two competing interests are balanced. On one hand, the need for criminal law 'to act as a barrier to prevent further crime', since the conduct of illegal access is often the prerequisite for committing more serious computer-contact and/or computer-enabled crimes.[67] This approach to the use of criminal law fits within the wider debates on inchoate offences and deterrence in criminal law.[68] On the other hand are questions of potential over-criminalisation, targeting non-harmful and inappropriate wrongs.

2.3.9 It is useful to keep this general conflict in mind as we explore specific elements of the CMA 1990 offences below.

[64] UNODC Report, 82.
[65] UNODC Report, 83.
[66] See, Wall, *Cybercrime*, *The Transformation of Crime in the Information Age* (Polity Press, 2007) Ch3; Walden, *Computer Crimes and Digital Investigations* (2nd edn, OUP, 2015) para 3.260, 3.272.
[67] See, Explanatory Report to the Convention on cybercrime [44]; Clough, *Principles of Cybercrime* (CUP 2015) 56; Miguel, Freitas and Gonçalves, 'Illegal access to information systems and the Directive 2013/40/EU' (2015) 29(1) *International Review of Law, Computers & Technology* 50, 55.
[68] Horder, *Asworth's Principles of Criminal Law* (9th edn, OUP 2019) Ch13.

The concept of 'access'

2.3.10 At international level, neither the Convention, nor the Directive define access. However, the Explanatory Report for the Convention defines access to 'comprise[…] the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data)'.[69] It excludes sending an email.[70] The word 'intrusion'[71] is also used for access, intrusions being characterised as the first steps in order to subsequently obtain passwords, information, or secrets, use a system without payment or commit fraud or forgery. Here, Article 2 must be read together with Articles 4 and 5 on data and system interference, which criminalise the alteration or deletion of data and the serious hindering of the functioning of a computer. In other words, access is not the alteration or deletion of data, even if the latter may be the first visible sign that access has been gained.

2.3.11 With regard to the Directive, while the Recitals do not suggest a definition, Article 3 requires access to be gained by infringing security measures. Security measures implicitly indicate a threshold, a locked door, and thus their infringement points towards intrusion. The articulation between Article 3 and Articles 5 and 6 on data and system interference confirms this reading of the law. As in the Convention, access precedes the alteration or deletion of data (Article 5), or the serious hindering of the functioning of an information system (Article 6).

2.3.12 This definition of access as intrusion, combined with the Convention's and Directive's need for 'access to the whole or any part of a computer system', implies that access not so obtained constitutes an attempt to access rather than the completed offence. For example, unsuccessfully entering a password would be an attempt under the Convention and the Directive. Consequently, switching on a computer is unlikely to be considered an attempt because of the timelag between switching it on and entering credentials, and the opportunity for an individual to desist. Switching on the computer would be a preparatory act and would fall outside the scope of criminal law under the Convention and the Directive.

2.3.13 Regarding national laws, determining the exact scope of offences can be challenging. Indeed, the completed offence can vary significantly in terms of the conducts covered, depending on the implicit understanding of what access means.

[69] Para 46.
[70] Ibid.
[71] Para 44.

2.3.14 As with the international texts, access can be analogous to 'cybertrespass',[72] to 'metaphorically […] entering a building'.[73] Attempts are thus defined by reference to what constitutes intrusion for the completed offence; and other conducts, post-intrusion, would constitute aggravating circumstances. For example, Article 615-ter of the Italian penal code criminalises 'access' and introduces aggravating circumstances where access leads to damage to the data or hindering of the functioning of a computer system.[74] Attempts at unauthorised access are criminalised as per the general rules. Similarly, article 323-1(1) of the French penal code identifies the offence as 'accessing' the whole or part of an information system.[75] Accessing is not defined but the second paragraph implicitly indicates that access means intrusion and does not incorporate deletion or alteration of data, or impairing of the functioning of the computer system. Indeed, access combined with the deletion or alteration of data, or impairing of the functioning of the computer system, brings aggravating circumstances (article 323-1(2)). Attempts are also criminalised.[76]

2.3.15 By contrast, Article 138ab of the Dutch criminal code defines their 'access' offence as 'any person who […] gains entry to a computerised device or system or a part thereof shall be guilty of a computer trespass'.[77] Aggravating factors arise when the offender 'subsequently copies the data stored, processed or transferred'. Thus, 'access' equates to 'intrusion' and 'trespass'.[78] Attempts are criminalised as per the general rules. The difference between attempting the offence and committing the offence itself may seem clear, stemming from the Dutch concept of access as intrusion. However, article 138ab indicates that access is gained, for example, by means of a false key (a password), by breaching a security measure, and 'by a technical intervention'. This could imply that access is constituted by the use of the password, even if unsuccessful. Consequently, clicking on a link to get to a log-in page would be an attempt and thus within the scope of criminal law. However, Koops, in his commentaries on the Dutch offence, interprets the law so that the use of a password

[72] Wall, 'Policing the Internet: Maintaining order and law on the cyberbeat', in Walker and Wall (eds) *The Internet, Law and Society* (Longman, 2000) 157.
[73] Clough, *Principles of Cybercrime* (CUP 2015) 68.
[74] Council of Europe, *Project on cybercrime, Country Profile* (2008) 1-2; a 2013 reform has not modified the definition of the offence.
[75] Access is used as a verb in the French original: 'le fait d'accéder'.
[76] In article 323-7 of the French penal code. Article 121-4 French penal code requires for a 'délit' (roughly a triable either way offence) that a statute specifies the criminalisation of attempting the offence. Attempts to summary only offences are prohibited. Attempts to indictable only offences are possible by virtue of article 121-4 penal code, without the need for specific legislation.
[77] Article 138ab, para 1, Dutch Criminal Code, in Council of the European Union, *Evaluation report on the seventh round of mutual evaluations, 'The practical implementation and operation of European policies on prevention and combating Cybercrime'- Report on the Netherlands* (2015) 93.
[78] Brazil also chose to refer to 'trespass'.

has to lead to the user successfully logging on the computer to complete the crime.[79] Unsuccessful use would then be an attempt and not the full offence. Accordingly, switching the computer on or clicking on a link to get to the log-in page would then be a preparatory act and outside the scope of criminal law.

2.3.16 The US federal law criminalises mere unauthorised access only to government computers.[80] For all other offences of unauthorised access, a certain threshold needs to be met, for example: an existing further intent (akin to section 2 CMA), a minimum value of use, or an additional conduct needs to occur, such as obtaining data. The meaning of access in the federal criminal code has been discussed in civil courts; and before state courts, as part of state legislation on computer misuse.[81] Reviewing the case law, Kerr interprets access as 'any successful interaction with the computer' rather than as a successful intrusion, because people interact with computers in 'myriads [of] ways', challenging the 'trespass paradigm'.[82] This would mean that using a password, even if unsuccessful, would constitute the main offence, rather than an attempt. Similarly, for an individual to scan an information system – as both security and threat researchers and criminals do to find vulnerabilities - is to communicate with the system, and could be considered as access, not an attempt to access.[83] Which interpretation of access (Kerr's or intrusion) prevails is unclear, although the most plausible is that of Kerr.[84] In any case, given that the US offences incorporate additional conduct such as obtaining information to describe the completed offence, access without these conducts would remain an attempt.[85]

2.3.17 According to the UNODC Report, this requirement of further intent or conduct for the completed offence of unauthorised access has been adopted by a number of countries in order to restrict the scope of their criminal law.[86] An attempt to commit these offences criminalises mere access; any conduct not constituting an attempt would then be a preparatory act, instead of an attempt at the completed offence when the completed offence is mere access.

---

[79] Koops, 'Privacy-related crimes in Dutch law', *TILT law & Technology Working Paper Series* (2017) 12; 'Cybercrime Legislation in the Netherlands' (2010) in van Erp & van Vliet (eds), *Netherlands Reports to the Eighteenth International Congress of Comparative Law* (2010, Intersentia) 595.
[80] 18 USC 1030(a)(3).
[81] Kerr, 'Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes.' (2003) 78 *New York University Law Review* 1596, 1598.
[82] Ibid. 1646-1647
[83] Ibid.
[84] Ibid, 1646-1647. By reference to *US v Morris*, the first case dealing with the spread of malicious software. See also Clough, *Principles of Cybercrime* (CUP 2015) 79.
[85] Clough, *Principles of Cybercrime* (CUP 2015) 79.
[86] UNODC Report, 84.

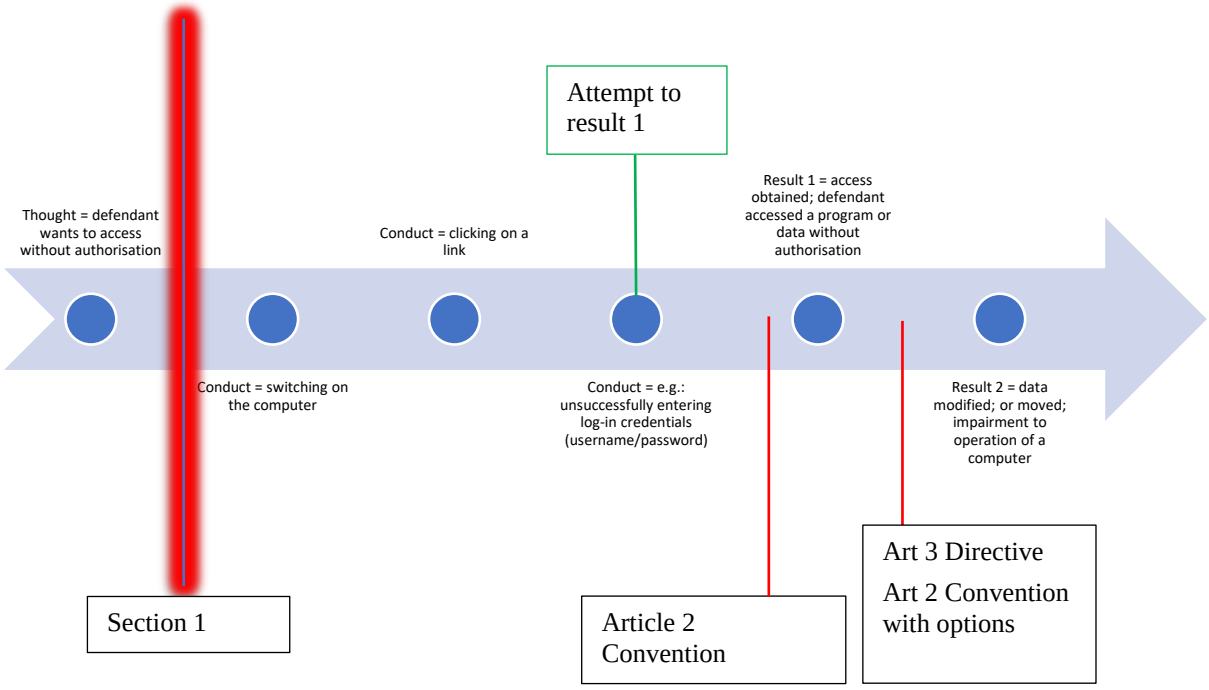
2.3.18 How the definition of access influences the difference between the completed offence, an attempt and a preparatory act, can also be seen in the Australian Legislation. 'Access' is defined as the 'display of the data or any other output', 'the copying or moving of the data', or 'the execution of the program', but the completed offence is not to obtain access: it is 'to cause unauthorised access', where 'the person's conduct substantially contributes to it'.[87] Thus, conduct does not have to be successful in obtaining access; data does not have to be moved, copied, printed, deleted or altered for the offence to be committed. Similarly, unsuccessfully entering a password will constitute the completed offence.[88] Far from being restricted by the incorporation of damage to data, the scope of the offence is significantly broadened (though still short of section 1 CMA 1990).

The concept of 'access': comparative analysis of the UK

2.3.19 Whereas the law in France, the Netherlands and Italy considers deletion of data as an aggravating circumstance to mere access, understood as intrusion, section 17 CMA defines access without such qualifications. The defendant only needs to 'cause a computer to perform any function' with intent to secure access. To apply the Australian wording, he does not even have 'to contribute substantially' to obtaining access. The UK definition stretches the concept of access to breaking. For example, the simple fact of clicking on a link, or switching the computer on, without even trying to enter a password, are conducts falling within the scope of the UK offence.[89]

2.3.20 In theory, the UK offence may be even broader than described. Since the 2006 reform has increased the penalty to two years, section 1 CMA ceases to be summary only and thus can be, in theory at least, attempted as per section 1 of the Criminal Attempts Act 1981. In practice, it is difficult to see what additional behaviours could be covered.[90] Based on the concept of access as intrusion, the following figure presents the diversity of conducts and results along the criminal pathway from thoughts of committing the offence to having obtained access and beyond. Two small red lines indicate the respective positions of Article 2 Convention (without the options), and Article 3 Directive and Article 2 Convention with the options, on the criminal pathway. The other red line relates to section 1 CMA.

[87] Section 476.2(3), added by the Cybercrime Act 2001. See Clough, *Principles of Cybercrime* (CUP 2015) 69.
[88] Ibid, 70.
[89] For clicking on a link: *Ellis v. DPP* [2001] EWHC Admin 362. And more generally, Ormerod and Laird, *Smith & Hogan's Criminal Law* (15th edn, OUP 2019) 1184; Walden, *Computer Crimes and Digital Investigations* (2nd edn, OUP, 2015) para 3.261; Clough, *Principles of Cybercrime* (CUP 2015) 58.
[90] Ibid, Walden, para 3.268.



2.3.21 The positive side of the breadth of section 1 is that we avoid the task of differentiating between the completed offence, an attempt and a preparatory act. This was a conscious choice of the Law Commission in its report of 1989.[91] But is such breadth is justifiable, especially when the penalty now reaches 2 years' imprisonment on indictment?[92] We are concerned that the offence is too broad (ie, overly inclusive), especially given the absence of defences (discussed in **Chapter 3**).

The concept of 'authorisation'

2.3.22 In their definition of the offence, the Convention and the Directive refer to access 'without right', rather than access being 'unauthorised'. However, this terminology is rarely used in legislation. Article 323-1 of the French penal code uses 'fraudulently', which in practice equates to 'unauthorised'. Article 615-ter of the Italian penal code refers to 'abusivamente' which can translate into 'abusively' or illegally/unauthorised, for a system 'protected by security measures', but without requiring their infringement. Article 138ab Dutch criminal code refers to 'unlawfully', and as an example of unauthorised access cites the infringement of a security measure. The US, the UK and Australia refer to 'unauthorised'. 'Without right' thereby expresses the nature of authorisation. System owners or controllers[93] determine the nature and

[91] Law Commission, *Computer Misuse*, (Law Com No 186, 1989), para 3.20.
[92] Contra. Giving the example of a defendant spreading a virus, Gillepsie concludes s1 CMA as an unproblematic inchoate offence, in *Cybercrime. Key issues and debates* (OUP 2016) 66
[93] The right to control may not correspond to legal ownership.

level of authorisation ranging from obtaining access to the use of resources accessed.[94] In other words, they grant rights to users to access and maintain themselves in the information system. This is what the Convention and the Directive tried to express through the concept of 'without right', as well as some national legislations when they define the term 'unauthorised'.

2.3.23 The Convention does not define 'without right', but the Explanatory Report provides more detail. The concept is described as reflecting 'the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. [...] The Convention, therefore, leaves unaffected conducts undertaken pursuant to lawful government authority' as well as for example 'legitimate and common activities inherent in the design of networks'.[95] With regard to Article 2, the Report states that 'there is no criminalization of the access authorized by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned)'.[96] It then adds that 'free and open access by the public' means that 'the access is 'with right''.[97]

2.3.24 Article 2(d) of the Directive defines 'without right' as 'conduct referred to in this Directive […] which is not authorised by the owner or by another right holder of the system […], or not permitted under national law'. It is meant to exclude law enforcement activities. Echoing the Explanatory Report to the Convention as to what authorised access is, it should be interpreted in conjunction with Recital 17: 'mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system' should not bring criminal liability. In addition, 'contractual obligations or agreements to restrict access […] should not incur criminal liability where the access under such circumstances would be deemed unauthorized and thus would constitute the sole basis for criminal proceedings'. To guard against this, Article 3 requires the infringement of a security measure for the offence to be committed.

2.3.25 Some national legislations do not define the terms they use for 'unauthorised', including France, Italy, the Netherlands, and the US.[98] Others do. For Australia, 'unauthorised' is when the person is not entitled to cause access.[99] Section 17(5) CMA

[94] Walden, *Computer Crimes and Digital Investigations* (2nd ed, OUP, 2015) para 3.236; Clough, *Principles of Cybercrime* (CUP 2015) 91.
[95] Para 38.
[96] Para 47.
[97] Ibid.
[98] Clough, *Principles of Cybercrime* (CUP 2015) 80-81.
[99] Criminal Code, s476(2).

defines by reference to a person 'not entitled to control access' or not having 'consent to access'. These notions of 'entitlement' and 'consent' indicate the starting point of the discussion, and echo the definition the Directive gives of 'without right'. Thus, behind the diversity in terminology, it could be stated that 'the essential concept is the same in each jurisdiction'.[100] Yet, difficulties in determining *precisely* what 'unauthorised' or 'without right' mean endure, even when definitions exist. The Convention and the Directive point to a number of grey areas in interpretation: security and threat intelligence research (the testing of information systems), contract law as a basis or not for criminal liability, and whether the lack of security measure(s) constitutes free and open access. There is also the issue of whether exceeding one's authorisation constitutes unauthorised access.

2.3.26 The concept of 'unauthorised' assumes that the decisions taken on authorisation can be identified and are adequately conveyed so that access can be objectively understood as 'unauthorised'. Problems arise when what the controller intends not to authorise does not match what the controller puts in place to restrict access and/or differs from what the user and the defendant perceive the lack of authorisation to be. In this sense, the concept of 'unauthorised' access spills into the issue of the defendant's knowledge of lack of authorisation. Section 1 CMA expressly distinguishes between the two: lack of authorisation (section 1(1)(b)) and the defendant's knowledge of it (section 1(1)(c)). In most legal systems, and in the international texts, the distinction is not clear,[101] perhaps because the two are so intertwined that the distinction at times seems artificial.[102]

2.3.27 A system owner or controller can restrict authorisation, partially or totally, by code, by contract or policy, or both.

2.3.28 The issue of authorisation by contract raises a more general question of whether a controller's privately defined policy can or should shape users' criminal liability. It has been prominent in the US, in particular with the case of *US v Drew*.[103] The defendant established a fake profile on MySpace to communicate with a child, a classmate of her daughter. The result, because of the more general context of bullying, led to the victim committing suicide. The argument for prosecuting under the US version of section 1

[100] Clough, *Principles of Cybercrime* (CUP 2015) 80.
[101] The Explanatory Report on the Convention is silent. Recital 17 Directive mentions the lack of liability when a person 'does not know that access was unauthorised'.
[102] For example, in the discussion on authorisation, Walden, *Computer Crimes and Digital Investigations* (OUP, 2015) raises the question of the defendant's knowledge at para 3.238, 3.243 (through the issue of a defence), 3.246 (public's perception), 3.259. Similarly, Clough, *Principles of Cybercrime* (CUP 2015) 85-86, 90-91, 93, 95. Whereas both have separate sections on the defendant's knowledge part of an offence.
[103] *US v Drew* 259 FRD 449 at 459 (CD Cal. 2009), see Clough, *Principles of Cybercrime* (CUP 2015) 79.

CMA[104] was that the defendant's actions were a clear breach of MySpace's terms of service. On appeal from her conviction, the Court struck down the verdict out of concern of the clarity of the terms of service, and what ordinary users of the site would understand to be criminal.[105] Users routinely do not read the terms and conditions of service and are in practice unaware of what they are not authorised to do and the potential impact on their criminal liability.

2.3.29 In the UK, the definition of authorisation in section 17(5) CMA is broad enough to incorporate contract law as the basis for committing the section 1 offence. It is likely though that the courts will undertake an objective assessment and pay particular attention to the controllers' policy or contract.[106] The *Drew* scenario has not arisen in the UK. However, the question of whether the controller's own policy can shape criminal liability was put to the courts of England and Wales in a different context, that of employment. It is now settled that 'unauthorised' includes exceeding one's authorisation granted by the system owner.[107] For example, the authority to read documents may not extend to that of copying them, of sharing them with others or with others for different purposes.

2.3.30 The breadth of the concept of 'unauthorised' in many European jurisdictions raised concerns at EU level during the discussions on the draft Directive. It was argued that employees who used their employers' computers for 'private purposes', for example to consult their private mailboxes, were thus in breach of their contract, and having exceeded their employer's authorisation, could face criminal prosecution for unauthorised access. It led the EU Parliament to successfully propose Recital 17 to the Directive and the requirement for security measures to be infringed, as an attempt to restrict the source of the lack of authorisation to code and contract, or code alone, rather than contract alone.[108] The UK courts should take this interpretation into account when considering whether exceeding an authorisation constitutes a lack of authorisation.

2.3.31 Regulation by code, another form of authorisation, involves creating a technologically-enabled security measure(s), for example, a log-in page requiring inputting a username and password, or other means so that access is restricted or denied. Circumventing these measures undoubtedly indicates unauthorised access.[109] The

[104] 18 USC ss 1030(a)(2)(C) and 1030(b)(b(2)(A).
[105] The US doctrine was 'void-for-vagueness', see Walden, *Computer Crimes and Digital Investigations* (OUP, 2015) para 2.236; Clough, *Principles of Cybercrime* (CUP 2015) 85-86.
[106] Walden, *Computer Crimes and Digital Investigations* (OUP, 2015) paras 3.2.37-3.2.38.
[107] *DPP v Bignell* (1997) [1998] 1 Cr.App.R 1; *Bow Street Metropolitan Stipendiary Magistrate, Ex parte Government of the USA 1999* [2000] 2 AC 216.
[108] Walden, *Computer Crimes and Digital Investigations* (OUP, 2015) para 3.242.
[109] Clough, *Principles of Cybercrime* (CUP 2015) 84.

Convention made it an *option* to require infringement of security measures for unauthorised access. In contrast, the Directive has *required* Member States to incorporate such wording as part of the main offence. At national level, infringement is rarely an explicit part of the offence. 70% of countries surveyed by UNODC, including the UK, Italy, the Netherlands since 2006, do not require the infringement of a security measure.[110] In the US, Kerr recommended that access should be limited to that of 'breach of a code-based restriction', a requirement that recalls Article 3 of the Directive. However, the US courts do not seem to have adopted this interpretation.[111] For European countries, the absence of the requirement will constitute a violation of the Directive, unless the courts incorporate the requirement within their definition of 'authorisation'.

2.3.32 The Directive requirement has been criticised, though, for being overly restrictive and ignoring the value of criminalising unauthorised access in the absence of effective security measures.[112] Vulnerabilities in information systems are common and many are listed in openly accessible lists for the purpose of helping controllers in finding them and fixing them.[113] Some are easy to find, by conducting a simple search for information with a standard search engine. Others require more specialised knowledge, although again difficulties in uncovering them can vary tremendously, from the sophisticated attack to the standard SQL injection performed by low-skilled hackers.[114] From the system owner's point of view, access was never intended to be open, but is it nevertheless unauthorised? Put differently, the presence of security measures clearly conveys lack of authorisation, but their absence or failure to work properly may not indicate the controllers' willingness to open access to their information systems. The question then is how to interpret the controllers' intention regarding authorisation, or lack of, when regulation by code fails.

2.3.33 The question is particularly difficult in the hardly regulated area of security and threat intelligence research. A number of companies and public authorities publish vulnerability disclosure policies to encourage security and threat intelligence researchers to discover and report code failures. By the policy, they generally authorise unknown security and threat researchers to access their information systems upon certain conditions in terms of conducts undertaken for finding the code failure(s) and for disclosing their findings to the controllers. The problem is that the

[110] UNODC Report, 84; see also Walden, *Computer Crimes and Digital Investigations* (OUP, 2015) para 3.242.
[111] Clough, *Principles of Cybercrime* (CUP 2015) 79, citing *US v Drew* 259 FRD 449 at 459 (CD Cal. 2009).
[112] Freitas and Gonçalves, 'Illegal access to information systems and the Directive 2013/40/EU' (2015) 29(1) *International Review of Law, Computers & Technology* 50.
[113] Guinchard, 'Transforming the Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime' (2018) 2(2) *Journal of Information Rights, Policy and Practice* 1, 3-5.
[114] Ibid, 11-14; Maurushat, *Disclosure of Security Vulnerabilities: Legal and Ethical Issues* (Springer 2013) Ch4.

quality of vulnerability disclosure policies varies. Some are relatively detailed, in addition to urging security and threat researchers to stop and report in case of doubt as to the authorisation.[115] Others are vague enough to give the impression that security and threat researchers can penetrate deep in the information system and access confidential (not necessarily private) information as long as there is no damage to data and/or violations of privacy.[116] To determine whether or not the system owner authorised access may be influenced by a number of interrelated factors: the concept of 'access' (intrusion or communication), the ease of access and the extent to which security measures are lacking, the defendants' background and related knowledge of the lack of authorisation, as well as their potential relationship with the controllers who may or may not have published vulnerability disclosure policies.

2.3.34 The Explanatory Report of the Convention links 'authorisation' or 'without right', and justification. It states that 'without right' 'reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The difficulty here is that the definition of 'authorisation', essential to determine whether an offence has or not been committed, is partially confused with the mechanism of a defence. The answer may thus not be about providing a definition and guidance to interpreting 'authorisation', but about accepting that a defence should be granted in specific circumstances such as security and threat intelligence research, and we discuss this in **Chapter 3**.

2.3.35 To summarise, compared with the two international texts and the national legislations above, section 1 CMA 1990 has the broadest scope, well beyond the criminalisation requirements of the Convention and the Directive.

Unauthorised act – the offence(s) of data and system interference

2.3.36 Like most international instruments,[117] the Convention on Cybercrime and the Directive 2013/40/EU include two offences of illegal interference: Article 4 of the Convention and Article 5 of the Directive define interference with computer data, and

[115] For example, US Department of Defense, *Vulnerability disclosure policy* (Online at https://hackerone.com/deptofdefense). Discussed by reputable security expert, Krebs, 'DoD Opens .Mil to Legal Hacking, Within Limits' (2016, Online at https://krebsonsecurity.com/tag/department-of-defense/).
[116] Discussed in Guinchard, 'Transforming the Computer Misuse Act 1990 to support vulnerability research. Proposal for a defence to hacking as a strategy in the fight against cybercrime' (2018) *Journal of Information Rights, Policy and Practice* 1.
[117] UNODC Report, 89.

Article 5 of the Convention and Article 4 of the Directive define interference with a computer system. The objectives were to cover both damage to data and denial of service attacks (DDoS) which, by overloading computer systems with communication requests, prevent or impair the functioning of a system.

2.3.37 In both texts, the offence to protect data requires the 'deleting, damaging, deteriorating, altering or suppressing computer data on an information system,' with the Directive containing the more general requirement of 'rendering such data inaccessible'. The result must be intended, and completed 'without right', which has the same meaning as for the offence of illegal access. The Directive raises the threshold for minimum criminalisation to 'at least for cases which are not minor', whereas the Convention makes it an option for Member States to restrict the offence to 'serious harm'.

2.3.38 The two texts also require States to criminalise, when done 'without right', 'seriously hindering of the functioning' of a computer system intentionally 'by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data'. The Directive adds: to the result, that of 'interrupting the functioning'; and to the means to achieve the result, that of 'rendering such data inaccessible'. As for interference with data, the Directive requires criminalisation 'at least for cases which are not minor'. The Convention does not offer an option in this respect, an approach probably more coherent than that of the Directive, given that the inference must be 'serious' in both texts.

2.3.39 Attempting both sets of offences is criminalised, although the Convention offers Member States the option not to do so.

2.3.40 At national level, over 90% of countries surveyed by UNODC in 2013 confirmed they criminalise illegal interference with a computer system or computer data, with 7% criminalising the offences both specifically and by the use of traditional criminal law offences.[118] 30% of countries regroup the two offences into one, some of them criminalising data interference only when it affects the functioning of a computer system. The law in France, Italy, the Netherlands, Australia, and the US criminalises the offences separately,[119] whereas the UK criminalises both in section 3 CMA and also, since 2015, for serious damage against critical infrastructures in section 3ZA CMA.

[118] UNODC Report, 89.

[119] For computer system, France: article 323-2 CP; Italy: art. 635quater CP; Netherlands: s138b and s350a; Australia: s477.1(1)(a)(ii0) and (477.3(1); the US: 18 USC 1030(a)(3). For interference with data, France: article 323-3 CP; Italy: art.635bis CP; Netherlands: s350a, 350b and 350c; the US: 18 USC 1030(a)(5).

2.3.41 The description of results within offences vary, more so for interference with data than with regard to interference with a computer system.[120] Emphasis is put on damaging/deleting and altering/modifying data, with suppressing, inputting and transmitting data less present in national legislations. However, it could be hypothesised that damaging and altering are common terms sufficient to cover the other results.

2.3.42 Some countries use additional terms not included in the international texts. For example, article 323-3 of the French penal code references 'to extract, to detain, to reproduce', as well as 'to transmit, delete or modify' as in the international texts. Compared with the UK offences, the French definition could refer to what the UK covers in section 1 CMA on illegal access as defined in section 17(5) CMA. However, French scholars consider that copying would not be covered without the modifying or deleting of data.[121] Caselaw has not yet clarified this aspect.

2.3.43 Section 3 CMA, before the 2006 reform, referred to a 'modification' with intent to impair the functioning of a computer. The problem is that DDoS attacks overloading the networks (but not the target computer) do not strictly speaking modify a network, but rather impair its access and use by overloading the system with requests for communication. To avoid any doubt of interpretation, the reference to modification was dropped in 2006 and replaced by 'any act'.[122] This leaves no doubt with regard to the criminalisation of DDoS attacks, but it also had the effect of further broadening the scope of the offence. The scope has also been broadened by the shift from 'the contents of the computer' to 'in relation to' a computer.

2.3.44 Lack of authorisation has the same meaning here as it did for the offence of illegal access. The meaning of authorisation has proved less difficult however. For example, the abuse of the right to send emails to flood a system and impair its functioning has been accepted relatively easily as demonstrating a lack of authorisation because the authorisation to send emails implies fair use, not the flooding of a system and its subsequent impairment.[123]

2.3.45 Most offences require the defendant to have intended the harmful results of his actions. However, the law in the UK (both section 3 and 3ZA CMA), the Netherlands, Australia, and the US also allows for broader states of recklessness or negligence.[124]

---

[120] UNODC Report, 90-91.
[121] Encyclopédie Dalloz, v° *Cybercriminalité*, para 33.
[122] *DPP v Lennon* [2006] EWHC 1201 (Admin).
[123] In the UK, *DPP v Lennon* [2006] EWHC 1201 (Admin); in France, TGI Nanterre, 8 juin 2006, Juritel n° MDN866TGI; TGI Paris, 24 mai 2002.
[124] For Australia and the US, see Clough, *Principles of Cybercrime* (CUP 2015) 113-114, 116-117. The Netherlands use the word 'negligence' but it is unclear whether its meaning matches the UK concept of

The position in the Netherlands, however, links 'negligence' to the commission of 'serious damage' (Article 350b penal code). France partially criminalises negligence (below recklessness), but as an aggravating circumstance to illegal access (article 323-1 al. 2 CP).[125] The choice of mental element for section 3 and 3ZA CMA renders the UK offences significantly broader in scope than those of the other countries criminalising recklessness. Attempts in national laws require intention. In contrast, the UK, by not requiring a result and criminalising attempt as an independent offence, criminalises in practice attempts with recklessness, not intention. Recklessness was introduced to mirror offences in the Criminal Damage Act 1971, but in that context damage, not merely a risk of damage, is required; whereas with the extension of section 3ZA to recklessness in creating a significant risk, the risk does not need to be realised.

2.3.46 To summarise, as for illegal access, the UK offences of section 3 and 3ZA CMA are significantly broader than other national laws and compared with the Convention's and Directive's requirements. This applies both to the conduct (no result; preparatory acts criminalised) and mental requirements (recklessness).

Offences to supply/misuse of tools

2.3.47 Article 6 of the Convention on Cybercrime requires the criminalisation of misuse of tools and passwords, on the basis that other offences – of illegal access and of interference with data or computer systems – are less able to cover the creation and development of tools facilitating computer misuse. Article 6(3) allows Member States to criminalise only the sale, distribution and otherwise making available (eg through forums or websites) passwords as per Article 6(1)(a)(ii). Member States can nevertheless go further and criminalise the possession of either passwords or devices including programs, or both (Article 6(1)(b)). They can also criminalise the 'production, sale, procurement for use, importation, distribution or otherwise making available of' devices (Article 6(1)(a)(i). All offences are intentional and without right.

2.3.48 Regarding the criminalisation of devices, the Council of Europe was very careful in establishing a structure for the offence that would protect legitimate developers of tools and security researchers. The need for protection arises from the fact that the security industry and criminal hackers mostly use the same hacking tools, albeit with

negligence or of recklessness. According to the UNODC Report, six countries out of 83 criminalise reckless or negligent data interference (but not computer interference), 91.

[125] Encyclopédie Dalloz, v° *Cybercriminalité*, para 24.

very different motives. They also borrow from each other the creation and development of these tools, but again with very different motives.[126]

2.3.49 To avoid criminalisation of legitimate developers and users, Article 6 establishes three main restrictions. First, 'a device including a computer program' can be criminalised only if 'designed or adapted primarily for the purpose of committing any of the [computer misuse] offences'. The objective behind the use of 'primarily' was to eliminate from the scope of the offence most dual-use hacking tools.[127] Secondly, 'direct intent' to commit a computer misuse offence is required. Thirdly, the offence must 'be interpreted' so as not to 'impose criminal liability' when the conduct described in Article 6 'is not for the purpose of committing an offence … such as for the authorised testing or protection of a computer system' (Article 6(2) Convention). Article 6(2) is not a defence, and the Explanatory Report indicates that it is linked to the concept of 'without right' or lack of authorisation, and with that of intent.[128] In other words, in case of doubt, individuals working in the security industry must be presumed to be authorised and acting legitimately.

2.3.50 At EU level, the 2005 framework decision did not require the criminalisation of tools, but Article 7 of the Directive 2013/40/EU does. The structure of the offence is extremely similar to that of Article 6 of the Convention, except for the fact that it does not include devices, just programs,[129] and that there is no interpretation guidance as in Article 6(2). Nevertheless, Recital 16 indicates the same preoccupation of not criminalising security and threat intelligence researchers, the Recital insisting on the requirement of direct intent, not general intent, in that respect.

2.3.51 At national level, 67% of the countries surveyed by UNODC criminalise the offence specifically, but 21% do not criminalise it, not even through a general criminal law offence.[130] 10% use the general criminal law, as the offence is akin to the frequent criminalisation of burglary tools.[131] There is a link here between the concept of unauthorised access as intrusion/trespass and the offence of misuse of tools.

2.3.52 The structure of the offence can vary significantly, with consequences for the criminalisation of security and threat intelligence researchers in particular. 50% of

[126] Guinchard, 'Transforming the Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime' (2018) 2(2) *Journal of Information Rights, Policy and Practice* 1.
[127] Explanatory Report, para 73; Clough, *Principles of Cybercrime* (CUP 2015) 134-136.
[128] Explanatory Report, para 76.
[129] So hardware is not covered, although the interweaving between software and hardware may blur the distinction.
[130] UNODC Report, 93.
[131] UNODC Report, 92-93.

countries restrict the tools to those 'primarily designed for the commission of an offence' *and* require direct intent. However, some countries do not require both: they either restrict the tools *or* require direct intent. The UNODC does not mention the transposition (or absence of) of Article 6(2) Convention.[132]

2.3.53 Article 615 quinquies of the Italian penal code criminalises the creation and dissemination of programs designed to damage or disrupt a computer system, but not 'primarily' designed. Article 615quater criminalises detention and diffusion of passwords. Article 139d para 2 of the Dutch penal code criminalises possession and/or distribution of tools 'primarily designed or adapted' with direct intent. Article 323-3-1 of the French penal code criminalises importing, offering, giving away or making available a device, program or data 'created or specially adapted to commit one or several [computer misuse] offences', 'without a legitimate reason, notably for research or for IT security'. Thus, the law in France does not criminalise the creation and adaptation of tools unless it is combined with the tools' distribution. It also has an additional element very close to Article 6(2) of the Convention on Cybercrime, so that security researchers (academics or not) can raise what effectively works as a defence. This requirement seems to be an exception in the pattern of national criminalisation of the misuse of tools, although there is uncertainty here since the UNODC report does not mention the matter and there is a lack of wide comparative research.

2.3.54 Whatever these uncertainties, the contrast between the UK and other national legislation is clear. The UK has the widest possible scope for the offence. First, section 3A CMA does not restrict 'articles' to those designed or created to commit an offence, let alone to those 'primarily' designed or created for such a purpose. This means that even Virtual Private Network software (VPNs) and Tor, the onion router allowing for secure communications, are within the scope of the offence, so long as they are used for the commission of the offences, as in the case of *Martin*.[133] Conversely, they would automatically fall outside the scope of other national legislations because of the requirement to be designed or 'primarily' designed to commit offences.

2.3.55 Secondly, section 3A only requires 'belief that it is likely' that the tools will be used illegally, when the conduct is that of supplying or offering to supply the tool. This contrasts with the specific intent recommended in the Convention and the Directive. The main problem with this broader mental element is that all security and threat researchers *know*, rather than just believe, 'that it is likely' that criminals will use the

[132] UNODC Report, 93-95.
[133] *Martin (Lewys Stephen)* [2013] EWCA Crim 1420.

hacking tools or anonymity tools like VPNs in order to facilitate crime, so security and threat researchers will be caught within the offence.[134]

2.3.56 Thirdly, section 3A makes no mention of a legitimate reason as in article 323-3-1 of the French penal code, or something similar as in Article 6(2) Convention.

2.3.57 Fourthly, section 3A does not criminalise possession alone. Possession is only indirectly recognised as part of other conducts: making, supplying, offering to supply, and obtaining. This contrasts with other national legislations (for example, article 323-3-1 French penal code), as well as comparable UK legislation such as the Fraud Act 2006, where an overlapping offence (section 7) criminalises making and/or supplying a tool for fraud only.

2.3.58 The combined effect of these requirements is that those who supply or offer to supply dual-use hacking tools as well as VPNs and Tor, and/or who obtain them for personal use or with a view to supply to others, are caught within section 3A. This brings into the scope of the offence: security and threat intelligence researchers; whistleblowers who may obtain a VPN or Tor to secure their communications in order to leak data accessed without authorisation (section 1 CMA); and journalists who supply the same tools (for example SecureDrop) in the belief that it will be used to receive data, notably from whistleblowers (section 3A(2)).

2.3.59 The UK Government has presented the introduction of section 3A as a means to comply with the Convention on Cybercrime, and its 2015 amendment (to add the obtaining of an article for personal use) to comply with Directive 2013/40/EU. But the breadth of the current offence seems to contradict these international documents, bringing into their scope defendants (such as security and threat intelligence researchers) who were meant to be specifically excluded. While Member States can go beyond what international texts require, the assumption is usually that the spirit of the texts is respected.

2.4 REFORMING THE OFFENCES

2.4.1 Our discussion above (**2.2-2.3**) has provided a clear case for reform. We find each of the CMA 1990 offences to be inappropriately broad in their potential catchment, and nothing from our international obligations or comparative legal systems suggests that such breadth is necessary or desirable. In this section, we pick up on some of these

[134] Guinchard, 'Transforming the Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime' (2018) 2(2) *Journal of Information Rights, Policy and Practice* 1.

discussions to provide recommendations for a way forward. However, before we consider the specific offences, we begin with the definition of terms that apply across the statute.

Definitions: 'computer', 'program' and 'data'

2.4.2 Section 17(6) CMA indirectly and only partially defines 'computer', implying that a computer is more than a storage medium and that it can contain 'any program or data held in any [removable storage] medium'. The absence of any complete definition means that any number of everyday devices could potentially fall within the offence-creating provisions of the CMA. This could include electronic keypads, satellite navigation devices, mobile telephones, washing machines, coffee makers, games consoles, baby monitors, security cameras, burglary alarms, calculators, digital watches, and so on.

2.4.3 This near total absence of specific definitions reflects the Law Commission's conclusions (pre-1990). The Commission consciously refrained from proposing any definition. In 1988, it had already rejected the option of a non-exhaustive definition which would list devices as in some national legislations.[135] In 1989, it agreed with a number consultees that 'it would be unnecessary, and indeed might be foolish, to attempt to define computer' not least because any definition would probably be too complex for magistrates, juries and judges to understand.[136] Nor did the Commission detect 'any enthusiasm' for definition by partial exclusion, where the term 'computer' would be undefined but the legislation would contain a list of devices that did not qualify as computers.

2.4.4 Instead the Commission consoled itself with the thought that in view of the nature of the hacking offences 'we cannot think that there will ever be serious grounds for arguments based on the ordinary meaning of the term 'computer'.'[137]

2.4.5 When in 2004 the All Party Parliamentary Internet Group (APIG) considered the provisions of the CMA 1990, it noted the absence of any definitions for specific words that appear repeatedly in the legislation.[138] The APIG noted that during the passage of the legislation through Parliament, attempts were made to add definitions but these attempts were rebuffed. At the time the concern of Parliamentarians was that

[135] Law Commission, *Computer Misuse* (Consultation No 110, 1988) 126-127, referencing the US, California and Tasmania.
[136] Law Commission, *Computer Misuse* (Law Com No 186, 1989), para 3.39.
[137] Ibid.
[138] All Parliamentary Internet Group, *Revision of the Computer Misuse Act* (2004) 12-19.

without definitions, words such as 'computer', 'program' and 'data' would be interpreted too widely, whereas in evidence given to the Group in 2004, the concern of many consultees was that those words would be construed too narrowly to exclude, for example, mobile devices, personal digital assistants, palmtops and network devices.

2.4.6 From this the APIG concluded that the absence of definitions in the CMA was a state of affairs that was 'working perfectly adequately'. In the event, the Government did resist calls for definitions and so to this day, nearly thirty years after its enactment, the CMA contains no definition section that seeks to explain what 'computer', 'data' and 'program' mean.

2.4.7 We have concerns about such important terms not being defined because that creates uncertainty as to the scope of offences. However, we also recognise that one of the perceived strengths of the present framework is its ability to adapt to advances in modern technology, and that quality could be lost if specific definitions were inserted into the legislation that failed to keep up with those advances.

2.4.8 It is noted that both the Convention and the Directive provide some definitions. Article 1 of the Convention defines 'computer system' as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'. Article 1(a) of the Directive, which uses the expression 'information system' rather than 'computer system', adds to this definition: any 'computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance'. Both texts have the same expression and definition for 'computer data': 'any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function'.

2.4.9 The UK legal system (except Gibraltar) has not transposed those definitions. It is not the only EU Member State not to have done so. For computer/information system, 11 Member States have not adopted the definition, whereas 15 have adopted the definition of 'computer data'.[139] The EU Commission has concluded that incorporating the definitions would constitute a major improvement and have 'an effect on the scope of offences defined by national law on the basis of the Directive'.[140]

[139] EU Commission Report (2017) 6.
[140] EU Commission Report (2017) 12.

2.4.10 Outside the EU, national laws are also split into two categories: those defining 'computer', such as the US; and those leaving the term undefined, such as Canada and Australia. In Australia, the Model Criminal Code Officers Committee considered the possibility of including definitions in the computer offences that are now contained in the Criminal Code Act 1995 (Cth) and rejected that approach as well.[141] The Committee concluded that the outer-limits of cybercrime legislation could not be determined by producing complicated definitions of key components. A better approach, in their view, was to make sure that the elements of the offence were 'tight' enough to ensure that computer crime did not spread outwards so as to engulf all manner of offences committed with, or in respect of, a variety of electronic devices that could be described as computers.[142]

2.4.11 The importance of definitions may be more visible with the development of Internet of Things (IoT). Prosecutors may have to be more careful in how they frame charges and particulars. IoT devices can include children's toys and domestic machines which can be controlled over the Internet. They can also concern controls and switches used in industrial processes and for the management of such items as the electricity grid, complex manufacturing plants and the railway system.

2.4.12 Technically, IoT devices can be said to fall into two broad categories. The first consists of items such as IP cameras (cameras which connect wirelessly to the Internet or a local area network within a home or office instead of via wires); Internet connected video recorders and smart TVs; and complex Internet switches. They do not look like computers, but they carry within them embedded 'computer-like' facilities, often using a version of the open-source Linux operating system, which can respond to various commands. Such facilities make them attractive targets for certain DDoS attacks, using variances of the Mirai malware to commit what would be section 3 CMA offences.

2.4.13 The second category relate to devices which have very simple functions: either to collect a reading of the state of a machine and its activities and transmit the results back to a central hub; and/or to accept commands from the central hub, which result in a physical switch being turned on or off, or a valve being adjusted. They do not have much in the form of intelligence and are often referred to as 'endpoint devices'. As such they may not be considered as a computer. If so, the solution for a prosecutor would be to frame charges in terms of attacks on the centralised hub which controls the devices – and which will undoubtedly be a 'computer'. Nevertheless, under the Convention's definition and that of the Directive, IoT devices of both categories are

[141] MCCOC, Chapter 4: *Damage and computer offences* (2001).
[142] Clough, *Principles of Cybercrime* (CUP 2015) 61-62.

likely to fall within the very broad definition they provide, as computers just have to automatically process data, i.e. collect and transfer data.[143]

2.4.14 For this reason, **we do not believe that reform proposals are appropriate in this area**, at least at the current time. It would be a difficult task to undertake, and consensus as to the terms of any definitions would be equally difficult to achieve. Thus, given the absence of evidence of unsatisfactory decisions in the courts thus far, we consider that reform of this kind remains unnecessary.

Offences of 'unauthorised access'

2.4.15 The breadth of section 1 CMA, discussed in **2.2-2.3**, raises two sets of interrelated questions: *Should the offence be restricted to make certain conduct only actionable in tort? Should the concept of access differentiate between access as intrusion and post-intrusion conduct such as copying and deleting?* In answering both questions, we believe that changes to the law should be made.

2.4.16 In their 1989 recommendations, the Law Commission intended the offence of unauthorised access to be summary-only, not to be triable-either way, because the offence's 'main purpose is the general deterrence of hackers, without requiring proof of an intent to commit a further crime'.[144] This logic was undermined by the subsequent increase in sentencing. **We recommend that, if the sentence is to remain as it is currently (see Chapter 5), the section 1 offence should be narrowed by distinguishing between mere access and access with aggravating circumstances.**

2.4.17 Costs has been a central reason for creating (and maintaining) an access only offence. This includes costs systems' owners incur dealing with attempts to gain unauthorised access (with the inference that access was intrusion/trespass); the costs of investigation to check whether the system was compromised and how/where, the costs of remedial work to prevent further access; and the costs of restoring/repairing the system when damage has been done inadvertently.[145]

[143] Weber and Studer, 'Cybersecurity in the Internet of Things: Legal Aspects' (2016) 32(5) *Computer Law & Security Review* 715, 722.
[144] Law Commission, *Computer Misuse*, (Law Com No 186, 1989) para 3.2, 3.1.
[145] Ibid. Para 1.19-1.21, 2.14, cited in Smith & Hogan, *Criminal Law* (7th edn, OUP 1992) 715; Ormerod and Laird, *Smith & Hogan's Criminal Law* (15th edn, OUP 2019) 1104-1105; Walden, *Computer Crimes and Digital Investigations* (OUP, 2015) para 3.272.

2.4.18 Two problems exist with the costs argument. Firstly, the remedial costs exist independently of the commission of the offence. Remedial costs stem from the existence of vulnerabilities in the information system; these vulnerabilities can be discovered by criminal hackers but also by security and threat intelligence researchers who the system owner can hire to secure the system. Whichever of the two find the door to unauthorised access, the cost of remedying vulnerabilities will be borne by the system owner. This cost is not specific to the commission of the offence and can be viewed as pre-dating the commission of the offence. In other words, unauthorised access should not be justified by reference to the remedial costs. This is a civil matter.

2.4.19 Furthermore, the costs of repairing the system because of damage created by access is a cost to be associated with data inference – section 3 CMA - rather than with illegal access per se.[146] To consider the costs of repairing seems logical if access is the alteration or deletion of data; but is it then logical to define the base offence of illegal access by damage to data, without making the difference between attempts to access the system without damage and attempts (successful or not) which caused damage? The Convention on Cybercrime and the Directive define damage to data as data interference, not as access. The law in France, Italy and the Netherlands also distinguishes between mere access and aggravating circumstances to unauthorised access, such as copying, deleting, damaging.

2.4.20 Building on the boundary between torts and crime, the UK has not used the Directive's option to restrict the scope of the offence of unauthorised access to 'cases not minor'. In *Ellis*, the defendant was found guilty of a section 1 CMA offence having taken advantage of students not logging off on a university library computer, so that the internet could be accessed.[147] Compared with Recital 11 of the Directive, this case raises serious questions about over-criminalisation. Recital 11 gives the following explanations for the lack of seriousness not to trigger the use of criminal law: 'the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary'.

2.4.21 There is also a concern that security and threat intelligence researchers are likely to be inappropriately caught. We have seen above that for the French courts, the act of connecting to a company website to observe the consequences of others' successful

[146] Walden, *Computer Crimes and Digital Investigations* (OUP, 2015) para 3.272.
[147] *Ellis v. DPP* [2001] EWHC Admin 362.

unauthorised accesses, does not constitute an attempt.[148] It is a preparatory act. In the UK, the conduct will fall within the section 1 offence. For security and threat researchers, observing network connections can be one of the first steps necessary to detect vulnerabilities, before engaging in further investigations.[149] This point will be looked at further with regard to the concept of 'unauthorised' and in defences in **Chapter 3**. At this stage, the point is that the breadth of the CMA offences makes security and threat researchers more likely to be criminalised.

Offences of 'unauthorised acts' and 'supply or misuse' of tools

2.4.22 For offences under section 3 and 3ZA CMA, our discussion in **2.2-2.3** has demonstrated both a worrying breadth of potential inappropriate criminalisation, as well as other models for liability that can be used to avoid it. In line with that discussion, we support two core changes to the current law. That is, **we recommend (i) requiring an 'intention' to pursue a criminal endeavour, or to enable or assist another in committing an offence under the CMA 1990 (i.e. removing the potential for recklessness) and (ii) for section 3ZA, requiring the creation of a 'significant risk' (i.e. as opposed to any risk of harms) for liability to arise**.

2.4.23 Similarly, in the context of section 3A CMA, our research identifies clear risks of over-criminalisation within the current law, with security and threat intelligence researchers perhaps the most vulnerable. With this in mind, **we recommend that the section 3A making, supplying or obtaining offence should be narrowed, to apply only where a defendant intends to pursue a criminal endeavour.**

2.4.24 Many of the concerns raised in this chapter are relevant to our discussion of defences in **Chapter 3** as well. We firmly believe that reform to offences and/or defences is essential to narrow liability within the CMA 1990 to only those deserving of criminalisation, and to protect legitimate (indeed beneficial) online practices.

2.5 CORPORATE LIABILITY

2.5.1 In the context of the law against computer misuse, Article 12 of the Cybercrime Convention provided:

[148] Paris, 15 mai 2001, Juris-Data n° 148055; in Encyclopédie Dalloz para 20.
[149] Guinchard, 'Transforming the Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime' (2018) 2(2) *Journal of Information Rights, Policy and Practice* 1, 11-14.

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons [i.e. corporations] can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a. A power of representation of the legal person;

b. An authority to take decisions on behalf of the legal person;

c. An authority to exercise control within the legal person.

2. In addition to cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

2.5.2 To what extent does the regime in the CMA 1990 achieve these aims?

2.5.3 Schedule 1 of the Interpretation Act 1978 provides that 'person' includes a body of persons corporate and unincorporated. The consequence of this, as section 5 of the 1978 Act makes plain, is that where the word 'person' appears in an Act of Parliament, unless the contrary intention appears, that word should be construed as including a company, a corporation (which will include a limited liability partnership) or an unincorporated association. It follows that the use of the word 'person' in the offence-creating provisions of the CMA could include a legal person, as opposed to a natural person, provided that is consistent with Parliament's intention.

2.5.4 Although there is no authority on the point, it is at least conceivable that a corporation can commit a computer misuse offence either in its own right or as a joint principal along with someone else, perhaps an employee. Even if the intention of Parliament was that corporations could not be principals, there is no reason why a corporation could not be an accessory to a computer misuse offence where it assisted or

encouraged the commission of that offence,[150] or even a co-conspirator to the commission of such an offence.

2.5.5 However, cases where corporations are prosecuted for computer misuse offences (whether as principals, joint principals, accessories or co-conspirators) are rather thin on the ground, as presented in **Appendix B**. The recent computer misuse prosecutions that, for one reason or another, have found their way into the law reports all concern natural persons rather than corporations.

2.5.6 Part of the reason for that is likely to be because where, as here, the offences have a mental element (intention or recklessness), that element has to be proved against the corporation as much as it will against the employee who gains unauthorised access to a computer, and that is not straightforward.

2.5.7 The 'identification doctrine' provides that the guilty mind of the company will have to come from a natural person who is considered to be a controller of the company (i.e. someone sufficiently senior within the corporation that the company's 'mind' can be identified with their mind). Irrespective of how many junior employees are engaged in offences of computer misuse the company itself cannot be charged unless one of its controlling minds was aware of their actions and endorsed them.

2.5.8 Away from forms of accessorial and inchoate liability, the criminal law of England and Wales has had a historically uneasy relationship with vicarious liability, which could, in theory, hold the corporation liable for the crimes of its employees even where the corporation itself was not at fault for those crimes.

2.5.9 Where vicarious liability arises in the criminal law it tends to be in relation to summary-only statutory offences where some specific provision within the statute recognises that basis of liability. One example is section 64(5) of the Road Traffic Offender Act 1988, which provides that the owner of a vehicle (which can include a corporation) shall be conclusively presumed to have been the driver at the time of the commission of certain offences and, accordingly, that acts or omission of the driver of the vehicle at the time were his acts or omissions.

2.5.10 There is certainly no licence in the CMA to suggest that Parliament intended vicarious liability to be a route by which corporations could be convicted when their employees committed computer misuse offences. Indeed, the trend in recent years has been for Parliament to move away from vicarious liability and towards 'failure to prevent'

[150] For a case where a company was convicted as a co-principal/accessory to the criminal conduct of its senior officer, see *Lewis v Crafter; Cavendish Laboratories v Crafter* [1941] SASR 30, from South Australia, discussed in Gillies, *The Law of Criminal Complicity* (The Law Book Company Ltd, 1980) 149–151.

offences where the corporation is personally liable for failing to stop someone associated with it from committing a crime. The obvious examples here are section 7 of the Bribery Act 2010 and sections 45 and 46 of the Criminal Finances Act 2017, to which we will return shortly.

2.5.11 Stepping back, it seems to us that the provisions of the CMA, even taken in conjunction with the ordinary laws of accessorial liability, inchoate liability and vicarious liability, are insufficient to satisfy the requirements of Article 12 of the Cybercrime Convention of providing for a robust framework whereby corporate bodies can be held criminally accountable for the offences of their employees. Article 12 clearly contemplates that parties to the Cybercrime Convention should create two routes to such an outcome. The first, where the corporate body is liable for the offence committed by the employee (Article 12(1)) and the second where the corporate body is liable in its own right for failing to prevent the employee from offending (Article 12(2)).

2.5.12 As to the first of these, as we have already noted, a mechanism does exist in the law of England and Wales whereby corporations can be liable for offences committed by their employees. There are problems with this, with the application of the identification doctrine probably meaning that corporate prosecutions for computer misuse offences will be a rarity. Nevertheless, reform is this area would be a massive undertaking as it would require any law reform body to look at the general principles of domestic criminal law in the context of accessorial, inchoate and vicarious liability and we doubt that there would be any serious interest from Government in such a review being undertaken. It is worth noting that between 13 January 2017 and 31 March 2017, the Ministry of Justice ran a consultation[151] that called for evidence to consider, amongst other things, whether the identification doctrine should be reformed. At time of writing, the responses to the consultation are still being processed. Clearly, any proposals to reform this area of the law should await the outcome of that review.

2.5.13 As to the second of these, the Ministry of Justice consultation will also consider whether the failure to prevent model should apply to other financial crimes, such as fraud and money laundering. Given the terms of Article 12(2) of the Cybercrime Convention it is likely the consultation will also consider within that rubric whether to insert such an offence into the CMA.

2.5.14 The offence in section 7(1) of the Bribery Act 2010 provides that a relevant commercial organisation (C) is guilty of an offence under that section if a person (A) associated with C bribes another person intending to obtain or retain business for C or to obtain

[151] *Corporate Liability for Economic Crime: Call for Evidence* (2017) Cm 9370.

or retain an advantage in the conduct of business for C. The offence is one of strict liability, in the sense that C does not have to be at fault for the commission of C's offence, but section 7(2) provides for a due diligence defence where the burden falls on C to prove that it had in place adequate procedures designed to prevent persons associated with C from undertaking such conduct.

2.5.15 The offence avoids the pitfalls of the identification doctrine by providing that A need only be associated with C, rather than being a controlling mind of C. Section 8 provides that A will be associated with C where A performs services by or on behalf of A, which will include situations where A is an employee of C or an agent of C or even a subsidiary company of A. Moreover, before proceedings for an offence contrary to section 7 can be instituted the consent of the DPP or of the Director of the Serious Fraud Office is needed.

2.5.16 The offences in sections 45 and 46 of the Criminal Finances Act 2017 were modelled on the offence in section 7(1) of the Bribery Act 2010 and the offence of corporate homicide contained in the Corporate Manslaughter and Corporate Homicide Act 2007. Sections 45 and 46 of the former criminalise corporates for failing to prevent the facilitation of domestic tax evasion and foreign tax evasion respectively. In either case it is a defence for the corporate to prove that when the relevant tax evasion offence was committed it 'had in place such prevention procedures as it was reasonable in all the circumstances to expect [it] to have in place' or that 'it was not reasonable in all the circumstances to expect [it] to have any prevention procedures in place.'

2.5.17 Importantly, there is no requirement in sections 45 and 46 of the Criminal Finances Act for the prosecution to prove that the person associated with the corporate intended, by the commission of their offence, to benefit the corporate. In contrast, under section 7(1) of the 2010 Act, the associated person must act with the intention of benefiting the corporate, and Article 12(1) of the Cybercrime Convention focusses on the liability of the corporate for the crimes of its associate where those crimes were committed for the benefit of the corporate. For this reason, the appropriate failure to prevent model for the CMA is more likely to be that contained within the 2010 Act than that contained within the 2017 Act.

2.5.18 With these considerations in mind **we recommend the inclusion of a failure to prevent offence in the CMA in these terms:**

(a) A body corporate or partnership (B) is guilty of an offence if a person (A) commits an offence contrary to sections 1, 2, 3, 3A or 3ZA of this Act when A is acting in the capacity of a person associated with B and provided that A committed that offence for the benefit of B.

(b) A will act in the capacity of a person associated with B where A is an employee of B, an agent of B, or any other person who performs services by or on behalf of B.

(c) It is a defence for B to prove that B had in place adequate procedures designed to prevent persons associated with B from committing such offences.

2.6 SUMMARY OF RECOMMENDATIONS

2.6.1 We recommend reforms to the section 1 CMA unauthorised access offence:

- **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 beyond simple unauthorised access.**

2.6.2 We recommend reforms to section 3 and section 3ZA CMA unauthorised act offences, by narrowing their application:

- **Requiring an 'intention' to pursue a criminal endeavour, or to enable or assist another in committing an offence under the CMA 1990 (i.e. removing the potential for recklessness); and**
- **For section 3ZA, requiring the creation of a 'significant risk' (i.e. as opposed to any risk of harms).**

2.6.3 We recommend that section 3A CMA making, supplying or obtaining offence should be narrowed, to apply only where a defendant intends to pursue a criminal endeavour.

2.6.4 We recommend the creation of a new corporate failure to prevent offence, to apply across all of the CMA 1990 offences [set out in 2.5.18].

CHAPTER 3

DEFENCES

3.1 INTRODUCTION

3.1.1 The CMA 1990 contains no specific defences to any of the offences in sections 1, 2, 3, 3A or 3ZA. Statutory defences exist in respect of a number of offences that are similar in some ways to the computer misuse offences, such as those discussed at **Chapter 1.4**, and so it is surprising that those defences are not also contained in the CMA, especially given the breadth of the offence-creating provisions, as discussed in **Chapter 2**. Moreover, if our recommendation to create a corporate 'failure to prevent' offence with regard to computer misuse is taken forward, and that offence is given its own specific 'adequate procedures' defence, then it will give rise to an obvious anomaly within the legislation whereby the employee who commits the computer misuse offence will have no defence but the company that allowed it to happen will.

3.1.2 In this Chapter we consider, by reference to the present law, whether any defences are available to those who commit computer misuse offences before we turn to examine the extent to which the various international instruments require national jurisdictions to recognise the existence of offence-specific defences. We then consider the specific defences that are available in domestic law for offences that share similarities with the computer misuse offences, and analyse the arguments for and against transposing some or all of those defences to the CMA 1990. In doing so we specifically consider the position of those who are more likely than most to find themselves falling foul of the CMA provisions even though they would maintain that their work is of benefit either to the public (such as journalists) or to the 'victim' of the computer misuse itself (such as security and threat intelligence researchers).

3.2 SECTION 10 SAVING/EXCLUSION AND THE GENERAL DEFENCES

3.2.1 Section 10 of the CMA 1990 creates a saving in England and Wales to the effect that where a person is required by any enactment to inspect, search or seize a computer or its contents no offence under the CMA will be committed. This will be the case even where the person entitled to exercise control over the computer or computer system withholds their consent to the inspection, search or seizure.

3.2.2 The rationale for this saving provision is obvious: police officers who seize and inspect computers pursuant to their statutory powers should not be at risk of prosecution under the CMA even where the owner of the device tells them not to inspect it. This saving is not limited to law enforcement officers, but it is limited to the operation of powers reposed in a person by a statute or statutory instrument. We discuss the application of the saving to other forms of statutory enforcement at **Chapter 1.4**.

3.2.3 But what is the position where a law enforcement officer accesses a person's computer pursuant to an order of a court rather than in furtherance of a specific statutory power granted to that officer? Suppose a court makes a serious crime prevention order (SCPO) under the relevant provisions of the Serious Crime Act 2007 and one of the requirements of the order is that an officer of the National Crime Agency is permitted, on the giving of notice to the defendant, to inspect any electronic devices in the defendant's possession. If the officer accesses those devices in the teeth of objections from the defendant, the issue will be whether that access was unauthorised within the meaning of section 17(5) CMA 1990 and that will turn on whether the order of the court means the officer is a person 'entitled to control access' to the electronic device in question. **Rather than having to construe the statutory provisions we think it would be easier in these circumstances if the CMA provided for a specific defence where the person who accesses etc the electronic device does so pursuant to a court order.**

3.2.4 We presume that the general defences, like duress, are not precluded by the legislative regime in the CMA 1990. Certainly, if it had been Parliament's intention to exclude those defences then that could have been achieved easily by the insertion of an appropriate clause into the Bill. In the absence of such a section it is safe to assume, we suggest, that someone whose life is placed in peril if he does not commit a computer misuse offence will have a defence available to him in the event of a prosecution. However, if the same person was to claim that his unauthorised access was in the public interest or was necessary for the purposes of preventing or detecting crime, he would have no defence on the law as it presently stands because those are not general defences.

3.2.5 Where the defendant suffers from a mental disorder, other general provisions may also come into play. Where the disorder significantly impacts the defendant's ability to participate in and understand his trial, he may be found to be 'unfit to plead' with the result that no trial takes place.[152] Even where the defendant is fit to plead, it may be that his condition affected his mental state (eg, foresight or intention) such that he lacked the mens rea (the mental element) of the crime charged. Where such denial is linked to a mental disorder, this is sometimes referred to as the 'computer addiction defence'. This was successfully argued in 1993 in the case of one among three teenage hackers who called themselves 8LGM (Eight Legged Groove Machine).[153]

3.3 INTERNATIONAL COMPARISON

3.3.1 In **Chapter 2** we considered the computer misuse offences in detail and in so doing we considered the provisions of the Convention on Cybercrime, Directive 2013/40/EU, and the national laws of a number of other countries, most notably France, Italy and the Netherlands.

3.3.2 Returning to those international instruments first, it is clear that they have very little to say about the provision of defences in domestic legislation.

3.3.3 As to the Cybercrime Convention, Article 6(1) concerns the misuse of devices and the need for domestic law to provide for criminal offences to cater for the possession, production, sale, procurement etc of devices, passwords and access codes where the intention is that they should be used to commit computer misuse offences. Article 6(2) provides that no criminal liability should attach where the possession, production, sale, procurement etc is not for the purpose of committing a computer misuse offence, 'such as for the authorised testing or protection of a computer system.'

3.3.4 The equivalent provision to Article 6(1) in the CMA 1990 is the offence in section 3A but, importantly for present purposes, that section contains no specific defence to protect those who make, adapt, supply or offer to supply articles that are intended to be used for authorised testing or for the protection of a computer system. This is not as significant an omission as it might at first appear: if the person making etc the article believes the user of the article will have authority to access a computer system then the offence under section 3A will not be made out because in those circumstances it could not be said against the maker that he intended the user to gain unauthorised

[152] Criminal Procedure (Insanity) Act 1964, s4 and 4A.
[153] *Bedworth* (1993) Unreported. The case is discussed in Charlesworth, 'Legislating against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990' [1993] 4(1) *Journal of Law, Information and Science* 80.

access to the system. However, where there is uncertainty about the legal practices of system testing (and associated academic testing etc), as we discussed in **Chapter 2**, there remains some cause for concern.

3.3.5 Recital 16 to Directive 2013/40/EU expands on Article 6(2) of the Convention by recognising that 'tools' which are capable of being used to commit computer misuse offences might have perfectly legitimate uses as well. For this reason Recital 16 makes it plain that domestic legislation should provide that only a specific intention on the part of manufacturer etc, that the 'tools' should be used to commit one or more computer misuse offences, should suffice to establish liability. This is done in order ensure that those who place such 'tools' on the market do not find themselves committing a computer misuse offence because the person who acquires the 'tools' chooses to use them for an illegitimate purpose rather than a legitimate one. It seems to us that section 3A achieves that objective.

3.3.6 Staying with the Directive, we observed in **Chapter 2** that Articles 3, 4 and 5 required Member States to take the necessary measures to create the criminal offences set out in those Articles 'at least for cases which are not minor.' Accordingly the Directive did not require Member States to criminalise minor examples of computer misuse, but at the same time the Directive did not stipulate that Member States could not penalise such minor infractions. It might be tempting to raise that aspect of the Directive in support of a general *de minimis* defence to the domestic computer misuse offences, but for the reasons articulated in the preceding sentence we do not believe that that is what the framers of the Directive had in mind. In the law of England and Wales there is no general *de minimis* defence and where such a defence appears in statute it is very tightly confined.[154]

3.3.7 The provisions of French domestic law concerning the supply of 'tools' that can be used for the commission of computer misuse offences, follow the spirit of Article 6(2) of the Convention by providing that an offence will only be committed where the supply etc is carried out without legitimate reason, notably for research or IT security. Arguably, a specific defence for those engaged in research rather than simply security testing is wider than the Convention recommends. It is also unclear the extent to which 'research or IT security' are merely illustrative examples of the sorts of legitimate reasons that will provide a defence, as opposed to limiting what that legitimate reason could be to 'research or IT security'.

[154] The Offences Against the Person Act 1861, s44, expressly preserves the power of 'the justices' to dismiss a complaint if it is 'so trifling as not to merit any punishment' and so there is at least one statutory precedent in this jurisdiction for the *de minimis* principle, although in *Austen v Crown Prosecution Service* [2016] EWHC 2247 (Admin) the Divisional Court held the provision applies only to private prosecutions.

3.3.8 Beyond this example from France, the domestic law of the other countries we considered in **Chapter 2** provide for no specific defences to computer misuse offences. However, in the case of the USA that could be about to change. In June 2019, the Active Cyber Defense Certainty Act (ACDC), a bipartisan Bill, was introduced into the House of Representatives in an effort to make targeted changes to the Computer Fraud and Abuse Act (CFAA), which penalises computer misuse. The short title to the Bill states that it will '*provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorised intrusions in their computers and for other purposes*'.

3.3.9 In particular the Bill provides an exclusion from prosecution for certain computer crimes for those taking active cyber defense measures. Where a person or entity is a victim of persistent unauthorised intrusion of their computers then they can access without authorisation the computer of their attacker in order to gather information about the attacker's criminal activities and to share this information with law enforcement. The victim will need to be careful to ensure that in accessing the attacker's computer it does not, inter alia, destroy any data that does not relate to the victim or create a threat to public health or safety. Before the victim takes any steps to access the attacker's computer authorisation will need to be sought from the FBI.

3.3.10 The Bill came about because of concerns about the ability of individuals and entities to protect themselves against cyberattacks. The guide to the Bill leans heavily on the notion that attack is the best form of defence. A 'feedback process' began in March 2017 and took in the views of members of the business community, academics, and cybersecurity policy experts before the Act was introduced. According to the guidance 'ACDC unties the hands of law-abiding defenders to use new techniques to thwart and deter attacks, while also providing legal certainty for industry experts to innovate, which could spur a new generation of tools and methods.'[155]

3.3.11 We feel that while the changes proposed in ACDC are interesting and innovative it is too early to say whether they will be successful in achieving the aims set by those who have championed the Bill, and in these circumstances we believe **it would be premature to make any recommendations that UK law follow a similar path**, especially where there is no parallel defence in any other domestic legislative provision of which we are aware.

3.3.12 In the defences we discuss (and recommend) below, our focus is on facilitating security researchers in identifying and reporting vulnerabilities, and to provide legal certainty for threat intelligence researchers investigating cyber criminals and

[155] House of Representatives, *Active Cyber Defense Certainty Act: Bipartisan Bill Empowers Americans to Develop New Defenses Against Cyber Attacks* (2019).

attackers. Our aim is not to facilitate active reverse attacks. In this manner, our approach is consistent with Article 6(2) of the Cybercrime Convention.

3.4 DOMESTIC COMPARISON

3.4.1 In their Final Report,[156] the Law Commission made no reference to stand-alone defences to the proposed computer misuse offences and nor was this a matter touched on by the APIG in its Report.[157] Mr Harry Cohen MP, during the discussion of the private member bill in May 1990, raised the issue of a defence for journalists and whistleblowers, based on the facts of the *Goodwin* case decided by the House of Lords, not yet referred to the European Court of Human Rights; but his argument was dismissed.[158]

3.4.2 This position can be contrasted with the law so far as it relates to the protection of personal data. Sections 170 and 171 of the Data Protection Act 2018 created two new offences and came into force on 25 May 2018.[159] Section 170(1) provides that it is an offence for a person knowingly or recklessly:

(a) to obtain or disclose personal data without the consent of the controller;
(b) to procure the disclosure of personal data to another person without the consent of the controller; or
(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

3.4.3 Section 170(2) provides for a number of specific defences to these offences, including that the person's act was 'necessary for the purposes of preventing or detecting crime,' or was 'required or authorised by an enactment, by a rule of law or by the order of a court or tribunal' or 'in the particular circumstances, was justified as being in the public interest.'

3.4.4 It follows that if someone obtains personal data by, for example, gaining unauthorised access to a computer without the consent of the data controller, it would be a defence to a charge under section 170 of the DPA 2018 if in the particular circumstances the obtaining of the personal data was justified in the public interest. The same would not,

[156] Law Commission, *Computer Misuse* (LC No 186, 1989).
[157] All Party Parliamentary Internet Group, *'Revision of the Computer Misuse Act': Report of an Inquiry by the All Party Internet Group* (2004).
[158] HC Deb, 4 May 1990, Col. 1331-1333.
[159] SI 2018/625.

however, be a defence to a charge under section 1 of the CMA of gaining unauthorised access to a computer.

3.4.5 This creates an anomaly between the two legislative regimes. If the personal data was kept in a written diary and a person copied it from that diary without the consent of the data controller the only offence available in these circumstances would be one contrary to section 170 of the DPA 2018 (since data is not 'property' within the meaning of the Theft Act 1968). Thus, the public interest defence would be available to the accused person. But, if the personal data was kept on a computer hard-drive and the person copied that data onto a memory stick without the permission of the controller or user of the computer, a prosecution could also be brought under the CMA, as to which there would be no public interest defence. Why should the law provide a public interest defence for someone who obtains personal data but only where that data was *not* obtained as a result of that person misusing someone else's computer as opposed to misusing someone else's notebook? Why should someone who holds data which he would prefer to conceal and which ought to be publicly available be better protected by the criminal law if he stores it on his computer?

3.4.6 Section 170(3) created a number of further defences that find no parallel in the CMA but where there are parallels in other legislation. One obvious example is section 170(3)(b) which provides that it is a defence for a person charged with an offence under sub-section (1) to prove that 'the person acted in the reasonable belief that that person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it.' It follows that if the person who obtains the personal data knows that the controller does not in fact consent to them obtaining the data but he believes that if the controller knew about his reason for obtaining the data, for example, the controller would have consented to his obtaining it, that is a defence.

3.4.7 That particular defence appears to be drawn from section 2(1)(b) of the Theft Act 1968 and section 5(2)(a) of the Criminal Damage Act 1981. As to the latter statute, under section 1(1) of that Act, a person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage such property or being reckless as to whether such property would be destroyed or damaged shall be guilty of an offence. Section 5(2)(a) provides that for the purposes of section 1(1) a person shall be treated as having a lawful excuse 'if at the time of the act or acts alleged to constitute the offence he believed that the person or persons whom he believed to be entitled to consent to the destruction of or damage to the property in question had so consented, or *would have so consented to it if he or they had known of the destruction or damage and its circumstances* [emphasis added].' Section 5(3) serves

to emphasise that the person's belief does not need to be justified provided it is honestly held.

3.4.8 However, the parallels with the Theft Act 1968 and Criminal Damage Act 1971 are not exact because in neither case does the requisite belief need to be held on reasonable grounds. By contrast, under section 170(3)(b) of the DPA 2018 – 'the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it' – the belief on the part of the accused has to be a reasonable one. An honest belief alone will not suffice.

3.4.9 The DPA 2018 also contains a defence in section 170(3)(a) that arises where 'the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining.' The obvious parallel here is with section 2(1)(a) of the Theft Act 1968, which provides that a person's appropriation of property belonging to another is not to be regarded as dishonest 'if he appropriates the property in the belief that he has in law the right to deprive the other of it, on behalf of himself or of a third person.'

3.4.10 For the purposes of the section 2(1)(a) defence in the 1968 Act, an honest if unreasonable belief will suffice whereas it is clear from section 170(3)(a) of the DPA 2018 that only a reasonable belief will do. The authorities decided under the 1968 Act hold that no such right need exist provided the accused believes the right does – in law – exist,[160] and that the onus is on the prosecution to disprove to the criminal standard the accused's belief in the existence of this right in order to prove that he acted dishonestly. It is probably the case under the DPA 2018 that, to similar effect, the legal right to obtain, disclose, procure or retain the personal data need not in fact exist but unlike the 1968 Act provisions, the accused person probably bears the burden of proving on the balance of probabilities that he had such a reasonable belief.[161]

3.4.11 Section 2(1)(c) of the 1968 Act also provides that a person's appropriation of property belonging to another is not to be regarded as dishonest 'if he appropriates the property in the belief that the person to whom the property belongs cannot be discovered by taking reasonable steps' (except where the property came to him as a

[160] See Ormerod and Williams, *Smith's Law of Theft* (9th ed, 2007) §2.276 at 104. The authors make the point at §2.279 that this defence is confined to the offence of theft. Parliament chose not to extend it to other offences contained within the 1968 Act.

[161] In the recent case of *Shepherd v Information Commissioner* [2019] EWCA Crim 2 the Court of Appeal held that defence-creating provisions of the now repealed Data Protection Act 1998 imposed a legal burden on the prosecution whereas it said, per incuriam, that the equivalent provisions in the DPA 2018 imposed a legal burden on the accused (at [54] – [55]). That position also emerges from a consideration of the Explanatory Note to the Bill that became the DPA 2018.

trustee or personal representative) the so-called 'finder's defence' that preserved the rule under the common law. There is no equivalent defence in the DPA 2018 available to an accused who was unable to discover, even by the taking of reasonable steps, who the data controller was.

3.4.12 The 'finder's defence' to theft could perhaps be more successful where the property appropriated is a computer. If a person finds a mobile telephone on the ground that is not pin-locked and they decide to take the device, then on a charge of theft their line of defence might be that the identity of the owner of the handset could not in law have been discovered by the taking of the necessary steps (ie without committing an offence under section 1 of the CMA 1990) and so, this step not being open to them, and perhaps not even open to the police, the provision in section 2(1)(c) ought to avail them, with the result that they were not dishonest when they took the device. Closing this potential loophole would require amendment to the CMA to ensure that seeking to discover the owner of the device does not attract liability.

3.4.13 Clearly, then, the DPA 2018 contains a raft of specific defences that mitigate the potential harshness of a very wide offence. That Act came into being partially as a consequence of the General Data Protection Regulations,[162] which themselves came into force on 25 May 2018 two days after the DPA 2018 received Royal Assent. The Conservative Party manifesto at the 2017 general election had contained a commitment to repeal and replace the UK's existing data protection laws to keep them up to date for the digital age and to help prepare the UK for a future outside the EU.[163]

3.4.14 This was followed by a 'Statement of Intent' published by the Department for Digital, Culture, Media & Sport on 7 August 2017 which set out the policy justifications underpinning the Data Protection Bill and emphasised that one of the purposes behind the new legislation was to 'bring EU law into our domestic law' in preparation for the day when the UK leaves the EU.[164]

3.4.15 The Statement of Intent went on to say that like the predecessor legislation (ie the Data Protection Act 1998) the Information Commissioner's Office and the Crown Prosecution Service will continue to prosecute offenders under the terms of the new statute, and added that the '[o]ffences will be modernised to ensure that prosecutions continue to be effective and we will also create new offences to deal with emerging threats.'[165] The Statement set out what the new offences would be and went on to say

[162] EU/2016/679. As a set of EU Regulations, the GDPR are directly applicable to the UK without the need for implementing legislation and have direct effect in UK law.
[163] See paragraph 1 to the Explanatory Notes to the DPA 2018.
[164] *A New Data Protection Bill: Our Planned Reforms* (2017) 2.
[165] Ibid. p10.

that '[t]he important role of journalists and whistleblowers in holding organisations to account and underpinning our free press will be protected by exemptions.' The Explanatory Notes to the DPA 2018 say very little about the operation of the defences in section 170 (and section 171) beyond re-stating what those defences are.[166] That is surprising given the specific reference in the Statement of Intent to the importance of exemptions (defences) for journalists.

3.4.16 The Statement of Intent also drew the important connection between cybersecurity and data protection: 'Effective data protection in part relies on organisations adequately protecting their IT systems from malicious interference.'[167] The Government's Cyber Security Regulation and Incentives Review, published in 2016, had concluded that the implementation of the new data protection law should result in significant improvements to the management of cyber security risks: 'Indeed, evidence gathered in the course of the *Review* indicated that the increased financial sanctions applicable for data breaches, and the introduction of aggravating and mitigating factors, will result in improved cyber security practices in the UK.'

3.4.17 Given the obvious connection between the protection of personal data and the protection of the integrity of computers and computer systems, it is now an unwelcome feature of the law of England and Wales that the former contains a comprehensive catalogue of offence-specific defences whereas the latter does not. Those who obtain personal data via non-electronic means are placed at a significant advantage over those who obtain personal data via electronic means and in circumstances where the obtaining of personal data involves the commission of a computer misuse offence. The Crown Prosecution Service will have a choice whether to charge that person with an offence that carries with it a range of possible defences or an offence to which there are no recognised statutory defences. That is an invidious position to place both the prosecutor and the accused person in.

3.4.18 Of course, where a person claims to have committed a computer misuse offence in the public interest, the CPS will always have to decide whether a prosecution would itself be in the public interest. We discuss this further in **Chapter 4**. There have been cases where the CPS has refused to charge journalists with 'hacking' offences because there would be no public interest in a prosecution.[168] However, the existence of prosecutorial discretion is not a substitute for legislative defences; at least, not if such defences can be properly drafted, and we suggest that they can.

[166] Paras. 490, 495 and 496.
[167] At p23.
[168] For example, see Sabbagh et al, 'Sky News admits hacking emails of 'canoe man'' (Guardian Online, 5 April 2012): https://www.theguardian.com/media/2012/apr/05/sky-news-hacking-emails-canoe-man.

3.5 REFORMING THE DEFENCES

3.5.1 Drawing on the DPA 2018 we now consider the separate and specific defences that could be considered for inclusion in the CMA.

Required by law

3.5.2 It seems to us that so far as law enforcement officers are concerned it would be helpful to **clarify the definition of 'unauthorised' in section 17(5) of the CMA** to make it plain that a person will be 'himself entitled to control access of the kind in question to the program or data' if he is 'entitled to exercise that control by an enactment, by a rule of law, or by the order of a court or tribunal', to borrow the language of section 170 of the DPA 2018. This will regularise the position of law enforcement officers as between the statutory regimes for regulating computer misuse and data dissemination, avoid technical arguments as to what 'entitled' means within the CMA and resolve any ambiguity with respect to the savings provision in section 10 of the CMA.

Reasonable belief in consent

3.5.3 As presently drafted section 17(5) of the CMA provides that access of any kind by any person to any program or data held in a computer is unauthorised if either (a) the person was not himself entitled to access that program or data, or (b) the person did not have consent to access that program or data from the person who is so entitled. If the person who accesses the program or data is not entitled to access it, does not have the consent of the person so entitled to access it, but reasonably believes that the person so entitled would give his consent if they knew the circumstances in which access was being sought, he will have no defence.

3.5.4 This harkens back to the example we gave earlier of the person who finds a mobile telephone on the ground and accesses it in order to find out who it belongs to, so he can return it. In doing so he commits a computer misuse offence contrary to section 1. We are not persuaded that the existence of prosecutorial discretion is a sufficient safeguard against the risk of prosecution in such a case; and nor should people who act in a way which they genuinely and reasonably consider to be in the interests of the person with the power to consent to the access sought be at risk of a prosecution. The law should not operate so as to deter the good Samaritan in cases such as this.

3.5.5 For these reasons **we recommend the insertion of an amendment in section 17(5)(b) to the effect that access will be unauthorised if the person accessing the program or data does not have the consent of the person entitled to control access or does not reasonably believe that he would have had the consent of the person entitled to control access if the controller had known about the access and the circumstances of it, including the reasons for seeking it**.

3.5.6 In the case of 'hackers' that latter requirement should serve to distinguish between legitimate security testers, who gain access to computer systems in order to stress test them but without necessarily obtaining the consent of the controller, and others whose intentions are malign and who seek to disrupt the activities of the controller. With respect to the former, the 'hacker' can legitimately say that if the controller had been aware of the reasons for gaining access to the program or data they would have consented, because the controller would want to ensure their systems were robust; whereas in the case of the latter it is difficult to see how the malign 'hacker' could successfully argue that they reasonably believed the controller would have consented to their access knowing that they intended to harm the controller's computer systems in doing so.

Public interest

3.5.7 In recent years, pressure groups have called for the insertion of a public interest defence into the CMA, and other statutes.[169] And with the introduction of such a defence within section 170 of the DPA 2018, those calls are likely to grow louder. We recognise that, notwithstanding the presence of a public interest defence in the DPA 2018, there are powerful arguments against the inclusion of a similar defence in the CMA. We will consider these arguments below.

3.5.8 With respect to this particular defence, concerns have been expressed to us by a number of interest groups, including journalists, academics, expert witnesses, security researchers, consultants and analysts that the valuable work they do can fall foul of the offence-creating provisions of the CMA because there is no specific exemption or defence available to them (in the case of security researchers, we will consider their role further in the section below, on whether to create a specific defence of crime detection/prevention). A public interest defence is most apposite to the role of journalists and whistleblowers who might have cause to gain unauthorised access to

[169] See, for example, https://hackinginquiry.org/journalism-and-the-public-interest-a-hacked-off-initiative/ and http://hackinginquiry.org/wp-content/uploads/2014/10/Speech-by-Dr-Evan-Harris-to-the-Liberal-Democrats-autumn-conference.pdf.

a computer system in order to access information, the disclosure of which is said to be a matter of public interest. Should 'hackers' whose activities are for the public good have a specific defence available to them or is their position adequately protected in other ways?

3.5.9 The possibility of inserting a public interest defence into a statute to sit alongside its offence-creating provisions has arisen before. In its Consultation Paper on the *Protection of Official Data*,[170] the Law Commission considered whether a public interest defence should be included in the Official Secrets legislation. At para 7.3, the Commission drew a distinction between two versions of a public interest defence. The first is objective and calls for an assessment of whether the disclosure of official data was in the public interest. The second is subjective and would require the court to examine whether the defendant believed that the disclosure of official data was in the public interest regardless of whether it was actually in the public interest.

3.5.10 In the White Paper that preceded the introduction of the Official Secrets Act 1989, consideration was given to the enactment of a public interest defence.[171] A subjective public interest defence was rejected on the basis that a person's motives for committing crime should not be relevant to his liability. It was said that it would also create difficulties where there are mixed motives in 'unpicking' the real or dominant reason for the disclosure having been made.

3.5.11 The Law Commission observed, as we have already noted, that an objective public interest defence was contained in section 55 of the DPA 1998. At para 7.10 the Commission pointed out that the 1998 Act was introduced to give effect to that in Data Protection Directive 95/46/EC, but that Directive did not require the inclusion of a public interest defence in the domestic legislation. From its research the Commission was unable to discern the rationale for the inclusion of that particular defence in the Bill that became the DPA 1998, and nor did it derive any assistance from the case law in this area. As an aside, section 78 of the Criminal Justice and Immigration Act 2008 was set to insert a subjective public interest defence into the DPA 1998, but it was never brought into force.

3.5.12 Objective public interest exemptions can be found in section 20 of the Commissioners for Revenue and Customs Act 2005 and section 3 of the Agricultural Statistics Act 1979. In both of those examples, a relevant disclosure is exempt from penalisation under the statute if either the Revenue and Customs Commissioners or the Minister respectively agrees that such a disclosure was in the public interest. However, a distinction should be drawn here between exemptions – where the elements of the

[170] Law Commission (Consultation No 230, 2017).
[171] *Reform of Section 2 of the Official Secrets Act 1911* (Cm 408, 1988).

offence are not made out if the exemption applies – and defences – where the elements of the offence are made out but the accused person is nevertheless entitled to be acquitted because the statute provides him with a standalone defence. In the 1979 Act and the 2005 Act the public interest exists as an exemption to liability for the offence rather than as a defence.

3.5.13 The Law Commission considered that the insertion of a public interest defence into the Official Secrets legislative regime could enhance the accountability of the government by revealing alleged illegality or impropriety. However, it seems to us that that justification would not apply in every case where a person commits a computer misuse offence because, while such an offence could be committed against a government computer system, it could equally be committed against a computer system operated by a private individual or entity.

3.5.14 In the Law Commission's view, a subjective public interest defence could serve to protect disclosures that are not in fact in the public interest and as a matter of policy the law should not be slow to allow accused persons to escape responsibility for acting in contravention of the public interest just because they erroneously believed that their actions were in the public interest.

3.5.15 With respect to an objective public interest defence, the Law Commission pointed out that such a defence would do little to help those inclined to disclose data (relevant to official secrets offences) to understand whether their intended actions would be lawful, because it would ultimately be for a jury to decide some time later whether their actions had been in the public interest. Similarly, anyone who decided to engage in computer misuse for a specific purpose that they considered to be in the public interest, if an objective public interest defence were available, would be rolling the dice. A jury could agree with them, in which case they would escape sanction, but equally a jury could disagree with them in which case they would be criminalised for their actions.

3.5.16 The Law Commission also felt that jurors would be faced with 'an impossible task' in seeking to distil the requirements of the public interest on the facts of any given case.[172] Such an exercise would require the jury to consider complex moral, political, social and economic issues, and could result in different juries reaching different conclusions on similar facts, which would do nothing for public confidence in the law more generally. Even more concerning than that, given the 'amorphous nature' of the very concept of the public interest, anyone charged with a computer misuse offence could be inclined to plead not guilty in reliance on the defence and throw themselves on the mercy of the jury. If that were to happen, the Law Commission opined, the

[172] Para 7.53.

floodgates could open. For these reasons, the Law Commission concluded that the problems associated with the introduction of a statutory public interest defence (whether objective or subjective) outweighed the benefits in the context of official secrets.

3.5.17 It seems to us that the concerns expressed by the Law Commission about the scope for the public interest defence to create 'legal uncertainty' and 'to undermine the efficiency of the criminal justice system'[173] are overstated.

3.5.18 A number of common concepts in domestic criminal law are arguably amorphous and could easily mean different things to different people. Dishonesty is one of them. Since the decision of the Supreme Court in *Ivey*,[174] which post-dates the publication of the Consultation Paper, whether a person's actions were dishonest has been an objective test and, like an objective public interest defence, it therefore falls to a jury to decide by the standards of ordinary and decent people whether that person behaved dishonestly or not.

3.5.19 The Supreme Court had no difficulty amputating the subjective limb of the test for dishonesty (as it existed prior to *Ivey)* and equally it had no hesitation, therefore, in supporting the ability of juries to apply an objective test that is likely to bring into play many of the factors a jury would have to consider in deciding whether an objective public interest defence was made out. There is no more reason to suppose that juries will make capricious assessments of a person's honesty than there is to suppose that they would do so when reflecting on whether a person's actions were or were not in the public interest.

3.5.20 Instead of a public interest defence, the Law Commission recommended the adoption of a statutory commissioner model whereby a commissioner could receive and investigate complaints from those working in the security and intelligence agencies and the members of those agencies who made those complaints would be protected from prosecution. However, those protections would not apply to journalists because they would be unable to make disclosures to the statutory commissioner.

3.5.21 The position of journalists making disclosures in the public interest was raised in Parliament at the Report stage of the *Digital Economy Bill*, but Matt Hancock MP responded to those concerns by saying that 'The public interest is not covered in this Bill, but that is because the nature of a public prosecution is that it has to be in the public interest.'[175]

[173] Para 7.64.
[174] *Ivey v Gentings Casinos (UK) Ltd* [2017] UKSC 67.
[175] HC Deb, 28 November 2016, Col 1349.

3.5.22 In its Consultation Paper on protecting official data the Law Commission specifically considered the role of journalists and disclosures in the public interest. Drawing heavily on Lord Justice Leveson's *Inquiry into the Culture, Practices and Ethics of the Press*, the Commission doubted whether journalists should be treated differently from other citizens. Lord Justice Leveson had made the point that introducing a public interest defence for journalists would be 'to emasculate almost all prospect of bringing a journalist to task for the way in which a story has been researched, whatever means, at first blush illegal, might have been used.'[176]

3.5.23 His Lordship added that journalistic activity was already adequately protected from a combination of the public interest test for all prosecutions, the ability of the courts to stay their own proceedings as an abuse of process, the role of the jury and the discretion of sentencing judges. Although not specifically referred to by the Law Commission in its analysis, a journalist-only public interest defence would also give rise to significant litigation on the question of who qualifies as a journalist. In an age where anyone with a computer is capable of blogging online about current affairs, there is an argument for saying that everyone could be a 'journalist'.

3.5.24 We note in passing that the focus of the Commission's Consultation Paper was on the disclosure of official secrets. It did not specifically consider the computer misuse offences and its publication preceded the introduction of the DPA 2018, where the objective public interest defence appears.[177]

3.5.25 Nevertheless, we agree with the Commission's analysis in two important respects. First, that a subjective public interest defence would be inappropriate for the CMA as much as it was for the DPA 2018. It should not be open to any individual to certify that their actions were lawful and for it to be so. Secondly, that an objective public interest defence should not be confined to journalists. Not only would that open up questions over who qualifies as a journalist but it would not protect pen-testers, forensic investigators, academics or expert witnesses whose actions could equally be said to have been in the public interest.

3.5.26 We consider that an objective public interest defence should be available under the CMA. We can see no principled reason why such a defence should exist in the context of the unlawful dissemination of data when it has not been extracted from a computer but not be available when access has been secured to a computer for that purpose. Moreover, we consider that the general objections to an objective public interest defence that were raised by the Law Commission in its Consultation Paper on the

[176] Vol 4, Ch 2, para 6.6.
[177] It only considered the CMA with regard to territoriality issues, discussed in **Chapter 2**.

protection of official data, when properly analysed, do not outweigh the benefits of having a public interest defence in the CMA.

3.5.27 In making that recommendation we recognise that it would not be appropriate to have an objective public interest defence for every CMA offence. Clearly, the defence should be available to those charged with unauthorised access contrary to section 1, because that is the sort of activity that journalists and others are most likely to engage in. It seems to us, however, that it would be inappropriate to have such a defence to a charge under section 2, where access is secured with the intention of committing a further criminal offence. With regard to section 3A we consider that such a defence would be unnecessary because a person could only be guilty of that offence if he intended the commission of a section 1 offence etc, which would only be the case if the person intended that the person committing the section 1 offence would *not* be acting in the public interest (that being a defence to an offence contrary to section 1, assuming our recommendation is followed).

3.5.28 The position with respect to offences in section 3ZA and section 3 is more difficult. Regarding the former, although section 3ZA entails a risk of serious damage, we are concerned that its broad interpretation in the current law (see **Chapter 2**) creates considerable overlap with section 1 offending, and thereby engages many of the same reasons for extending a defence. However, it is our view that this is better corrected at the offence stage, in line with our **Chapter 2** recommendations, rather than the use of defences.

3.5.29 We are convinced, however, that defences should apply to section 3: where D gains unauthorised access to a computer with intention or recklessness as to whether that act will or might impair the operation of a computer etc. If someone commits an unauthorised act in relation to a computer, not to access information on it that would be in the public interest to disclose, but in order to compromise that computer, then the more appropriate defence (if any) would be the prevention of crime, which we consider below. Nevertheless, there is an obvious potential overlap between the public interest and the detection and prevention of crime, and it would be artificial, we think, to say that the former should not be a defence to a section 3 offence but the latter should be. That would create an incoherent scheme of defences within the CMA and could lead to those who commit section 3 offences in the public interest having to mould their actions to the contours of a different defence, namely the detection and prevention of crime.

3.5.30 For these reasons **we recommend that an objective public interest should be available to those who commit offences contrary to sections 1 and 3 of the CMA.**

Detection and prevention of crime

3.5.31 It should be borne in mind when considering this possible defence that there are two distinct strands to it. This is because the steps a person might need to take in order to detect whether another person has committed a crime could be different to the steps they might need to take in order to ensure that that person does not commit any more crimes. One obvious example is where a computer system comes under attack from an outside source. The controller of the system could seek to identify the source by securing unauthorised access to the attacker's computer. That unauthorised access could be protected from criminalisation by the introduction of a 'detection of crime' defence. If, having secured that access, the controller realises that the attacker intends to carry out further attacks on other computer systems, and so he takes steps to disable the attacker's computer (and hence his ability to commit further crimes) then that additional step taken by the controller would not be covered by a 'detection of crime' defence but could be by a 'prevention of crime' defence.

3.5.32 This raises an issue as to how proactive a 'detection/prevention of crime' defence should allow a person to be. It would clearly be inappropriate if the defence permitted members of the public to gain unauthorised access to the computer systems of others just to see if those others were in the business of committing crimes, and it would be equally inappropriate if, having gained access to the computer systems of others, members of the public could interfere with or even disable those systems in order to guard against even the slightest risk that crimes could be committed at some unspecified time in the future. In either of these cases the actions of the members of the public would be open to fair criticism on the basis that they could, and arguably should, have taken their concerns to the police rather than becoming investigators themselves.

3.5.33 In the context of the use of force, section 3(1) of the Criminal Law Act 1967 provides that a person may use such force as is reasonable in the circumstances in the prevention of crime etc. This provision has been interpreted by the courts to mean that a person cannot use force once the crime he intends to prevent has already been completed,[178] but he can use force before the wrongdoer has embarked on the crime provided the user of the force immediately apprehends that a crime will be committed.[179] The speculative possibility that a crime will take place at some time hence will be no justification for the use of force in order to prevent it.

[178] See *Bowden* [2002] EWCA Crim 1279.
[179] See *R (DPP) v Stratford Magistrates' Court* [2017] EWHC 1794 (Admin).

3.5.34 Section 3 is crafted to defend forceful intervention, the traditional means of preventing criminal acts. This will not, of course, apply to typical non-forceful interventions to prevent cyber offences. But the same rationale, to justify and enable crime prevention, drives our recommendations for a defence of crime prevention in the latter context as well.

3.5.35 Such a defence is crucial, but also importantly narrow and targeted. By extending the reasoning behind section 3 to any proposed 'prevention of crime defence' in the CMA, it should only be in those situations where a crime is in the process of being committed or is about to be committed that a person would be able to rely on the defence to justify their unauthorised access to a computer system. And even then, we suggest, where alerting the authorities is not a realistic alternative to the taking of direct action. By analogy, in the case of a proposed 'detection of crime defence' it should only be in situations where a crime has been committed, or is in the process of being committed, that a person would be justified in gaining unauthorised access to a computer system and even then only where it was necessary for them to do so because no other realistic alternative was available to them.

3.5.36 In our view these concerns go to the very heart of this defence. Its function is to protect those who take immediate action to uncover and/or to stop an ongoing or imminent risk that crimes will be committed against themselves or others in circumstances where there is no reasonable course available to them at that particular time. In much the same way as self-defence, the law should recognise that there will be circumstances where committing an offence in order to detect or prevent the commission of further, potentially more serious, offending ought to be justified. The contours of such a defence have to be tightly drawn to ensure that it is not abused, but as the courts have shown with regard to section 3 of the 1967 Act, the common law is very much up to that task. Nevertheless, we feel that if such a defence is to be introduced into the CMA it will be important to stress in the statute itself that the invocation of the defence should be limited to situations where it is *necessary* for the defence to apply.

3.5.37 It seems to us that there is a strong argument in favour of including a 'detection/prevention of crime' defence in the CMA, in the same way that such a defence appears in the DPA 2018. There are likely to be situations where it is necessary to gain urgent access to a computer (whether a mobile telephone, a laptop, or other device) in order to detect and/or prevent the commission of a serious criminal offence, but under the law as it presently stands that access would itself be an offence. If, fearing that someone is about to commit a serious offence, it would *not* be a crime to flick through their diary or notebook in order to find out what they intend to do, it would be somewhat anomalous if it would be a crime to check their electronic

organiser or other digital device for the same purpose. Given the potentially broad meaning of the word 'computer' this would place cyber criminals at a distinct advantage when compared to their old-fashioned counterparts.

3.5.38 Following on from our analysis of any potential public interest defence, **we consider that the CMA should be amended to provide for a defence where it was necessary for a person to act in order to detect and/or prevent crime.** It seems to us that such a defence should apply to section 1 CMA and also section 3, because situations could arise where in order to prevent the imminent commission of an offence it is necessary to take the steps set out in section 3(2). We anticipate that the circumstances in which a person who acts in any of the ways contemplated by section 3(2) will be able to avail themselves of the defence will be rare, but there *could* be situations when it is vital for the protection of themselves and others from further imminent criminal offences that they so act in which case they should have the protection of the defence.

3.5.39 We are not persuaded that a detection/prevention of crime defence should be available in respect of section 2, which requires the 'accessor' to intend to commit further crimes themselves, or section 3ZA. As to the latter, where the unauthorised access gives rise to the risk of damage or disruption, and thus could result in causing more harm than the person seeking access is trying to prevent, it would be incongruous we think for the defence to apply. In those circumstances the appropriate person to take action would be law enforcement. Again, we feel there will be no need to extend a detection/prevention of crime defence to section 3A because that offence can only be committed where the person intends that an offence, inter alia, contrary to sections 1 or 3 will be committed. They would not have that state of mind unless they intended that the person carrying out those offences would not thereby be acting to detect or to prevent crime.

3.6 SUMMARY OF RECOMMENDATIONS

3.6.1 In these circumstances we believe that the changes listed below should be added to the CMA 1990. In doing so we recognise that in keeping with the form of the defences as set out in the DPA 2018, it should be made clear in any amendments to the CMA to insert a new defence that the burden of proving those defences rests on the accused person on the balance of probabilities and that where any particular defence requires that person to prove that he held a particular belief, he will have to prove not only that he honestly held that belief but that he reasonably held it as well.

3.6.2 We recommend amending the CMA 1990 as follows:

(a) Amending section 17(5) to add (c) – 'he does not reasonably believe that the person entitled to control access of the kind in question to the program or data would have consented to that access if he had known about the access and the circumstances of it, including the reasons for seeking it.'

(b) Amending section 17(5) to add (d) – 'he is not empowered by an enactment, by a rule of law, or by the order of a court or tribunal to access of the kind in question to the program or data.'

(c) Add a new section 18 in these terms:

'It will be a defence to a charge contrary to sections 1 and 3 for a person to prove that in the particular circumstances the act or acts (i) was necessary for the detection or prevention of crime, or (ii) was justified as being in the public interest.'

CHAPTER 4

GUIDANCE TO PROSECUTORS

4.1 INTRODUCTION

4.1.1 The Crown Prosecution Service (CPS) prosecutes offences under the CMA 1990, after the investigation is completed either by the police or by the National Crime Agency (NCA). The prosecutor decides whether to prosecute and does so by reaching his or her own opinion on the likelihood of conviction and the public interest in proceeding, based on the evidence passed on by the investigator. Both tests must be satisfied affirmatively for the prosecution to go ahead. The latest version of the general Code for Crown Prosecutors was promulgated in October 2018,[180] though these basic principles have been unaltered since the inception of the CPS.

4.1.2 It is common for the general guidance in the Code to be supplemented by guidance which applies to particular crimes, or to particular defendants, usually to ensure consistency in relation to issues which recur often, or perhaps to alert prosecutors to certain problems. Save in exceptional circumstances, these documents supplement and seek to apply rather than contradict the core principles in the Code itself.

4.1.3 The CPS has published guidance on cybercrime that deals with both cyber-dependent crimes and cyber-enabled crimes.[181] It is not stated when it was last updated but, notably and unlike the guidance on the Computer Misuse Act 1990, it does not refer to the Data Protection Act 2018 (DPA 2018) when such reference would be expected.

[180] CPS, *The Code for Crown Prosecutors* (Online at https://www.cps.gov.uk/publication/code-crown-prosecutors).
[181] CPS, *Cybercrime - Prosecution Guidance* (Online at https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance).

Various charges are noted in the guidance on cyber-enabled crimes. There are also notes on digital evidence gathering and joint investigation teams for cases that span a number of jurisdictions. The guidance is purely functional with no discussion of any contentious policy matters.

4.1.4 The content on cyber-dependent crimes is largely replicated in a separate guidance document on the CMA 1990, last updated on 18th December 2018.[182] For the main part, the guidance seeks to distinguish between the charging options within the CMA 1990 and seeks to ensure that readers understand the basic elements of the offences therein. Prosecutors are alerted to the possibility of alternative charges under the DPA 2018; the supply of articles in connection with fraud under the Fraud Act 2006, sections 6-7; the offence of interception of a public telecommunication system contrary to the Investigatory Powers Act 2016, section 3; and the common law offence misconduct in public office. Prosecutors are also advised to refer cases of unauthorised acts causing or creating risks of serious damage (under CMA section 3ZA) to the Special Crime Counter-Terrorism Division, where appropriate.

4.1.5 However, the latest version (2018) seems mainly to have been updated to the extent that it now refers to the offence in section 3ZA, as inserted by Serious Crime Act 2015, section 41. Reference is made to only one recent case, on sentencing, namely *Mudd*;[183] but there is no suggestion that the slight reduction in sentence in that case should influence future decisions to prosecute. There is no indication that the rest of the guidance has been reconsidered at any time recently. Possibly it was thought useful to revise the guidance in order to alert prosecutors who are considering charges under CMA section 1 to the raft of new offences in the DPA 2018, but notably nothing is said as to how prosecutors should pick between charges under the 1990 and 2018 Act, where they might have a choice. As discussed below, the guidance ignores altogether the point that the DPA 2018 contains defences which are unavailable in the CMA, and charging advice in situations where both charges would seem to be apposite should surely be available. In other words, the guidance has been updated to reflect legislative developments, but no recent policy rethinking or revision is apparent at all.

4.2 THE NEED FOR REVISED GUIDANCE

4.2.1 Since it is maintained in this project that the offence under section 1 of CMA 1990 is too wide (**Chapter 2**), and that it is unsatisfactory that no defences are provided (**Chapter 3**), it follows that we are surprised that there is no explicit public interest direction in the CPS guidance on computer misuse. It is surely wrong to think that the

[182] CPS, *Computer Misuse* (Online at https://www.cps.gov.uk/legal-guidance/computer-misuse).
[183] [2018] 1 Cr App R (S) 33 (7).

'general' criteria for assessing the public interest in bringing prosecutions in the Code for Crown Prosecutors offers sufficient guidance for the peculiarities of the offence of computer misuse. The present Code for Crown Prosecutors makes it clear, inter alia, in section 4.14 (b) that prosecutors must have regard to the culpability of the offender, as follows:

(b) The greater the suspect's level of culpability, the more likely it is that a prosecution is required.
Culpability is likely to be determined by:

i. the suspect's level of involvement;

ii. the extent to which the offending was premeditated and/or planned;

iii. the extent to which the suspect has benefitted from criminal conduct;

iv. whether the suspect has previous criminal convictions and/or out-of-court disposals and any offending whilst on bail or whilst subject to a court order;

v. whether the offending was or is likely to be continued, repeated or escalated;

vi. the suspect's age and maturity.

4.2.2 Perusal of this content would suggest that a prosecution for most cases of hacking (intentionally gaining unauthorised access) is highly likely. The conduct would often be premeditated and quite likely repeated. It is true that the low level of maturity of some suspects will be considered, as might be the fact that the offender might not be benefitting personally, but there is no indication of the relative weight that will be put on such factors. Moreover, there is nothing at all in the Code which suggests that consideration of any *good* motives, or of any positive consequences which may have arisen from the offender's activities, might be pertinent.

4.2.3 It should be acknowledged that prosecutors are not competent to rewrite the criminal law. So if, for example, our proposals for new legislative defences in **Chapter 3** were not to find favour, it would not be possible for the CPS to declare that cases where such defences would have been applicable will categorically not be prosecuted 'in the public interest'. However, more can be done in this area, whether our recommendations elsewhere in the report are taken forward or not.

4.2.4 The Netherlands has adopted prosecutorial guidelines following two high-profile incidents in 2011. Academic security researchers who found serious vulnerabilities in the Dutch public-transport chip card were investigated for having violated the Dutch criminal code on computer misuse. To avoid similar situations arising, the Dutch National Cyber Security Centre (NCSC) issued guidance for both vendors and security

researchers on responsible disclosure policy in 2013, updated in 2018.[184] This was followed by clearer guidance for prosecutors.

4.2.5 The Dutch prosecutorial guidelines contain the following three-part test:

- Were the security researcher's actions necessary within a democratic society (general interest)?
- Were the actions proportionate to the goal to be achieved?
- Could the security researcher have taken other possible courses of action that were less intrusive?

In particular, the security researcher should not use brute force attacks or compromise further the security of the system. She should also avoid copying, modifying or deleting files, the alternative, whenever possible, being to create a directory listing for the system as proof of concept of the vulnerability.

4.2.6 We are somewhat doubtful that such an approach would be possible in England and Wales. The Dutch guidelines appear to be very close to the terms of a legal defence; should the questions be answered affirmatively, non-prosecution would seem to be all but certain. In other words, they may be thought in England to be trespassing into the forbidden area of effectively rewriting the criminal law. In R (on the application of Nicklinson and AM) v Minister of Justice, DPP,[185] Lord Sumption said the following about the appropriate level of precision in prosecutorial guidance:

> 239. We are not, however, concerned with the elements of criminal liability but with the likelihood that those who have incurred criminal liability will be prosecuted. That is not a matter of definition but of discretion. The degree of clarity and precision which it is reasonable to expect of a published policy about the exercise of the prosecutorial discretion is different in at least two important respects from that which can be expected of a statutory provision creating an offence.
>
> 240. The first is that the pursuit of clarity and precision must be kept within the bounds of practicality. … It is not practically possible for guidelines to prosecutors to give a high level of assurance to persons trying to regulate their conduct if the range of mitigating or aggravating factors, or of combinations of such factors, is

[184] NCSC, *Coordinated Vulnerability Disclosure: the Guideline* (Online at https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline). See also The European Union Agency for Cybersecurity (ENISA) *Good Practice Guide on Vulnerability Disclosure* (Online at https://www.enisa.europa.eu/publications/vulnerability-disclosure).
[185] [2014] UKSC 38.

too wide and the circumstances affecting the weight to be placed on them too varied for accurate prediction to be possible in advance of the facts.

241. The second limitation is a point of principle. The pursuit of clarity and precision cannot be allowed to exceed the bounds of constitutional propriety and the rule of law itself. The Code and associated guidelines may be 'law' in the expanded sense of the word which is relevant to article 8.2 of the Convention. But they are nevertheless an exercise of executive discretion which cannot be allowed to prevail over the law enacted by Parliament. There is a fine line between, on the one hand, explaining how the discretion is exercised by reference to factors that would tend for or against prosecution; and, on the other hand, writing a charter of exemptions to guide those who are contemplating breaking the law and wish to know how far they can count on impunity in doing so. The more comprehensive and precise the guidelines are, the more likely they are to move from the first thing to the second.

4.2.7 Checklists of relevant factors (as per **4.2.1**), but without watertight indications of their weight, are therefore more typical of prosecutorial guidance. So there would be little objection to a prosecutor merely taking into account (but still better than to entirely ignore) that, on a charge under section 1 CMA, the alleged hacker was trying to detect suspected fraudulent activity and tried to minimise any risk to the security and operability of the computer system. These could be stated as factors suggesting that a prosecution would not be in the public interest, provided that due consideration was given to factors which might point the other way. These 'other' factors might include the facts of any damage actually caused and the cost of reparation, and the extent of any co-operation on the part of the accused with the police investigation. Such matters should be relevant to sentencing as well, should the offender be prosecuted and convicted (see **Chapter 5**) but they should be considered too when deciding whether to prosecute in the first place.

4.2.8 Such checklists may have altered the decision to charge Mr Dan Cuthbert under section 1 of the CMA.[186] Cuthbert was a penetration tester, someone employed to test the security of complex computer systems. On New Year's Eve 2004 he had visited a charity website and donated £30, but had become concerned at its slow response and what he had regarded as poor graphics. He thought there was a possibility that the website was a fake designed to capture and exploit his financial details. He decided to test the site, sending a simple command via his Internet browser to see whether the security settings on the charity's website would allow him to access beyond the web server root. His attempt was rejected and he felt relieved. But his test had set off an

[186] See Sommer, 'Computer Misuse Prosecutions' (2006) *Journal of the Society of Computers and Law*.

alarm in the website intrusion detection system, and he was then interviewed by the Metropolitan Police Computer Crime Unit and then charged.

4.2.9 Mr Cuthbert was convicted as charged, the court presumably finding that he must have known that he was using the website in an unauthorised fashion (which is all that the prosecution needs to prove). We do not say that the presence of an extra checklist of factors would have guaranteed that Mr Cuthbert would not have been prosecuted; indeed he was, apparently, originally uncooperative with the police investigation. But he may conceivably have been more cooperative had there been a policy document indicating that cooperation would be relevant to a decision to prosecute in a case such as his, as well as his relatively benign purposes for doing what he did.

4.2.10 The case created considerable alarm within the UK penetration testing community. Cuthbert was afraid that his conviction would result in his having to leave his line of work but in fact such was the level of sympathy expressed by the community that he continues to work in this area to this day. This, in itself, seems to challenge the wisdom of the prosecutorial decision, and helps to make the case for prosecutorial guidelines even if they cannot be quite as directive as those in the Netherlands.

4.3 THREE PARTICULAR REASONS FOR PUBLIC INTEREST GUIDANCE

4.3.1 There are three further reasons for wishing to include public interest criteria, in the form of checklists, in the guidance on computer misuse.

Public good done by some security researchers

4.3.2 It should be noted that a number of companies and public authorities publish vulnerability disclosure policies to encourage security researchers to discover and report code failures. By these policies, they generally authorise unknown security researchers to access their information systems upon certain conditions in terms of conducts undertaken for finding code failure(s) and for disclosing their findings to the controllers. The authorisation then depends on whether the conducts of the security researcher align with the description in the policy.

4.3.3 The problem is that the quality of vulnerability disclosure policies varies. Some are relatively detailed, in addition to urging security researchers to stop and report in case of doubt as to the authorisation.[187] Others are vague enough to give the impression

[187] For example, US Department of Defense, *Vulnerability disclosure policy* (Online at https://hackerone.com/deptofdefense). Discussed by reputable security expert, Krebs, 'DoD Opens .Mil to Legal Hacking, Within Limits' (2016, Online at https://krebsonsecurity.com/tag/department-of-defense/).

that security researchers can penetrate deep in the information system and access confidential (not necessarily private) information as long as there is no damage to data and/or violations of privacy.[188]

4.3.4 It is our view that security testers, upon whose services there is widespread reliance on the Internet, are entitled to greater transparency as to what will happen if it is thought that they have in fact infringed the CMA. Greater transparency of public interest decisions in such cases is capable of assisting not only suspects acting in good faith, but also those police and the NCA called upon to investigate their activities, who would prefer them to cooperate. Prosecutors, too, when faced with wide law and severe penalties under the CMA, have difficult decisions to make and risk 'over-deterring' valuable research work when prosecuting cases comparable to Mr Cuthbert.

Article 10 European Convention on Human Rights

4.3.5 Arguably, it is even more important that journalists and others who obtain material to be used for bona fide journalism should have access to guidance which helps them to assess the risk of prosecution should they need to infringe the CMA in order to obtain material. This is because such activities may presumptively engage the protections of Article 10 of the European Convention on Human Rights (ECHR), which provides:

> Article 10: Freedom of expression
>
> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of

[188] Discussed in Guinchard, 'Transforming the Computer Misuse Act 1990 to support vulnerability research. Proposal for a defence to hacking as a strategy in the fight against cybercrime' (2018) *Journal of Information Rights, Policy and Practice.*

information received in confidence, or for maintaining the authority and impartiality of the judiciary.

4.3.6 It can be argued that prosecution of the hypothetical 'hacker' would infringe his 'right to impart information … without interference by public authority' under Article 10(1) ECHR, and could only be justified under Article 10(2) if the interference were 'prescribed by law and necessary in a democratic society … in the interests of national security … prevention of crime … protection of the reputation or rights of others, [or] for preventing the disclosure of information received in confidence.'

4.3.7 The Court of Appeal has recently held that the prohibition in section 1 CMA 1990 is not incompatible with Article 10 because the information sought by hacking could instead be sought by lawful means.[189] This arguably makes a big factual assumption about the likelihood of gaining some sensitive material 'by lawful means', but in any event the decision only addresses the question of justifying the state intrusion as proportionate under Article 10(2) and nothing more than that. However, it may also be that for the offence to be 'in accordance with the law', as also required under Article 10(2), there needs to be clearer guidance as to how such cases will be considered for prosecution in the public interest.

4.3.8 This point, that the enjoyment of qualified human rights may mean that suspects should be able to make informed decisions as to their risk of prosecution, was upheld in the context of assisted suicide in R (on the application of Purdy) v DPP.[190] Neither the general Code for Crown Prosecutors, nor the more specific guidance on cybercrime, offer much guidance on the public interest element in prosecuting computer misuse (see **4.2** above). A continued failure to do so may amount to a violation of Article 10 in those cases where suspects can credibly assert to be imparting information of a public nature and concern.

Defendants who are disappointed at the decision to prosecute them cannot seek any internal review of the decision

4.3.9 Judicial review of decisions to prosecute is only exceptionally permitted and defendants are generally required instead to plead abuse of process at the outset of their trial if they believe that the prosecutor has departed from established guidance. This is a very hard argument to maintain, since courts allow prosecutors considerable room for judgment in applying their own guidelines, and even if an error can be established, defendants must still show that the decision to prosecute was

[189] *Coltman* [2018] EWCA Crim 2059.
[190] [2009] UKHL 45.

'oppressive' in all the circumstances.[191] Few examples of either decision exist and none in the field of computer misuse.

4.3.10 It follows therefore that if there are good reasons for prosecutors not to proceed in certain circumstances concerning computer misuse, on account of public interest arguments, these grounds should be addressed in the relevant prosecutorial guidance on computer misuse, in order to minimize the risk of inappropriate prosecutions.

4.3.11 A further reason to be clearer about the public interest element would be better to enable a regime of civil penalties for minor infringements which ought not to be ignored but for which prosecution seems heavy handed and/or unduly expensive. This is the subject of **Chapter 6**. However, such a regime would likely depend first on a prosecutor deciding that prosecution is not, or is not necessarily, in the public interest. So we now outline areas in which we think that the prosecutorial guidance on the offences in the CMA could usefully be supplemented.

4.4 LISTS OF FACTORS THAT SHOULD INFLUENCE CHARGES UNDER SECTIONS 1 AND 3 OF THE CMA

4.4.1 We noted above that the width of the offences in the CMA suggest that more transparency be supplied concerning when prosecution would be in the public interest. We consider this to be most important for the offences under sections 1 and 3, since it is relatively easy to prove guilt for some of these offences (in law) and yet the defendant may have had no intention to commit or assist any other criminal activity, and may even have been trying to help to prevent the same by others. We assume here that cases where a defendant is thought to have intended other criminal activity will be prosecuted instead under section 2 of the CMA.

4.4.2 **We suggest that guidance should be produced whereby lists are provided of relevant factors that point towards prosecution for an offence under sections 1 or 3 of the CMA being in the public interest and, separately, factors which point away from prosecution.** It will be recalled that this is unproblematic provided that it is not indicated how much weight should be put on the respective factors in all cases. Ideally the final list would be drawn up after consultation with security testers and companies who spend large amounts of capital in trying to defend their own security. But we start by suggesting the following:

[191] See *Moss and Son Ltd v CPS* [2012] EWHC 3658 (Admin).

4.4.3 **List of factors pointing towards prosecution:**

(i) Actual or anticipated gains by defendant in the pursuit of organised crime;
(ii) Actual losses caused by activity, whether or not anticipated, but bearing in mind that companies can in any event be expected to incur reasonable expenditure in updating computer security;
(iii) Securing or attempting to secure access in order to perform other criminal or malicious activity in pursuit of a criminal enterprise;
(iv) Use of another person's password or other activity which may incriminate an innocent person, or any act designed to conceal unauthorised access;
(v) Unauthorised acts committed to obtain private information, other than in the course of responsible journalism, securities and/or threat intelligence research;
(vi) Intention to save expenditure (in money, time or other resource) which the system owner clearly intends users to make;
(vii) Repeated unauthorised acts, and any accompanying harassment or targeting of vulnerable persons;
(viii) Any act which creates a significant risk of causing a denial or loss of service or other impairment to the system.

4.4.4 **List of factors pointing away from prosecution:**

(i) Motive to prevent crime, or to reveal security flaws and method known by the offender to be unlikely to endanger the integrity of the system;
(ii) Motive to obtain and reveal information in the course of responsible journalism, taking into account methods used and their lasting impact on victim's cybersecurity;
(iii) Motive to obtain information in the course of responsible cyber threat intelligence collection;
(iv) Co-operation with police investigation;
(v) Co-operation with agencies responsible for cyber threat intelligence;
(vi) Isolated incident, and one not intended to facilitate criminal activity or result in disclosure of confidential information;
(vii) Previous relationship between defendant and victim such that action in civil courts seemingly more appropriate.

4.4.5 This last item in para **4.4.3** (above) is intended to give guidance to the 'time lock' problem, which may lead to a charge under section 3 of the CMA. A common feature of many items of software sold to various professional markets is that after a time they cease to work unless the customer has purchased a renewal subscription. Similar

techniques are used when a trial of software is being offered – the potential purchaser can try the software with all its features for a period of a week, or a month or so, at the end of which it ceases to work unless there is a formal purchase. This technique is perfectly sound, provided that adequate notice has been given to the purchaser.

4.4.6 But arguments, ordinarily apt to be resolved in the civil courts, may arise as to when the lock should start to operate. In *Alfred Whittaker*, a software developer of bespoke software had a dispute with his customer and allowed a covert time lock to be activated which denied access to the software. This was regarded by the courts as an unauthorised modification. The defendant was convicted but given a conditional discharge.[192] We consider that such prosecutions should be considered with the viability of civil action strongly to be considered, albeit besides other relevant factors.

4.4.7 We say more below of the separate problems of young defendants, which, we consider, should be addressed separately in prosecutorial guidance.

4.5 INTERPRETATION OF THE WORD 'LIKELY' in SECTION 3A(2) OF THE CMA

4.5.1 This offence prohibits, by virtue of section 3A(2), the supply of articles which the defendant believes are 'likely' to be used in committing an offence under section 1, section 3, or section 3ZA of the Act. Regrettably, the word 'likely' is not defined in the statute and is yet to be interpreted in the courts. We consider this to be problematic, as discussed in **Chapter 2**.[193] Many hacking tools are dual-use and are indistinguishable from utilities that are essential for the maintenance and security of computers and networks. Researchers in information/cyber security, penetration testers and other professionals in the field may develop and make available such tools in the course of their study or business.[194] If these tools are then used, security and threat intelligence researchers may fear that they can be found guilty under section 3A(2).[195]

4.5.2 It is therefore important that the preferred interpretation of the word 'likely' by the CPS be considered and publicised, as reference to this is likely to the most practical step which manufacturers and researchers can take to avoid prosecution. In this area, then, it would be useful to know how the CPS interprets the law, as well as its public interest criteria, which would become relevant if it decides that the 'likelihood' threshold in law can be proven.

---

[192] See case summary in **Appendix B** (Online at http://www.computerevidence.co.uk/Cases/CMA.htm).
[193] We have gratefully borrowed here from the work of Sallavaci, 'Combating Cyber Dependent Crimes: The Legal Framework in the UK' (2017) *Communications in Computer and Information Science*.
[194] Walden, *Computer Crimes and Digital Investigations* (2nd ed, OUP, 2016).
[195] Discussed in Sommer, 'Criminalizing hacking tools' (2006) 3 *Digital Investigations* 68.

4.5.3 The CPS attempts to offer such guidance in the 2018 policy, in terms which replicate its previous policy. It provides the following list of factors to be taken into consideration:

1. Has the article been developed primarily, deliberately and for the sole purpose of committing a CMA offence (i.e. unauthorised access to computer material)?
2. Is the article available on a wide scale commercial basis and sold through legitimate channels?
3. Is the article widely used for legitimate purposes?
4. Does it have a substantial installation base?
5. What was the context in which the article was used to commit the offence compared with its original intended purpose?

4.5.4 Sallavaci suggests that the first factor in the guidance is helpful, but the remaining factors are 'somewhat problematic'.[196] She writes that 'the second factor misses the legitimate freeware tools' while articles commonly used for legitimate purposes are also commonly used for illegitimate purposes. The fourth question is a complex one, which requires professional expertise contribution on a case by case basis, whilst the introduction of 'context' could cause problems with respect to the dual use of the hacking tool.[197] Her conclusion is that the offence in section 3A should have adopted (and adapted) the wording of Article 6(2) of the Cybercrime Convention which focuses entirely on the intention of the defendant.

4.5.5 It is not open for prosecutors to rewrite the criminal law, and it seems impossible to offer an interpretation of the word 'likely' which is synonymous with the pure intentions of the defendant. Indeed, there is a separate offence in section 3A(1) where the article is made or supplied with the *intention* of facilitating other offences under the CMA. So notwithstanding the criticisms that can be made, we consider that the guidance offered by the CPS constitutes a brave attempt to cure the problem of an overly wide offence which itself can strongly be argued to be incompatible with the UK's obligations under Article 6 (2) of the Cybercrime Convention.

4.5.6 We suggest however that it is open to the CPS to advise that, primary legislation notwithstanding, prosecutors should be slow to take decisions that would put the UK in violation of its treaty obligations, and that when applying the evidential test (ie. whether there is a realistic prospect of proving guilt in law) the word 'likely' should accordingly be given a high threshold (eg. something higher than 'more likely than

[196] Sallavaci, 'Combating Cyber Dependent Crimes: The Legal Framework in the UK' (2017) *Communications in Computer and Information Science*.
[197] See Katos and Furnell, 'The security and privacy impact of criminalising the distribution of hacking tools' (2008) *Computer Fraud and Security* 9.

not'). It should also be specified that prosecutors should be slow to conclude that they have strong evidence that a maker or distributor 'believed' in the likelihood of the articles being used for criminal purposes where that person had attempted to set appropriate restrictions on the supply or availability of the item.

4.5.7 Further guidance on the public interest factors that should inform a decision whether to prosecute under section 3A(2) would also be invaluable. Where it is clear that the product was not made or supplied with the intention of facilitating crime, prosecutors should consider any unique or unusual legitimate uses to which the product might be put, so as to reduce further the risk of prosecution where a useful new product carries an acknowledged risk of misuse.

4.5.8 Other factors can surely be added, and we would encourage the CPS to develop a list in consultation with both manufacturers and senior police officers who investigate hacking and are familiar with the most commonly used tools. Evidence that suppliers and manufacturers have already sought advice from responsible sources on these matters may also be relevant in determining the need for prosecution.

4.6 OVERLAP WITH DATA PROTECTION ACT 2018

4.6.1 We noted above (**4.1**) that both the CPS guidance on cybercrime and the guidance on the CMA 1990 refer to a number of other charging possibilities (e.g., under the DPA 2018, Fraud Act 2006, etc). But nothing is said as to which charge should be preferred when a choice arises.

4.6.2 We are concerned most of all about charges being selected under the CMA in circumstances where data has been sought, and where a defence might be available had the charge been laid under the DPA 2018, by virtue of the provisions in sections 170-172 (discussed in **Chapter 3**). The CPS guidance on the DPA 2018 is also silent on the relationship between charges under the CMA and under the DPA. Our preferred solution is to legislate for defences in the CMA, but in the meantime the CPS should undertake to address the choice of charges. If legislation were not forthcoming this would indeed be the only way forward.

4.6.3 There may be cases where it makes sense to charge defendants with both offences. This is especially so where there is no possible justification for the activity. Then, a charge for a data protection offence may be said to relate to the wrongfulness of the intrusion in gaining private information, and a charge for a separate computer misuse offence might reflect any damage caused or risked to the computer system itself. But it might be thought that where charges are laid under the CMA in order to evade the defences provided for in the DPA 2018, there would be an abuse of process.

4.6.4 The leading analogous case appears to be *Asfaw*,[198] where an asylum seeker was prosecuted on two counts, one of which (using a false passport) attracted a possible application of a statutory defence for asylum seekers, which was run and on which the jury acquitted her. But the same defence was not provided for by statute in relation to the other count, attempting to obtain services (of the airline service team) by deception, even though this related to the same conduct of showing the false passport.

4.6.5 On appeal to the House of Lords, their Lordships considered the question regarding the second count of attempting to obtain services by deception. They held that the second count ought to have been stayed after the jury had decided that it accepted the (available) asylum seeker's defence on count one. Whilst their Lordships accepted that the two charges may have had different harms in mind, and could both lawfully have been prosecuted had the defence not been made out at all, they did not consider that the difference in subject matter between the offences could justify the difference in the availability of the defence. So it was held that when the defence succeeded on count one, the trial judge should then have stayed the second count.[199]

4.6.6 This leaves open the problem that may have arisen had the prosecution elected *only* to prosecute Ms Asfaw for obtaining property by deception. Seemingly, the judge would be in no position to stay the prosecution, unless the prosecutor were actually to admit that the charge had been picked purely to avoid a defence being put to the jury. Assuming, as is more likely, that the prosecution's case is that the defence would not be made out in any event, it is hard to see how the judge could properly stay the case where the more problematic charge is selected by itself.

4.6.7 It seems to us that the situation of the person charged under the CMA in circumstances where their search for data would or might attract a defence under the DPA 2018 is somewhat analogous to the situation in *Asfaw*. Article 6 of Regulation (EU) 2016/679, from which the defences in section 170 of the DPA 2018 seem to derive, requires the conduct mentioned to be treated as lawful. However, we accept that a difficult situation may arise if the financial costs of the hacking are unusually high, or where the damage to the computer might have been avoided by some other hacking technique for obtaining the information.

[198] [2008] UKHL 31.

[199] As Lord Hope indicated, at [71], this means that the defendant ought not to have been invited to plead to the second count until the outcome on the first count were known: then, if acquitted on count one, abuse of process could still be raised and should succeed.

4.6.8 Thus, **where a person has gained unauthorised access to a computer in order to seek data, and the defendant would be expected to rely upon a defence in relation to any data protection charge, we believe it would be best practice for the CPS document to advise that:**

i. the charge to be put under the Data Protection Act 2018 alone, where no serious damage was caused to the computer; or
ii. if a computer misuse offence is included, despite the absence of serious damage, prosecutors should be advised to suggest in court that the defendant should not be asked to plead at trial to the computer misuse offence until a verdict has been reached in relation to the data protection charge. Then, if acquitted (suggesting that the relevant defence has been accepted) the judge can hear submissions on abuse of process concerning the computer misuse charge, with reference to *Asfaw*;
iii. Where serious or unnecessary damage was caused to the computer, then it is still important to include the data protection charge, and the defendant may be asked to plead to them both in the usual way at the start of the trial. But an acquittal on the data protection charge should influence any sentence on the computer misuse charge; that is, assuming that gratuitous damage to the computer system was not in fact intended;
iv. In no such case should the charge be laid under the Computer Misuse Act 1990 alone.

4.7 THE TREATMENT OF YOUNG AND NEUROLOGICALLY DIVERSE SUSPECTS

4.7.1 We consider that a separate section on young suspects should also be included in prosecutorial guidelines, though it is acknowledged that in serious cases it may be more appropriate for a judge to show mercy and that therefore sentencing guidelines are of greater importance (see **Chapter 5**). The CPS guidance on prosecuting computer misuse does indirectly draw attention to the fact that a significant number of those who commit versions of the offence are autistic. The guidance mentions *Mudd*.[200] In this case, a teenage autistic defendant had devised a distributed denial of service program and distributed it to others, thus enabling 1.7 million DDoS attacks; he received approximately £250,000 for the supply of the program. A twenty-four month sentence of detention in a young offender institution was reduced to twenty-one months' detention.

4.7.2 It would be best for young suspects to be given separate treatment from neurologically diverse suspects, though it may be that some young defendants, such

[200] [2018] 1 Cr App R (S) 33 (7).

as Mudd, overlap the two categories. As we shall see, it is not yet obvious that autistic defendants need separate treatment in prosecutorial guidelines.

Young Suspects

4.7.3 The general Code for Crown Prosecutors clearly attaches weight to the age of the suspect when considering whether it is in the public interest to prosecute. By virtue of section 4.14 (b):

> The criminal justice system treats children and young people differently from adults and significant weight must be attached to the age of the suspect if they are a child or young person under 18.
>
> The best interests and welfare of the child or young person must be considered, including whether a prosecution is likely to have an adverse impact on their future prospects that is disproportionate to the seriousness of the offending.
>
> Prosecutors must have regard to the principal aim of the youth justice system, which is to prevent offending by children and young people. Prosecutors must also have regard to the obligations arising under the United Nations 1989 Convention on the Rights of the Child.
>
> Prosecutors should consider the suspect's maturity, as well as their chronological age, as young adults will continue to mature into their mid-twenties.
>
> As a starting point, the younger the suspect, the less likely it is that a prosecution is required.

4.7.4 Second, when considering the maturity of the suspect more generally, 4.14 (d) states:

> However, there may be circumstances which mean that, notwithstanding the fact that the suspect is under 18 or lacks maturity, a prosecution is in the public interest. These include where:
>
> i. the offence committed is serious;
>
> ii. the suspect's past record suggests that there are no suitable alternatives to prosecution; and
>
> iii. the absence of an admission means that out-of-court disposals that might have addressed the offending behaviour are not available.

4.7.5 This guidance, however, is of little assistance where the offence may properly be regarded as serious. Further, it is clear that police forces now pay special attention to cybercrime by juveniles, and recently the National Crime Agency has advertised its association with programmes which aim to educate young persons about the law and the potential consequences of committing an offence under the CMA. It is made clear that activities that may seem to be pranks, such as using a friend's password, without permission, to unlock their phone to look at photographs, or booting someone offline during a game, may constitute offences under sections 1 and 3 of the CMA respectively.[201] Individual police forces maintain their own sites about computer misuse by youngsters for whom hacking starts off as a game, or something to show off about to their friends, which in turn leads to liaising with unknown hackers online who give further advice about their new found hobby, and from which they may easily be tempted into assisting serious criminal activity.[202]

4.7.6 The police are now open about their maintenance of several PREVENT programmes run for young people who are known to have committed cybercrime or are likely to do so (eg. from purchases of hacking tools),[203] not dissimilar to that which operates for youngsters who may be groomed or inspired by others into encouraging, preparing or facilitating acts of terrorism. Cease and desist visits are apparently common.

4.7.7 One distinguishing feature, however, is that the cybercrime programme includes incentives not to offend. Far from being deterred from computer use altogether, participants are shown how they can use their cyber skills legitimately and have lucrative careers as security testers among other roles. This also serves a greater public interest; the National Cyber Security Centre, part of GCHQ, runs certification programmes in anticipation of the growing numbers of persons who will be needed to combat the growing threat of cybercrime worldwide, whether as part of the police or as independent security consultants.[204]

4.7.8 Naturally, such initiatives by the police are to be welcomed. However, we are still unclear what recognition is given to these programmes by prosecutors and indeed the extent of their involvement. If a young person has already committed serious criminal activity, then it seems to us that the decision how best to deal with the person should be made jointly by police and prosecutors, as would normally be the case with crimes

[201] See online at https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved.
[202] See for example the content and video at https://yhrocu.org.uk/departments/regional-cyber-crime-unit/prevent/.
[203] See Dearden, 'Child hackers who break law helped into high-flying IT jobs to turn them away from a life of cybercrime' (Independent Online, 2019).
[204] See, for example, https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/law-enforcement-and-security/certified-cyber-security-courses.

of a serious nature. But there appears to be no publicly available information regarding whom makes such decisions, nor precisely how they are made. We consider that minimal levels of transparency are yet to be attained.

4.7.9 Such guidance should be available and should address in general terms not only the initial decision to put the offender on a PREVENT programme rather than to prosecute, but also the consequences of further offences or the belated discovery of offences committed earlier than entry to the programme. We would also regard it as important to verify the level of separation between an agreement (or otherwise) by the offender to undergo training in countering cybercrime and the likelihood of prosecution for past offending.

Neurologically Diverse Suspects

4.7.10 Nothing is said in the CPS guidance on computer misuse document of neurologically diverse suspects, who in most cases have autism or are showing autistic traits.[205] Autism should be distinguished from autistic traits such as social imperviousness, directness in conversation, lack of imagination, affinity for solitude and difficulty displaying emotions.[206]

4.7.11 Despite the lack of guidance, there are a number of specific examples where mitigation has been given. These include the case of Ryan Cleary of the LulzSec hacking group (though there was the additional dimension of possession of indecent images of children), Seth Nolan McDonagh and *Glenn Mangham*.[207]

4.7.12 There is reason for caution, however. Researchers have recently suggested that whereas there is an increased risk of committing cyber-dependent crime among those with higher autistic-like traits (much of which is attributable to more advanced digital skills), there is a *decreased* risk of cyber-dependent offending among those diagnosed as autistic.[208] This is thought to be consistent with other research showing that autistic people are at least, if not more, law-abiding than the general population.

---

[205] For the purposes of this report, our definition of autism/autistic spectrum disorder refers to a diagnosis of 'persistent difficulties with social communication and social interaction' and 'restricted and repetitive patterns of behaviours, activities or interests' (this includes sensory behaviour), present since early childhood, to the extent that these 'limit and impair everyday functioning.' See https://www.autism.org.uk/about/diagnosis/criteria-changes.aspx.

[206] The distinction is carefully made in the scientific literature. See Payne, Russell, Mills, Maras, Rai, and Brosnan 'Is there a relationship between cyber-dependent crime, autistic-like traits and autism?' (2019) *Journal of Autism and Developmental Disorders*, which has informed much of this discussion.

[207] [2012] EWCA Crim 973

[208] See n206.

4.7.13 **The current research base does not provide grounds for recommending further provisions regarding autism in the CPS guidance.** To that end, a firmer link between actual autism and a propensity to be easily tempted into cyber-dependent crime is needed. Currently there seems to be better reason to suppose such a link in the case of children between immaturity and computer offending, whether or not they are autistic or display autistic like traits.

4.8 SUMMARY OF RECOMMENDATIONS

4.8.1 We consider that the CPS should offer more guidance on various aspects concerning computer misuse, and on the public interest element in particular. **We recommend that revised CPS Guidance on the CMA 1990 should:**

a) **Include a list of factors that point both towards and against prosecution for the core offences in sections 1 and 3 of the CMA (examples included at 4.4.3-4.4.4);**
b) **Should section 3A(2) continue to require belief as to a likely outcome (see our recommended narrowing of this offence in Chapter 2), the word 'likely' should be interpreted by the CPS in order to give as much reassurance as possible to responsible manufacturers and researchers;**
c) **Address the difficult charging decisions to be made where a charge could be laid in relation to the same activity both under the DPA 2018 and the CMA 1990, but where the defendant would be expected to raise one of the defences which are provided for only in the DPA 2018, sections 170-172;**
d) **Clarify the relationship between the police, NCA and CPS in making prosecutorial decisions where young defendants are thought to have committed offences of some seriousness.**

CHAPTER 5

SENTENCING

5.1 INTRODUCTION

5.1.1 This chapter examines the sentencing regime of the CMA 1990, examining various developments and amendments since its enactment (in particular the amendments to the maximum sentences). We consider the extent to which sentencing under the CMA 1990 can be said to be in need of reform. This discussion is informed by broader theories about the role of sentencing in legal reform, applicable both within and beyond computer misuse offences. These broader theoretical points are summarised in **Appendix C**.

5.1.2 Alongside our consideration of appropriate sentencing ranges, we focus in particular on the lack of Sentencing Guidelines for the CMA 1990. We believe that the creation of such guidance is an essential component of reforming the CMA 1990 as a whole, and provide some direction on how this should be taken forward.

5.2 THE CMA 1990 REGIME

5.2.1 The history of the CMA 1990, and in particular its origins in a Law Commission Working Paper, are summarised in **Chapter 1**. It is, however, useful to briefly set out an analysis of the offences, and their maximum sentences for the purposes of the discussion in this chapter.

5.2.2 The CMA 1990, as originally enacted, created three offences: an offence of unauthorised access contrary to section 1; an offence of unauthorised access with

intent to commit or facilitate the commission of further offences contrary to section 2; and an offence of unauthorised modification of computer material contrary to section 3.

5.2.3 As recommended by the Law Commission, the offence under section 1 was initially triable summarily only, albeit it was punishable by up to six months' imprisonment, rather than the maximum of three months' imprisonment recommended[209] (and greater still than the non-imprisonable offence the Law Commission had provisionally considered[210]). The two additional offences under sections 2 and 3 were both triable either way and, on enactment, both had maximum sentences of five years' imprisonment on indictment.[211]

5.2.4 Since 1990 major amendments have been made to the CMA. Sections 35 and 36 of the Police and Justice Act 2006 amended sections 1 and 3 of CMA. Section 1 became an either-way offence with a maximum sentence of two years' imprisonment. The scope of the section 3 offence was broadened, and the maximum sentence increased to ten years' imprisonment. Section 37 of the Police and Justice Act 2006 introduced section 3A of CMA making it an offence to make, supply or obtain articles for use in a section 1 or 3 offence. The new section 3A offence was triable either way with a maximum of two years' imprisonment.

5.2.5 The Serious Crime Act 2007 made minor amendments to the scope of the regime,[212] but more significant amendments followed with the Serious Crime Act 2015. Section 41 of the 2015 Act introduced section 3ZA of the CMA, making it an offence to perform an unauthorised act in respect of a computer that causes or creates a significant risk of serious damage of a material kind, either with the intention to cause such damage, or being reckless as to whether it is caused. The maximum sentence of the section 3ZA offence varies depending on the type of damage risked or caused: ordinarily it is 14 years' imprisonment but where there is serious damage to national security, or human welfare by loss of life or human illness or injury, the maximum sentence is life imprisonment.

5.2.6 The maximum sentences for the CMA offences (as amended) are as follows:

Offence	**Maximum sentence**
s.1 (access)	2 years

[209] Law Commission, *Computer Misuse* (Law Com No 186, 1989) para 3.45.
[210] Law Commission, *Computer Misuse* (Working Paper No 110, 1988) para 6.38.
[211] As per the recommendations of the Commission, paras 3.59 and 3.79.
[212] See section 61.

s.2 (access with intent)	5 years
s.3 (computer damage)	10 years
s.3ZA (causing or creating risk of serious damage)	14 years/Life[213]
s.3A (tools etc for use in CMA 1990 offences)	2 years

5.2.7 The low maximum sentences for the offences *as originally enacted* have been directly responsible for a number of the amendments to the regime, including the creation of the offence under section 3ZA. While it may have been difficult to foresee the potential damage that could be wreaked by computer misuse offences in the modern world when drafting the Act in 1990, the resulting piecemeal amendment has led to a regime with significant anomalies.

5.2.8 Many of these anomalies stem from the reactive nature of the amendments to the CMA which have predominately been designed to ensure compliance with European Union legal obligations.[214] While it is inevitable that some law reform will be reactive, it must be acknowledged that overly reactive law reform can lead to bad law. There has been a failure to consider the underlying aims of these European requirements alongside the wider CMA scheme. Similarly, there has been a failure to consider their effect in the context of the criminal law in general, and in particular the disparities they may introduce in relation to similar alternative offences. These cumulative failures have resulted in an Act crying out for reform.

Ordinal proportionality within the regime[215]

5.2.9 The most significant problem within the CMA 1990 offences from a sentencing perspective is the stark lack of ordinal proportionality within the current regime. It is tempting to blame this on European Union legal obligations, but while in a very direct

[213] Maximum sentence of 14 years' imprisonment unless the offence was committed by way of an act causing or creating a significant risk of serious damage to national security or to human welfare (by way of loss to human life or causing human illness or injury): CMA 1990, s3ZA(6), (7).

[214] Section 3ZA of the CMA 1990 was introduced in order to ensure compliance with Directive 2013/40/EU on attacks against information systems; and the amendments to the maximum sentence of section 1 by the Police and Justice Act 2006, s35(3) was required for compliance with Council Framework Decision 2005/222/JHA on attacks against information systems.

[215] 'Ordinal proportionality requires that a penalty should be proportionate to the gravity of the offence for which it is imposed. Those convicted of grave crimes ought to have correspondingly severe sentences, and those convicted of less grave crimes ought to have correspondingly less severe sentences. It is thus a relative concept.' Kelly, 'Reforming maximum sentences and respecting ordinal proportionality' [2018] *CrimLR* 450, 451.

way these issues can be partially attributed to these requirements, the relevant Directives and Decisions require only that states provide a certain minimum standard of criminalisation. It has always been open to parliament to provide for higher maximum sentences (and criminalisation) than that mandated by European Union law, and in fact, while the section 3ZA offence was driven by Directive 2013/40/EU that directive required only a maximum sentence of five years' imprisonment and that such offending be punishable by 'effective, proportionate and dissuasive criminal penalties'. It would have been open to parliament here to simply make no amendment to CMA 1990 at all.

5.2.10 As we discuss in **Appendix C**, examining the ordinal proportionality of a regime requires at least a brief consideration of the different offence models chosen, and the wrongs being targeted. Ensuring ordinal proportionality is always trickier when offences target different wrongs or adopt drastically different models. It is quite easy to compare offences such as sexual assault contrary to section 3 of the Sexual Offences Act 2003 and sexual assault by penetration contrary to section 2 of that Act. The basic wrongs being targeted are the same, and the penetration of another is clearly more serious than non-penetrative touching. In contrast, it can be exceptionally difficult to compare the seriousness of offences that target completely different wrongs. Comparing rape to burglary, for example, is arguably like comparing apples to oranges.

5.2.11 The CMA 1990 is particularly problematic here in that every offence targets a different wrong. It is therefore useful to compare each CMA 1990 offence with a similar offence of the same type, before being compared for ordinal proportionality (within the CMA scheme)?

5.2.12 The offence under section 1 is a simple 'access' offence.[216] The offence is completed simply by performing a function with intent to secure access, regardless of whether access is in fact successfully achieved. The wrong targeted by the offence is the unauthorised access of computer programs or data. No malicious intent is required: simply an intention to secure access.

5.2.13 The offence under section 2 is an aggravated/pre-inchoate type offence.[217] It is committed by committing a section 1 offence with a particular, more serious, *mens rea*: an intent to commit or facilitate the commission of an offence with a maximum sentence of more than 5 years' imprisonment. The primary wrong targeted is the commission of further, serious, criminal offences.

[216] Law Commission, *Computer Misuse* (Law Com No 186, 1989) paras 2.10-2.15 and 3.4-3.12.
[217] The Law Commission report leading to the offence compared the offence closely to that of attempt. Ibid. paras 3.49-3.60.

5.2.14 The offence under section 3 is a 'criminal damage' type offence.[218] It is completed by committing an unauthorised act either with an intention to impair the operation of, or access to, a computer, or a program or data held on a computer. While the act must be unauthorised, the wrong targeted by the offence is damage to computers, programs or data. In this respect it is analogous to the offence of criminal damage contrary to section 1 of the Criminal Damage Act 1971 which prohibits the destruction or damage of property belonging to another (intentionally or recklessly) without lawful excuse. It is worth noting however that the section 3 offence is a conduct crime, rather than a result crime (as criminal damage is), as the computer, program or data does not actually need to be impaired.

5.2.15 The offence under section 3ZA is concerned with the 'national interest'. It requires an individual to commit an unauthorised act that causes or creates a significant risk of serious damage of a material kind, either with an intention to cause serious damage of a material kind, or being reckless as to whether such damage is caused. Damage of a material kind includes damage loss of life, human illness or injury, damage to the environment of any place; to the economy of any country; to the national security of any country or disruption to a system of communication or transport. The wrong targeted is of course such damage being caused or risked.

5.2.16 The offence under section 3A is a combination of a 'middle man'[219] type offence and a 'pre-inchoate' offence.[220] It is committed by making, adapting, supplying, or obtaining articles with either an intent to use it for a CMA offence, believing it will be used in a CMA offence, or for further supply for use in a CMA offence. The explanatory notes to the Police and Justice Act 2006 explain that the wrong targeted here is the creation and provision of such tools, which aid the commission of CMA offences and organised crime and for which a secondary market has arisen.[221]

5.2.17 Reflective of the different wrongs targeted are the different models of criminalisation adopted by the regime. The offences under sections 1 to 3 are all conduct offences. For all three the only *actus reus* requirement is the unauthorised access of a computer. For the section 1 offence this access must simply be intentional; for the section 2 offence it must be intentional and there must be an intention to commit or facilitate a further qualifying offence; and for the section 3 offence the access must be intentional and the offender must either intend, or be reckless, to impairing the operation of a computer, program or data. Despite the section 3 offence being billed

[218] The Law Commission report leading to the offence directly acknowledged this basis, and discussed the difficulties of simply amending the existing offence of criminal damage to deal with such behaviour. Ibid. paras 3.61-3.64 and 3.78.
[219] Ormerod and Laird, *Smith, Hogan and Ormerod's Criminal Law* (15th edn, OUP, 2018), 1114.
[220] In a similar manner to the offence under section 2.
[221] Explanatory Notes to the Police and Justice Act 2006, paras 302-303.

as a 'criminal damage' offence, in contrast to the offence under section 1 of the Criminal Damage Act 1971, the offence under section 3 is complete as soon as the act is committed, regardless of whether the operation of, or access to, a computer or a relevant program or data is in fact impaired. The result of these offence models is that the harm threshold for the commission of all the offences is very low, ensuring that the behaviour caught by each offence covers a wide range of seriousness.

5.2.18 In contrast, the offence under section 3ZA is a result-based offence and has a much higher harm threshold, requiring that the act causes, or creates a significant risk of, serious damage. It has a similarly high *mens rea* requirement, requiring not just intention to do the act but also intention or recklessness as to the serious damage. The offence under section 3A of making, supplying, adopting, or obtaining articles sits separately still. It is a risk-based offence with a particularly low *mens rea* requirement: the offence can be committed merely if the offender thinks it is likely the article will be used in a CMA offence, in contrast to the offences under sections 1 and 2 which require intention. As with the offences in sections 1, 2 or 3, however, the offence is complete where there is such a belief, even if in fact there is no chance of anyone using the article in a CMA offence. The *actus reus* amounts merely to supplying, offering, making or obtaining a computer program or data; and there is no requirement that said computer program or data be anyway effective in the commission of a computer misuse offence.

5.2.19 Thus, while all the offences are *prima facie* similar computer misuse offences, aimed at the social wrongs that can be caused by computer misuse, a closer analysis reveals a more complex and nuanced story. For example, are the offences under sections 1 or 2 best characterised as trespass offences, or is the section 2 offence truly a pre-inchoate offence? Are both better considered together with the offence under section 3 as offences of interfering with property?

5.2.20 The primary issue for our purposes is that because the offences are all aimed at subtly different wrongs, the range of seriousness for each of these offences is overlapping. Let us again consider current maximum sentences:

Offence	**Maximum sentence**
s.1 (access)	2 years
s.2 (access with intent)	5 years
s.3 (computer damage)	10 years
s.3ZA (causing or creating risk of serious damage)	14 years/Life

s.3A (tools etc for use in CMA 1990 offences)	2 years

5.2.21 At first glance, the maximum sentences for these offences do not seem to present significant issues of ordinal proportionality. An average 'access' offence under section 1 will of course require a less severe sentence than an offence under section 3 that impairs the computer accessed. However, it must be remembered that these offences are targeted at differing wrongs. Unlike, for example, offences of assault under the Offences against the Person Act 1861 which can be easily categorised with a cleanly increasing line of seriousness (i.e. assault, assault occasioning actual bodily harm, assault occasioning grievous bodily harm, causing grievous bodily harm with intent), the CMA offences cannot be neatly categorised in order of seriousness.[222]

5.2.22 There is an exceptionally wide range of seriousness for each offence within the CMA regime. While this is a questionable model of criminalisation in principle, it is not necessarily problematic in practice, provided that the maximum sentences are sufficiently high so as to allow for the most serious type of offending to be properly marked. In fact, it is not, practically speaking, necessarily problematic even where the most serious type of one offence is more serious than the average seriousness of another offence with a higher maximum sentence. An example here might be perverting the course of justice (maximum sentence of life imprisonment but with an average perhaps somewhere in the region of 12 months for a single offence) and causing death by dangerous driving (maximum sentence 14 years' imprisonment but with an average sentence of somewhere in the range of 6 years' imprisonment).[223]

5.2.23 Issues in practice do arise, however, where the maximum sentence for an offence is too low, and does not leave sufficient room to mark the most serious types of that offence; where the presence of a single additional factor has a disproportionate effect on the maximum sentence that can be imposed; or where the offences differ to an extent that ordinal proportionality comparisons are hard to make. A further point arises in practice when one considers how a sentencing court is to determine the seriousness of the offence. To continue with the above example, how is a judge to know that the 'going rate' for an ordinary offence of perverting the course of justice

[222] However, as the Law Commission has noted, even in the Offences against the Person Act the hierarchy of offences is not as clear as first appears: (1) the maximum sentence for sections 20 (malicious wounding or grievous bodily harm) and 47 (actual bodily harm) is the same at five years' imprisonment; and (2) the special status given to wounding by sections 18 and 20 means that offences are not clearly distinguished by the seriousness of the harm caused, as a wound can be a relatively minor form of harm. Law Commission, *Reform of Offences against the Person* (Law Com No 361, 2015) para 3.4.

[223] These figures are anecdotal and illustrative but reflect our understanding of sentencing practice for these offences.

is approximately 12 months, but for an ordinary offence of causing death by dangerous driving it is approximately 6 years?

5.2.24 Unfortunately, the CMA is a prime example of a regime where there are such difficulties with determining the proportionate sentence in a given case without further assistance, say, in the form of an offence-specific sentencing guideline or a guideline case from the Court of Appeal (Criminal Division).

5.2.25 Take, for example, an offender who breaches a large multinational company's security system and gains access to information worth millions of pounds due to its confidential nature (perhaps a proprietary blend of 11 herbs and spices). The offender then leaks that information to the public at large causing a significant financial loss to the company. In doing so the offender did not attempt to profit personally, or to commit any other offence. If the offender had done so by using a computer program that impaired the operation of the company's security system temporarily, so as to grant him access, he would be guilty of the section 3 offence for which the maximum sentence is 10 years' imprisonment. If the offence was committed by identifying a user who wrote down their passwords and accessing those notes, without permission, at an opportune moment, and no computer program or data had to be impaired in the course of the offence, he would be guilty of the section 1 offence for which the maximum sentence is 2 years' imprisonment. In both of these hypothetical cases the offender intentionally exploited a system to cause very significant harm to the victim. The offender's culpability may arguably differ slightly in the two cases, the use of a computer program may, for example, have required more planning and could be interpreted as a more deliberate attack. It may even be that the offender in the section 1 example is more culpable than that committing the section 3 offence – for example the section 1 offender may be an employee engaging in a significant breach of trust, whereas it is possible the section 3 offender is a teenager experimenting with off-the-shelf software. The arbitrary difference in the maximum available sentence that results is, however, clearly unsatisfactory and unfair, from both the perspective of a victim and the wider public (who may feel justice has not been served by a disproportionately low sentence) and that of the offender (who may be liable to a far more severe sentence simply by virtue of having committed their offence in a slightly different manner).

5.2.26 A key question is whether or not the differences in the maximum sentences can be justified by reference to a special social need to punish or deter a certain kind of wrong. The offences under sections 1 and 3 appear to have an enhanced focus upon harm caused or risked (which may well be justifiable) and as a result instances where there is high culpability but low harm caused or risked may be under-sentenced. This is at odds with the approach to sentencing in, for example, cases of drug importation

where the substance is not in fact a controlled drug; in such cases, where there is high culpability but low harm, condign punishment will often still follow. What this illustrates is, perhaps, that the wrongs that the individual CMA offences are aimed at have not been sufficiently theorised.

5.2.27 The offence under section 3ZA, by way of contrast, separates itself cleanly from the offences in sections 1 to 3, requiring not just a significantly higher *mens rea* – an intent to cause serious damage of a material kind or being reckless as to whether such damage is caused – but also a higher *actus reus*, namely that the act causes, or creates a significant risk of, serious damage of a material kind. The distinction between the maximum sentence of ten years' imprisonment for the section 3 offence and life imprisonment for the section 3ZA offence is therefore far more justifiable.

5.2.28 In light of this analysis, **we do not recommend changes to the current maximum sentences applicable within the CMA 1990.** However, we raise concerns about a lack of guidance (relevant to **5.5** below), and we highlight the need for proportionality considerations in future reviews of the statute.

5.3 THE ABSENCE OF GUIDELINES

5.3.1 While sentencing guidelines (at least in the form now issued by the Sentencing Council) are a relatively new feature of English criminal law, their importance in ensuring greater consistency in sentencing, and in reducing unwarranted disparity is now widely recognised.[224] They help to identify factors pertinent to culpability and harm, and provide sentencing ranges and starting points thereby structuring judicial discretion. This promotes a consistent approach to sentencing thereby increasing the consistency of sentencing outcomes. As foreshadowed above, there are at present no sentencing guidelines issued by the Sentencing Council for the offences under the CMA 1990.

5.3.2 Particularly pertinently for the CMA regime, sentencing guidelines can also create a greater degree of ordinal proportionality between offences, even where maximum sentences are out of kilter, by achieving more proportionate sentencing ranges. Take, for example, the Assault Guideline issued by the Sentencing Council.[225] While the maximum sentence is 5 years' imprisonment for both assault occasioning actual bodily

[224] Pina-Sanchez and Linacre, 'Enhancing Consistency in Sentencing: Exploring the Effects of Guidelines in England and Wales' 30(4) (2014) *Journal of Quantitative Criminology*, 731. See also more generally, Ashworth and Roberts (eds), *Sentencing Guidelines: Exploring the English Model* (OUP, 2013).
[225] Sentencing Council, *Assault: Definitive Guideline* (June 2011).

harm,[226] and for inflicting grievous bodily harm,[227] the guideline category ranges reflect the increased severity of the grievous bodily harm offence. The guideline range for assault occasioning actual bodily harm is a fine to 3 years' custody,[228] and the guideline range for inflicting grievous bodily harm is a community order to 4 years' custody.[229] The effectiveness of this will, of course, always be blunted where maximum sentences are disproportionately low; by way of contrast the guideline range for inflicting grievous bodily harm with intent,[230] which carries a maximum sentence of life imprisonment, is 3 years' custody to 16 years' custody. However, guidelines can still mitigate the effects of disproportionate maximum sentences in some ways, and perhaps crucially, do not require further legislative reform.

5.3.3 Such a task is comparatively easy with a genus of offences such as assaults against the person, as the wrongs targeted are broadly the same. By contrast, the differences in the wrongs the CMA regime aims to address, and the models adopted by the various offences, make sentencing these offences particularly challenging, as discussed above. For example, given that the offences contrary to sections 1, 2 and 3 are conduct-based offences presumably any case in which damage or a negative consequence in fact occurs these must be significantly aggravating factors. What role is culpability to play in relation to the intention of that harm, and what weight is to be given to differing types of harm? The difficulty of sentencing such offences is exacerbated by the additional factual complexities that these cases raise in practice.

5.3.4 Many cases involve particularly young and immature offenders, and a number are complicated by the presence of autism.[231] It is difficult for courts to assess the extent of any impairment or immaturity and its impact on the offender's culpability in the individual circumstances on the case. Courts are often required to consider detailed and complex expert reports in an area they have limited prior experience in to do so. Moreover, such cases also raise particularly difficult questions about the competing purposes of sentencing, and the extent to which the rights and needs of the offender, and the desire to ensure effective rehabilitation, must be balanced against the need for punishment, deterrence and public protection.

5.3.5 As Penny Cooper has argued, there is a shortage of research on the impacts of various sentences on those with autism,[232] and as a result the courts also have limited resources available to them in order to properly understand how best to address the

[226] Contrary to section 47 of the Offences against the Person Act 1861.
[227] Contrary to section 20 of the Offences against the Person Act 1861.
[228] Sentencing Council, *Assault: Definitive Guideline* (June 2011) 12.
[229] Ibid. 8.
[230] Contrary to section 18 of the Offences against the Person Act 1861.
[231] See, for example, *Mudd* [2017] EWCA Crim 1395.
[232] Cooper, 'Sentencing: Autism Spectrum Disorder - R. v Mudd (Adam Lewis)' (2018) *CrimLR* 243.

offending (discussed at **Chapter 4.7**). Further, such offenders may present differently than expected to the court and probation officers, and may have limited ability to process their actions and their impact.[233]

5.3.6 These difficulties are only further exacerbated by how easy it is for offenders to cause significant harm by way of computer misuse offences. A young offender could inadvertently cause serious financial loss to a company while engaging in what he considers to be a fun intellectual challenge. Should this high risk of damage lead to an overall increase in sentencing either on a simple proportionality basis or for deterrence purposes; should it decrease the sentences in recognition of the likelihood of lower culpability than would normally be expected in relation to an offence causing such significant harm; or does the increase in harm (interpreted as caused, risked or foreseen) balance out the reduction in culpability?

5.3.7 In *Mangham*,[234] the Court of Appeal, having considered a number of previous authorities, attempted to provide some guidance as to the proper approach to sentencing CMA offences, identifying a number of relevant factors that will bear on sentence:[235]

(1) Whether the offence is planned and persistent;
(2) The nature of the damage caused to the system;
(3) The nature of the damage caused to the wider public interest such as national security, individual privacy, public confidence and commercial confidentiality (whether or not information received is passed on to others will be a particular factor here);
(4) The motive (revenge will be a serious aggravating factor);
(5) The benefit (where the offence was motivated by financial benefit by the sale of information that will be a serious aggravating factor; similarly the value of the intellectual property will be relevant to both benefit and damage); and
(6) The psychological profile of the offender.

5.3.8 *Mangham* provides valuable guidance and structure to the sentencing of CMA offences, helping to identify the primary factors that will inform an assessment of the seriousness of an offence, and providing guidance as to factors that will be considered particularly relevant or aggravating. However, its value is ultimately limited in that it does not attempt to provide any guidance as to the appropriate sentencing levels for the CMA offences, nor does it offer guidance as to the quantification of the listed

[233] Cea, 'Autism and the Criminal Defendant' (2014) 88 *St John's Law Review* 495.
[234] [2012] EWCA Crim 973.
[235] Ibid, [19].

factors. This requires those involved in the sentencing of such offences to rely on previously reported sentences and decisions and to try to draw comparisons with appropriate sentences for other similar offences. Reliance on previously reported sentences and decisions is particularly difficult in relation to CMA offences due to the rarity of their prosecution (see **Appendix B**) and the differing wrongs the CMA offences target; and, further, is a practice that has drawn the ire of the Court of Appeal.[236] Moreover, comparisons with other similar offences are particularly difficult in relation to offences under the CMA regime due to the CMA regime's low maximum sentences.

5.3.9 The shortcomings of *Mangham* were, unfortunately, further exacerbated by the decision in *Martin*.[237] The court in *Martin* held that the capacity for harm, and the wider implication for society at large, of the CMA offences was great, and that accordingly the sentences for such offences must involve a real element of deterrence. The sentence in *Mangham*, handed down a mere 15 months earlier, or any of the older decisions of the court, could no longer be taken to be representative of the appropriate sentencing range for CMA offences. In the opinion of the court in *Martin*, sentences for such offences would now, in the ordinary course of things, attract longer sentences: measured in years rather than months.

5.3.10 The effect of the *Martin* decision is in essence to render any previously imposed sentences for CMA offences useful only as minimum benchmarks. While it gives some guidance as to appropriate sentence levels in that it notes that sentences are likely to be longer than those that have previously been imposed, and that they ought to be in years not months, it does not give any real guidance as to how much greater they ought to be. The difficulties presented by the decision in *Martin* are further exacerbated by the fact that since the decision in that case there have been only a small number of cases that have come before the Court of Appeal. Moreover, the Court of Appeal has depreciated the use of guidelines for other similar offences, such as fraud, on the grounds of the different harms the offences focus on and the differing *mens rea* requirements and maximum sentences.[238] Sentencers are then largely adrift in relation to offences under the CMA regime, a regrettable state of affairs which will undoubtedly lead to inconsistent sentencing.

5.3.11 A guideline would undoubtedly bring a degree of clarity and consistency to the sentencing of such offences which is currently lacking. This raises the question as to whether or not the Council, in producing a guideline, ought to produce a distinct guideline for young offenders. This approach has been adopted in the case of sexual

[236] See, for example, *Thelwall* [2016] EWCA Crim 1755.
[237] [2013] EWCA Crim 1420.
[238] See, *R (Pensions Regulator) v Workchain Ltd* [2019] EWCA Crim 1422.

offences, robbery offences and bladed articles and offensive weapons. In other cases, offence-specific guidelines apply to those aged 18 or over only; sentencers are left to apply the overarching guidelines for children and young persons, which is (by its nature) not specific to the particular offence.

5.3.12 It is clear that young offenders convicted of CMA offences present particular issues which may not be present, or may not be as prevalent, in cases involving non-CMA offences. While the occurrence of such offences is low, and even lower for those aged under 18, there appears to be a strong case for a specific guideline which can cater for the specific issues often raised by young persons convicted of these offences. Indeed, the rarer a particular occurrence, the greater the need for guidance as courts cannot rely on experience or intuition to arrive at an appropriate disposal. **We therefore recommend the creation of an offence-specific sentencing guideline for CMA offences, including specific consideration of sentencing children and young offenders.**

5.4 ANCILLARY ORDERS

5.4.1 The CMA regime is well catered for in terms of ancillary preventative orders, a number of which are available when sentencing offenders convicted of CMA offences.

5.4.2 Under section 19 of the Serious Crime Act 2007, where an offender is being sentenced in the Crown Court the court may, if it has reasonable grounds to believe that the order would protect the public by preventing, restricting or disrupting the offender's involvement in serious crime in England and Wales,[239] make a serious crime prevention order. A serious crime prevention order may contain any such prohibitions, restrictions or requirements as the court considers appropriate for this purpose. This includes significant restrictions on the offender's ability to use, possess or come into contact with computers and telephones.[240]

5.4.3 Similarly, under section 22 of the Anti-social Behaviour, Crime and Policing Act 2015, where the offending caused, or was likely to cause, harassment, alarm or distress the court may, for the purpose of preventing the offender from engaging in such behaviour, make an order prohibiting or requiring the offender from doing anything described in the order.

[239] That is the facilitation or commission of offences listed in Part 1 of Schedule 1 to the Serious Crime Act 2007 (which includes all offences under the CMA).
[240] See, for example, *McGrath* [2017] EWCA Crim 1945 and *Strong* [2017] EWCA Crim 999.

5.4.4 The only notable legislative gap is in relation to sexual harm prevention orders under the Sexual Offences Act 2003. Sexual harm prevention orders are available where an offender is convicted of an offence listed in either Schedule 3 or 5 of the Sexual Offences Act 2003 and the court is satisfied that it is necessary to make a sexual harm prevention order to protect the public from sexual harm by the offender, or to protect children or vulnerable adults from sexual harm from the defendant outside the United Kingdom.[241] Schedule 3 lists a series of sexual offences and Schedule 5 lists a series of non-sexual offences. A sexual harm prevention order may prohibit an offender from doing anything described in the order, including imposing significant and severe restrictions on the use of computers and telephones.[242] CMA offences are not, however, listed in Schedule 5 to the 2003 Act. In the modern world, where increasing sexual interactions occur online and where sexual images are stored electronically, this seems odd. Take the example of an offender who commits a section 1 access offence with intent to obtain private sexual images, and to then disclose such images in contravention of section 33 of the Criminal Justice and Courts Act 2015.[243] Simply because they were unsuccessful, and only charged under the section 1 offence, should not properly be able to prevent the court in an appropriate case from imposing a sexual harm prevention order. Similarly, consider an offender who takes steps to improperly impair computer monitoring software, with the intent to obtain child pornography unmonitored, and is caught prior to taking active steps to obtaining such pornography and is accordingly charged only under section 3 of CMA. Their lack of success in causing sexual harm on this occasion should not restrict the court from taking appropriate preventative steps.

5.4.5 Perhaps unsurprisingly then, considering the numerous different varieties of existing preventative order, and their broad natures, it does not seem like the CMA regime would benefit further from a bespoke preventative order. Where the continuing threat is further CMA offending a serious crime prevention order is available to the Crown Court in sufficiently serious cases. Similarly, where the behaviour is simply at a low level causing harassment, alarm or distress a criminal behaviour order will be available. **There is, however, an odd legislative gap in relation to sexual harm prevention orders and we recommend that the CMA offences should be added to the list of relevant offences for which such orders are available.**

5.4.6 In practice though, the more significant issue in relation to preventative orders for CMA offending is how they are used. Ensuring prohibitions on the use of computers and technology are effective and proportionate is particularly difficult. As has been

[241] Sexual Offences Act 2003, s103A.
[242] See, for a recent case discussing such restrictions, *Parsons* [2017] EWCA Crim 2163.
[243] The offence under section 33 of the Criminal Justice and Courts Act 2015 has a maximum sentence of 2 years' imprisonment and so this offending would not fall within section 2 of the CMA 1990.

noted in the context of sexual harm prevention orders, the use of the internet and internet-enabled devices is now an integral part of daily living and blanket bans on the use of the internet, of cloud-enabled devices or of encryption, will only in the most exceptional cases be justifiable and proportionate.[244] Similarly, requirements that police approve the use of individual devices, or install monitoring software on them prior to use are simply impractical given the realities of police time and resources.[245] The result is that prohibitions on the use of the internet and internet enabled devices must be very carefully and precisely drafted – a difficult task for courts without a particular expertise in the subject – and are inevitably limited in their ability to address the risk of further CMA offending.

5.4.7 This is not an issue that can (or should) be solved by legislative reform of the scope of preventative orders. Any order imposing blanket bans on internet use would likely breach an offender's right to private life under Article 8. However, it does mean that more careful consideration needs to be given to how to ensure effective ancillary orders. In particular, it is suggested that effectively addressing CMA offending requires a greater use of mandatory requirements in ancillary orders, focussed on changing behaviour, increasing the offender's understanding of the harms of their offending, and helping offenders find productive ways to engage their skills. This is, of course, more expensive, and in many areas, it is likely that such programmes are not currently available. This is a regrettable state of affairs. **It is also recommended that guidance be issued to the courts on the use of ancillary orders, focussing not just on common pitfalls to avoid, but also giving examples of effective prohibitions and requirements to courts who are unlikely to have significant expertise in this complex area.**

5.4.8 We explore the potential for broader use of civil penalties, as opposed to ancillary orders, in **Chapter 6**.

5.5 CONCLUSIONS

5.5.1 In this chapter we have sought to raise questions as to the need to reform the CMA 1990. The current regime suffers from disproportionate maximum sentences with the inevitable result of inconsistent sentences (both as compared with the offences within the CMA 1990 and beyond). We believe that this is best met through the creation of new CMA specific sentencing guidelines.

5.5.2 A guideline would provide structure to the sentencing decisions under the CMA 1990 and could help mitigate some of the issues raised by the current regime. Further, the

[244] See, *Smith* [2011] EWCA Crim 1772 and *Parsons*; *Morgan* [2017] EWCA Crim 2163.
[245] See, *Hewitt* [2018] EWCA Crim 2309.

guideline could go further than current offence-based sentencing guidelines. Appropriate terms of ancillary orders could be suggested, for instance, the monitoring of internet use or access, or a prohibition on purchasing items which are commonly associated with hacking or similar activity targeted by the regime.

5.6 SUMMARY OF RECOMMENDATIONS

5.6.1 We recommend that:

- **The Sentencing Council should produce an offence-specific guideline for CMA 1990 offences;**
- **Consideration should be given to producing a specific children and young persons guideline;**
- **Both the adult and children and young persons guidelines should expressly deal with autism and Asperger syndrome;**
- **New guidance should be issued for sentencers addressing how to draft preventative orders that effectively tackle CMA offending, providing examples of effective and proportionate prohibitions and requirements to courts who are unlikely to have significant expertise in this complex area; and**
- **CMA 1990 offences ought to be added to Schedule 5 of the Sexual Offences Act 2003 enabling a court to impose a sexual harm prevention order on conviction in appropriate cases.**

CHAPTER 6

THE SHORT CASE FOR THE INTRODUCTION OF CIVIL PENALTIES

6.1 INTRODUCTION

6.1.1 The creation of a statutory scheme of civil penalties that is capable of operating in parallel with criminal sanctions is of relatively recent origin, although the principle can be traced back to the Factories Act 1833. The earliest reference to a 'monetary penalty' on the United Kingdom legislation website is in 1993 following the introduction of the Hearing Aid Council Monetary Penalty (Increase) Order, which increased the pre-existing sanction in the parent Hearing Aid Council Act 1968, from £1,000 to £5,000. The imposition of the monetary penalty was a form a disciplinary sanction. The 1968 Act was subsequently repealed by the Health and Social Care Act 2008, which, in similar vein, created a scheme of fixed penalty notices. The penalty notice was imposed by the regulator, the Quality Care Commission, and offered 'the person the opportunity of discharging any liability to conviction for the offence to which the notice relates by payment of a penalty in accordance with the notice.'[246]

6.1.2 There are many examples of regulators being empowered to impose financial penalties on the organisations that fall under their compass. The most pervasive regulatory provision for the imposition of civil penalties is the Regulatory Enforcement and Sanctions Act 2008. This empowers designated regulators to impose fixed monetary penalties under sections 39-41 of the Act in respect of certain offences as an alternative to the institution of criminal proceedings.

6.1.3 Following the introduction of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, the Data Protection Act 1998 was amended so as to provide for the imposition of a Monetary Penalty Notice (MPN). A notice could be issued by the Information Commissioner where (i) there had been a serious contravention of the data protection principles under the 1998 Act, (ii) the

[246] Health and Social Care Act 2008, s86(3).

contravention was likely to cause substantial damage or distress, and (iii) either the contravention was deliberate, or the data controller ought to have known of the risk of contravention and damage but failed to take reasonable steps to prevent the breach. The upper limit of the penalty was £500,000. The Data Protection Act 2018 includes in sections 155 to 159 provision for a range of penalty notices.

6.1.4 The Investigatory Powers Act 2016 (IPA), section 7 and Schedule 1, also makes provision for the imposition of an MPN by the Investigatory Powers Commissioner. The imposition of an MPN under the IPA is limited to the interception of communications. However, interception can include equipment interference where this provides access to stored communications. The IPA, as the Code of Practice on Equipment Interference makes clear at paragraph 1.1, 'provides a statutory framework for authorising equipment interference when the European Convention of Human Rights (ECHR) and/or the Computer Misuse Act 1990 (CMA) are likely to be engaged.' In limited circumstances, an MPN can be issued where computer misuse falling short of an offence occurs (on the basis of an absence of intent) and no lawful authority exists for doing so. This short paper discusses the case for wider application of civil penalties in the context of computer misuse more generally and how this might operate.

6.2 CIVIL PENALTIES AND THE CMA 1990

6.2.1 The principal characteristic of the current schemes where MPNs are imposed are generally regulatory in nature. But as Garoupa and others have noted, the 'reasons for different arrangements in the criminal justice and regulatory spheres are not obvious, given in particular that the criminal justice system plays an important part in regulatory enforcement.'[247] It has been suggested that the distinction arises because of a difference in imperatives between prosecutors and investigators: the former is concerned with evidence an offence has been committed and whether this is sufficient to secure a conviction, whereas the latter is preoccupied with the offender's profile and compliance behaviour. This may or may not be a correct analysis, but it would certainly identify a tension between the role of the integrated regulator as both investigator and prosecutor. With the exception of the Investigatory Powers Commissioner, those regulators referred to so far are also empowered to prosecute offences. Other than where computer misuse arises in the context of the deployment of covert investigatory powers without lawful authority, no independent regulator

[247] Garoupa, Ogus and Sanders, 'The Investigation and Prosecution of Regulatory Offences: Is there an Economic Case for Integration' (2011) 70(1) *Cambridge Law Journal,* 229–259.

exists to undertake oversight of those engaging in activities that might constitute offences under the CMA 1990.

6.2.2 The absence of a regulator should not be determinative of the case for the introduction of a monetary penalties regime. If the underlying rationale for their existence is compliance (and in some cases, the absence of criminal intent where non-compliance would otherwise constitute an offence) then it is this that should influence whether legislative reform could include the imposition of fines. This report highlights groups that have a considerable public interest in engaging in activities that could constitute offences under the CMA 1990: investigators (who have some limited protection from liability), technicians, journalists and academic researchers; but there others, including internet service providers and social networking sites. If any person from these groups commits an offence under the CMA 1990, the state is left with a stark choice: to either prosecute or not.

6.2.3 Garoupa and others identify a number of advantages and disadvantages that arise from the integration of investigatory and prosecutorial functions.[248] Benefits include, a possible reduction in costs, specialisation, fast track intervention and 'monopoly power' (single agency bargaining leverage viz a viz a defendant or defendants). On the other hand, there is an increased risk of error costs (arising out of the poor exercise of prosecutorial judgment), a dilution of accountability and behavioural effects (as distinct from professional law enforcement officers). Their thesis develops an economic framework based on these factors predicated on the underlying logic that 'different types of crime and the behaviours that give rise to them impact differentially on society; thus enforcement policy and practice (broadly defined) should vary from one type of crime or offence to another.'[249] These, not the architectural constraints of existing legislation, should be the drivers for possible reform.

6.2.4 The groups identified in this report (but not limited to them) are vulnerable to criminal liability but their behaviour is (or may be) different from a typical offender. The case for the introduction of a civil penalties scheme can at least in principle be made out. The challenge is less one of principle however and more of practicality: who would or could act as regulator for the purposes of the imposition of civil financial penalties? This should not necessarily be unwieldy, Garoupa and others opining that:

[248] Ibid, 252-257.
[249] Ibid, 258.

> Integrated arrangements are easily tailored to specific industries or violations. It could also be a sign of rent-seeking by potential victims and potential violators of the law as we have explained before. Finally, the complexity of many areas of economic activity requires simplified procedure and faster decisions.[250]

6.2.5 Certainly, the framework set out in Schedule 1 of the IPA, could lend itself to individuals or corporate entities suspected of committing CMA 1990 offences where there is a lack of intent or countervailing public interest reasons not to prosecute. It is procedurally straightforward: there must be prior consultation before service of a notice; there are formalities to be met of any notice thereafter served (including specifying the grounds upon which the notice is served); provision for variation and cancellation; appeals and enforcement.

6.2.6 The Investigatory Powers Commissioner would be well suited to the task of acting as regulator for the purpose of imposing civil penalties in such circumstances, or jurisdiction could be accommodated through an amendment to the Regulatory Enforcement and Sanctions Act 2008. However, there would remain the difficulty of the lack of integration on the part of the Commissioner or designated regulator. This is problematic but not insurmountable: pragmatically, the Crown Prosecution Service (or equivalent in Northern Ireland and Scotland) could be given the discretion to make a referral (something akin to but less than seeking the Director of Public Prosecutions permission to prosecute certain offences) when advising on charge.

6.2.7 **The case for the introduction of civil financial penalties is logical in the context of CMA offences, and we recommend that a scheme of this kind should be taken forward**. The real difficulty is in implementation. A workable scheme exists in Schedule 1 of the IPA and the Investigatory Powers Commissioner or other suitable designated regulator could act as regulator for the purposes of such a scheme. This would require any legislative reform to emulate the pre-existing scheme and create a mechanism of referral by the relevant prosecutorial body.

6.3 RECOMMENDATIONS

6.3.1 We recommend the introduction of a civil financial penalties scheme to regulate computer misuse alongside the CMA 1990.

[250] Ibid, 252.

APPENDIX A

FULL LIST OF RECOMMENDATIONS

OFFENCES

R1. We recommend reforms to the section 1 CMA unauthorised access offence:

- 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 beyond simple unauthorised access.

R2. We recommend reforms to section 3 and section 3ZA CMA unauthorised act offences, by narrowing their application:

- Requiring an 'intention' to pursue a criminal endeavour, or to enable or assist another in committing an offence under the CMA 1990 (i.e. removing the potential for recklessness); and
- For section 3ZA, requiring the creation of a 'significant risk' (i.e. as opposed to any risk of harms).

R3. We recommend that section 3A CMA making, supplying or obtaining offence should be narrowed, to apply only where a defendant intends to pursue a criminal endeavour.

R4. We recommend the creation of a new corporate failure to prevent offence, to apply across all of the CMA 1990 offences in these terms:

(a) A body corporate or partnership (B) is guilty of an offence if a person (A) commits an offence contrary to sections 1, 2, 3, 3A or 3ZA of this Act when A is acting in the capacity of a person associated with B and provided that A committed that offence for the benefit of B.
(b) A will act in the capacity of a person associated with B where A is an employee of B, an agent of B, or any other person who performs services by or on behalf of B.
(c) It is a defence for B to prove that B had in place adequate procedures designed to prevent persons associated with B from committing such offences.

DEFENCES

We recommend amending the CMA 1990 as follows:

R5. Amending section 17(5) to add (c) – 'he does not reasonably believe that the person entitled to control access of the kind in question to the program or data would have consented to that access if he had known about the access and the circumstances of it, including the reasons for seeking it.'

R6. Amending section 17(5) to add (d) – 'he is not empowered by an enactment, by a rule of law, or by the order of a court or tribunal to access of the kind in question to the program or data.'

R7. Add a new section 18 in these terms: 'It will be a defence to a charge contrary to sections 1 and 3 for a person to prove that in the particular circumstances the act or acts (i) was necessary for the detection or prevention of crime, or (ii) was justified as being in the public interest.'

GUIDANCE TO PROSECUTORS

We recommend that revised CPS Guidance on the CMA 1990 should:

R8. Include a list of factors that point both towards and against prosecution for the core offences in sections 1 and 3 of the CMA (examples included at **4.4.3**-**4.4.4**);

R9. Should section 3A(2) continue to require belief as to a likely outcome (see our recommended narrowing of this offence in **Chapter 2**), the word 'likely' should be interpreted by the CPS in order to give as much reassurance as possible to responsible manufacturers and researchers;

R10. Address the difficult charging decisions to be made where a charge could be laid in relation to the same activity both under the DPA 2018 and the CMA 1990, but where the defendant would be expected to raise one of the defences which are provided for only in the DPA 2018, sections 170-172;

R11. Clarify the relationship between the police, NCA and CPS in making prosecutorial decisions where young defendants are thought to have committed offences of some seriousness.

SENTENCING

We recommend that:

R12. The Sentencing Council should produce an offence-specific guideline for CMA 1990 offences;

R13. Consideration should be given to producing a specific children and young persons guideline;

R14. Both the adult and children and young persons guidelines should expressly deal with autism and Asperger syndrome;

R15. New guidance should be issued for sentencers addressing how to draft preventative orders that effectively tackle CMA offending, providing examples of effective and proportionate prohibitions and requirements to courts who are unlikely to have significant expertise in this complex area; and

R16. CMA 1990 offences ought to be added to Schedule 5 of the Sexual Offences Act 2003 enabling a court to impose a sexual harm prevention order on conviction in appropriate cases.

CIVIL PENALTIES

R17. We recommend the introduction of a civil financial penalties scheme to regulate computer misuse alongside the CMA 1990.

APPENDIX B
COMPUTER MISUSE ACT 1990 PROSECUTION STATISTICS

In this short appendix we discuss current data on CMA incidents, prosecutions and convictions. We also scrutinise the sources of this data, highlighting and criticising inconsistencies that severely limit their credibility as sources for informing both reform and enforcement of the law.

STATISTICAL SOURCES

Data on computer misuse crime is available from a number of sources that include:

1. Office for National Statistics - Crime Survey for England and Wales;
2. Action Fraud referrals to National Fraud Intelligence Bureau;
3. Ministry of Justice - Criminal Justice System statistics quarterly;
4. Hansard Written Answers;
5. Freedom of Information Act 2000 Requests; and
6. Computer Misuse Act 1990 - Table of Cases database.

1. ONS Crime Survey for England and Wales (CSEW)

The ONS CSEW is a UK government survey of individual victims of offences in England and Wales.

The Computer Misuse Offence Group category is defined in the CSEW User Guide as: 'when fraudsters hack or use computer viruses or malware to disrupt services, obtain information illegally or extort individuals or organisations.' Further explanation of Computer misuse is given in a footnote in Crime in England and Wales: 'Any unauthorised access to computer material, as set out in the Computer Misuse Act 1990.'

The Computer Misuse category is broken down in to two sub-categories:

- Computer virus; and
- Unauthorised access to personal information (including hacking).

Computer virus is defined in the CSEW User Guide as: 'Computer viruses or malware: a computer virus is a computer program that can replicate itself and spread from one computer to another by using executable code; malware is short for malicious software and consists of programming (code, scripts, or other software) designed to disrupt or deny the operation of a computer.' *Unauthorised access to personal information (including hacking)* is defined in the CSEW User Guide as: 'Hacking: unauthorised modification of the contents of any computer.'

The ONS Offence Group and sub-category names and definitions are confusing and do not map easily on to the structure of CMA 1990 offences. As a result the ONS sub-categories are of limited value. Despite this, the ONS believes that 'CSEW provides the best indication of the volume of computer misuse offences,' and the figures certainly suggest high levels of offending conduct.

The CSEW estimates the total numbers of incidents in the Computer Misuse category:

- For the year to June 2018 CSEW estimated a total of about 1,121,000 incidents of computer misuse; and
- For the year to June 2019 CSEW estimated a total of about 977,000 incidents of computer misuse.

2. National Fraud Intelligence Bureau (NFIB)

The NFIB records offences referred by Action Fraud, who collate reports (predominantly by businesses) of computer misuse offences. NFIB Computer Misuse analysis categories include:

- Computer viruses;
- Hacking – extortion;
- Hacking – social media and email; and
- Hacking – personal.

For 2018, NFIB report a total of the above four categories of 23,683 offences referred by Action Fraud. For the year to June 2019, the total fell by 7% to 20,329 offences.

It is widely believed that many computer misuse incidents are not reported (either by individuals or businesses) and that as a result the Action Fraud data on computer misuse

represents only a fraction of all computer misuse crime. Comparing the NFIB/Action Fraud data with the CMA offence estimates (CSEW), it can be seen that only about 2% of CMA offences (CSEW) result in a police investigation.

3. Ministry of Justice (MoJ)

The MoJ provides a quarterly statistical analysis of all criminal court proceedings analysed by offence and outcome. MoJ Computer Misuse analysis categories include:

- CMA Section 1;
- CMA Section 2;
- CMA Section 3; and
- CMA Section 3A.

A useful table of this data is maintained by independent expert Michael Turner. The data is extracted from the Courts Proceedings database. Statistics on prosecutions, convictions and sentencing are derived from the LIBRA case management system (for the magistrates' courts records) and/or the Crown Court's CREST system which holds the trial outcome and sentencing data.

The data set appears to be incomplete**.** Although CMA Section 3A came into effect on 1 October 2008, there are no entries for this category in the years 2008, 2009 and 2012. In particular, the absence of CMA Section 3A entries for 2012 is an anomaly. Similarly there is no data on new Section 3ZA (although there have not yet been any reported cases).

The MoJ data includes private prosecutions (for example, by government departments, private organisations and individuals) of offences where there has been no police involvement.

For 2018 MoJ report totals of the above four categories for Defendants Proceeded against (51), Convicted (45) and Sentenced (46).

4. Hansard

Hansard is the official record of debates in the UK parliament that includes written answers by government minsters. Two written answers to questions about the number of CMA Prosecutions have been published that cover the period 2004 – 2010. Again, useful record of the data is maintained on the website of independent expert Michael Turner.

The time period for Hansard data overlaps that given for the MoJ data for the period 2008 – 2010. In this period there are numerous differences between the number of Prosecutions given in the Hansard data and the number of offences Proceeded against in the MoJ data. No explanation is given.

5. Freedom of Information Act 2000 Requests (FOIAR)

There have been several Responses to FOIARs of individual Police forces relating to CMA 1990 crimes over a number of years. Two significant Responses from Northumbria Police and West Yorkshire Police have been identified and analysed. Both cover the period 2015-2017.

Northumbria Police Freedom of Information Act 2000 (FOIA) Request 212/18 response has been examined. Outcomes of the CMA 1990 cases are listed using the Outcome codes set out in the Home Office Counting Rules for Recorded Crime and are summarised as follows:

Northumbria Police Outcomes of CMA Crimes Reported 2015 -2017

Outcome	**CMA Reported Crimes**	**%**
Caution adult	4	5
Caution youth	1	1
Charge/Summons	9	10
Community Resolution	1	1
Evidential Difficulties	7	8
Investigation Complete - No suspect identified	39	44
Not in Public Interest (Police)	1	1
Taken into consideration	1	1

Undetected	2	2
Victim declines or is unable to identify suspect	8	9
Victim does not support police action	14	16
Victim or key witness is deceased or too ill to give evidence	1	1
Total CMA Crimes Reported 2015 -2017	**88**	**100**

In summary between 2015 and 2017 Northumbria Police recorded 88 reported crimes under the CMA 1990 resulting in nine prosecutions (8% of reports). There is no record of any CMA crime reports originating from Action Fraud/NFIB.

West Yorkshire Police Freedom of Information Act 2000 (FOIA) Request 212/18 response has been examined. Outcomes of the CMA 1990 cases are listed using the Home Office Counting Rules and are summarised as follows:

West Yorkshire Police Outcomes of CMA Crimes Reported 2015 -2017

Outcome	**CMA Reported Crimes**	**%**
Caution adult	3	1
Caution youth	-	-
Charge/Summons	2	1
Community Resolution	4	2
Evidential Difficulties	97	48
Investigation Complete - No suspect identified	93	46
Not in Public Interest	5	2
Taken into consideration	-	-
Undetected	-	-
Victim declines or is unable to identify suspect	-	-
Victim does not support police action	-	-
Victim or key witness is deceased or too ill to give evidence	-	-
Total CMA Crimes Reported 2015 -2017	**204**	**100**

The introductory preamble to the Response states that 'between 01.01.2015 and 31.12.17 West Yorkshire Police have recorded 247 crimes under the Computer Misuse Act.' Our

analysis shows a total of 204 (including two with no description in the column Crime Notes) reported crimes under the CMA 1990. There is no explanation of the difference between these two totals. There is no record of any CMA 1990 crime reports originating from Action Fraud/NFIB.

In summary between 2015 and 2017 West Yorkshire Police recorded 204 reported crimes under the CMA 1990 resulting in only two prosecutions (1% of reported crimes). The column Crime Notes provides details of each reported crime. Most of these entries have been redacted or heavily redacted, so that it is generally difficult to understand the circumstances described. However, in the only two cases in the Charge/Summons category the Crime Notes include sufficient details to identify the target of the crime as being a Police computer system:

> 2016 ACCESSED POLICE COMPUTER SYSTEMS REGARDING NUMEROUS PERSONAL FRIENDS AND THAT ACCESS WAS NOT FOR A POLICING PURPOSE
>
> 2016 ACCESSED POLICE RECORDS HAS THEN DISCLOSED THIS INFORMATION

It is remarkable that there were only two reported crimes that resulted in offenders being prosecuted out of 204 CMA cases investigated in 2015-2017 by this police force. It appears that none of the other 202 investigations resulted in a prosecution. It is also astounding that both these two prosecutions relate to unauthorised access to police computer systems.

It is also necessary to comment on the high proportions (44% and 45%) of CMA crimes recorded by both police forces that have been coded as 'Investigation Complete - No suspect identified.' It is appreciated that it is the Home Office that is responsible for the definition of these categories of Outcome. The word 'Complete' risks giving a false impression that all investigative avenues have been exhaustively explored. In many cases it will merely be a preliminary triage that has been completed. Digital forensic investigations are almost never complete and routinely continue to reveal new evidence right up to, and sometimes during, a CMA trial.

6. Computer Misuse Act 1990 - Table of Cases database (CMA ToC)

The CMA ToC is a repository of published material on CMA cases located at **http://www.computerevidence.co.uk/Cases/CMA.htm**. The CMA ToC has been maintained by independent expert, Michael Turner, since 1992. The list is linked to and credited within

CPS guidance. For 2018 CMA ToC includes comprehensive details of ten CMA cases that refer to prosecutions of 22 Defendants.

The data available here is very useful for the analysis of CMA 1990 offences, collating a wide variety of information within a single accessible site. Authors across this report have made use of this resource. However, it is inevitably limited by the resources used to feed into it (i.e., the statistical sources discussed across 1-5 above).

COMPARISON

It will be seen that there is little agreement between the above sources on how CMA 1990 cases should be categorised. We believe that it is only meaningful to compare the total number of cases referenced for the most recent reporting year.

In many CMA 1990 cases the time scale from the original offence to a disposal in court will be measured in years. That makes it generally impossible to identify the progress of individual CMA 1990 cases by correlating multiple sources of data including: Experience of an incident as a victim (CSEW); Reporting an alleged offence to Action Fraud (NIB); Proceedings Initiated against Defendant (MoJ); Defendant Convicted (MoJ); Defendant Sentenced (MoJ and CMA ToC); that may be recorded over a number of years.

There is no reason to assume that the timing of the reporting of such events is consistent between the various evidence sources and between years. As a result it is also difficult to make any meaningful comment on rates of increase/decrease between reporting years.

CMA PROSECUTION TIME SERIES

We have combined data from three of the above sources to produce a time series of CMA Prosecutions for the period 1990 to date:

Year	CMA Prosecutions	Source
1991 - 2003 estimate	40	ToC
2004	21	Hansard
2005	24	Hansard

2006	25	Hansard
2007	19	Hansard
2008	6	MoJ
2009	8	MoJ
2010	7	MoJ
2011	10	MoJ
2012	22	MoJ
2013	53	MoJ
2014	51	MoJ
2015	56	MoJ
2016	57	MoJ
2017	63	MoJ
2018	51	MoJ
Total Prosecutions	**513**	

The Total number of CMA Prosecutions in the period 1990 – 2018 is 513. Given that the number of acquittals in the period 1990–2018 identified in ToC is 10, we conclude that there have been about 500 convictions under CMA in the period 1990 – 2018.

SUMMARY

Summarising the above results for the sources of data in the reporting year 2018:

Source	**Number in 2018**
CSEW estimate of CMA incidents	1,121,000
NFIB reported CMA offences	23,683
MoJ Defendants Proceeded against	51
MoJ Defendants Convicted	45
MoJ Defendants Sentenced	46
CMA ToC Cases where Defendant(s) Sentenced	10
CMA ToC Defendants Sentenced	22

Whatever the difficulties in analysing these different sets of data, the overall impressions are clear:

- About 2% of CMA offences (CSEW) result in a police investigation (NFIB);
- Only a minuscule proportion of CMA offences (CSEW) result in a prosecution (MoJ); and
- Only a fraction of 1% of CMA reported offences (NFIB) result in a prosecution or a conviction (MoJ).

APPENDIX C

THE ROLE OF SENTENCING IN LAW REFORM

INTRODUCTION

In this appendix, we ask ourselves: *What role, if any, should sentencing have in the reform exercise?* It is our hypothesis that an examination of the sentencing powers (both primary disposals and ancillary orders) of an existing regime can aid the evaluation of the case for reform and inform any proposals for change to substantive offences as well as (self-evidently) the sentencing regime. The theoretical discussion in this appendix provides a useful background and context for the CMA 1990 sentencing recommendations in **Chapter 5**.

Sentencing has typically been viewed as secondary, the poor cousin to the substantive criminal law – perhaps even not a 'real' subject. Volume upon volume of punishment theory asking (and answering) philosophical questions such as *Who should we punish?* and *How much?* aside, sentencing in England and Wales only began to be considered a subject worthy of study after David Thomas' seminal work *Principles of Sentencing* (1970). There has since, however, been an increasing number of more practically minded sentencing scholars such as Ashworth, Padfield, Roberts and Hood who have championed the importance of properly considered sentencing. Certainly the Sentencing Council and Court of Appeal (Criminal Division) no longer view sentencing as a secondary subject, given the increasing workload with which it provides the latter, and the difficult task faced by the former.

A reform exercise will inevitably start with questions of models of criminalisation and consideration of the type of behaviour the offences are seeking to address. We suggest however that express consideration of sentencing at an early stage can inform the process to a material extent. The significant safeguards that accompany a criminal investigation and prosecution are reflective of what is at stake in such proceedings. Much has been written about criminalisation and where the law draws the line between behaviour: that which is morally reprehensible but lawful, that which is actionable at civil law, and that which is criminal. The importance of a criminal investigation and prosecution cannot be underestimated and stems from its consequences; a finding adverse to the defendant may expose them to the coercive power of the state to deprive them of their liberty and to punish to the degree it deems appropriate. Such is surely uncontroversial. It is therefore appropriate to dedicate time and effort to the examination of the substantive criminal law and how it might be reformed, but such consideration should, we suggest, include consideration of sentencing powers. Further, the efficacy of the response to crime, whether it be punishment,

rehabilitation or a combination of retributive and consequentialist considerations, is important. There is accordingly a need to focus greater effort on sentencing as a subject.

SENTENCING AS A 'CHECK' ON THE SCOPE OF PROPOSED CRIMINAL OFFENCES AND MAXIMUM SENTENCES

In this section, we consider a possible methodological approach to involving sentencing in the reform of criminal offences at an earlier stage in the process. There are two ways that sentencing can inform the reform process. First, sentencing can operate as a 'check' on the model of criminalisation most suitable for a given behaviour. It is in the gift of parliament to create an offence which is easy to prove – perhaps by virtue of a low *mens rea* requirement or by being an inchoate or pre-inchoate offence – which also has a high maximum sentence. But we argue that parliament should not 'have it both ways'. One might counter with the proposition that where an offence which has a low threshold has the capability of causing high levels of harm, the maximum sentence should be high. In theory, this may be correct. But it seems obvious that in such circumstances, the preferable approach would be to have multiple offences, with different thresholds, and appropriate maximum sentences spanning the range of seriousness. For instance, we do not have, and would not want, a single offence of violence against the person with a maximum sentence of life imprisonment, to cover offending from common assault to wounding or causing GBH with intent. In such circumstances, the elements of the offence would have to be easier to prove than is currently the case with causing grievous bodily harm with intent (such as a recklessness requirement and a low harm requirement) but would expose offenders to the gravest penalty available to a sentencing court. Not only does this risk (and perhaps invite) inconsistency, but it is submitted that it is an inappropriate label for such offending.[251] It is intuitive that there are protections in place to prevent offenders being subjected to disproportionate sentences.[252] Involving sentencing at an earlier stage than hitherto, can draw attention to such problems and make for a more principled regime.

An examination of the general sentencing scheme can also inform the discussion as to the appropriate maximum penalty for a given offence; it may even be able to act as a form of restraint if other methods are capable of dealing with an offender in a less coercive way. For instance, if creating a new offence of throwing a corrosive fluid causing grievous bodily harm, the maximum sentence for the new offence should be informed by the maximum sentences for wounding or grievous bodily harm with intent (contrary to section 18 of the Offences

[251] For more on fair labelling, see Tadros, 'Fair labelling and social solidarity' in Zedner and Roberts (eds.) *Principles and Values in Criminal Law and Criminal Justice: Essays in Honour of Andrew Ashworth* (OUP, 2012).

[252] We would argue here that a right to apply for leave to appeal is an insufficient protection and that the protection should come before the point of conviction, not after it.

against the Person Act 1861) and wounding or causing grievous bodily harm (contrary to section 20 of that Act), so as to ensure some ordinal proportionality. It would be theoretically inconsistent (and difficult in practice) to create a new offence which has a maximum sentence significantly higher than another offence which caught the same behaviour. Further, to create a new offence with a maximum sentence that is lower than an existing offence which entirely subsumes the behaviour caught by the new offence would seem to create a redundant offence. This comparative exercise requires an understanding of the current regime in order to identify any lacunae in the arsenal of sentencing orders capable of being imposed on conviction.

THE SENTENCING REGIME IN ENGLAND AND WALES

The following paragraphs briefly detail the sentencing regime in England and Wales. They are by no means comprehensive but provide an overview for the purposes of this appendix. The sentencing scheme in England and Wales operates a form of limiting retributivism: the scheme is principally retributive – i.e. concerned with punishment and retribution – but subject to consequentialist considerations – i.e. concerned with forward-looking concepts relating to crime reduction including rehabilitation and deterrence.[253] Sentence is determined, principally, by the seriousness of the offence (a retributive consideration), an assessment of which must involve consideration of the culpability of the offender and the harm caused or potentially caused. Supplementary to this, Parliament has provided five purposes of sentencing for offenders aged 18 or over at the date of their conviction. Section 142 of the Criminal Justice Act 2003 states:

> 142(1) Any court dealing with an offender in respect of his offence must have regard to the following purposes of sentencing—
>
> (a) the punishment of offenders,
>
> (b) the reduction of crime (including its reduction by deterrence),
>
> (c) the reform and rehabilitation of offenders,
>
> (d) the protection of the public, and
>
> (e) the making of reparation by offenders to persons affected by their offences.

The system operates thus: The outer limits or 'permissible range' is set by retributive principles as driven by consideration of offence seriousness (that in itself requiring a

[253] For consideration of the 'shades' of retributivism, including an explanation of limiting retributivism as proffered by Norval Morris, see Ashworth, *Sentencing and Criminal Justice* (CUP, 2015), 95.

consideration of the concepts of culpability and harm). From there, the consequentialist considerations can determine the sentence within that range.[254] The resultant sentence accords with the principle of proportionality and desert theory while affording the sentencer the flexibility to reflect particular aspects of the case by reference to other considerations.[255]

ACHIEVING A COHERENT AND PROPORTIONATE SENTENCING REGIME

So how can sentencing inform the discussion of potential reforms? It will first be necessary to consider the maximum sentences in the current regime. Wasik and Pease argue that it is generally accepted that maximum sentences are irrelevant to the control of judicial sentencing.[256] We suggest that this may be somewhat of an exaggeration, given the obvious effect that maximum sentences can have in controlling or informing judicial practice. A two-year maximum sentence for indecent assault will clearly affect judicial practice, prohibiting a sentence in excess of that limit. Maximum sentences can and do act as aids to interpreting the gravity of an offence and the appropriate sentence within the maximum.[257] Wasik and Pease are, however, right in cases of high maximum sentences: the maximum sentence for perverting the course of justice is life imprisonment but this can be confidently said to have no impact upon practice. Offences such as perverting the course of justice (as with many other offences for which the sentence is life imprisonment) are outliers where the average severity of the offence is not aptly captured by the maximum sentence.

This brings us to questions of proportionality. Kelly describes von Hirsch's account of proportionality thus:

[254] Ashworth, *Sentencing and Criminal Justice* (CUP, 2015), 113

[255] Ashworth notes that in practice, section 142 is problematic, providing no hierarchy among the purposes, but simply enabling the courts to pick one (or more) to prioritise in any given case. This, he says, is the 'worst of pick and mix sentencing', Ashworth, *Sentencing and Criminal Justice* (CUP, 2015) 82. An alternative view is that the provision enables the court to do justice to the differences between cases: e.g. two cases which are ostensibly similar in terms of their offence seriousness (as required to be considered by s143 of the CJA 2003) might reasonably be treated differently (within the range set by the principle of proportionality) by reference to non-offence-based factors, such as an amenability (or otherwise) to rehabilitation. In contrast, one might argue that rather than the purposes of sentencing expressed in section 142 impacting upon the location of the appropriate sentence in the range set by the principle of proportionality, the purposes should be able to affect the width of the range and its upper and lower limits. This, however, would undermine the principle of proportionality and would seem to run counter to Parliament's intention. However, this is not the appropriate forum to enter into a critique of the sentencing regime and it suffices here to note the operation of the scheme.

[256] Wasik and Pease, 'Discretion and sentencing reform: the alternative' in Wasik and Pease (eds) *Sentencing Reform: Guidance or guidelines?* (Manchester University Press, 1987) 1.

[257] See Kelly, 'Reforming maximum sentences and respecting ordinal proportionality' [2018] *CrimLR* 450, 450-461.

> Ordinal proportionality requires that a penalty should be proportionate to the gravity of the offence for which it is imposed. Those convicted of grave crimes ought to have correspondingly severe sentences, and those convicted of less grave crimes ought to have correspondingly less severe sentences. It is thus a relative concept. Cardinal proportionality, by contrast, is a non-relative concept. It sets the overall level of punishment on a scale. So a sentencing system may be cardinally disproportionate if the sentences it imposes are too high even if graver offences are punished more severely than less grave offences.[258]

It is argued that one must start by considering the regime in isolation: Are the maximum sentences proposed for the newly created (or amended) offences ordinally proportionate *inter se*? This will require a consideration of the offence model(s) chosen and the wrongs being targeted. For instance, consider the offences under the Road Traffic Act 1988. A driving offence involving dangerous driving would likely be charged as dangerous driving contrary to section 2 of the Road Traffic Act 1988, which carries a maximum sentence of two years' imprisonment. The same offence resulting in a collision leaving a victim in a permanent vegetative state would likely be charged as an offence of causing serious injury by dangerous driving contrary to section 1A of the 1988 Act, an offence which carries a maximum sentence of five years' imprisonment. The same offence resulting in the victim's death would be charged as an offence of causing death by dangerous driving contrary to section 1 of the 1988 Act,[259] an offence which carries a maximum sentence of 14 years' imprisonment. One could debate the relative disparity in seriousness between the three offences, but it is suggested that the disparate maximum penalties demonstrate that at least one of them must be ordinally disproportionate, i.e. the seriousness of the offence is not matched by the maximum sentences.

Once the sentences proposed can be said to be broadly ordinally proportionate, one can consider ancillary sentencing orders. Does the current scheme provide the sentencer with sufficient tools? In general terms, the sentencing scheme in England and Wales provides for disposals which are designed to punish and deter. Principally these are fines, non- (or non-immediate) custodial sentences such as community orders, and imprisonment (including sentences for public protection). These disposals can also meet considerations of rehabilitation, deterrence, incapacitation and restitution, though one might dispute the efficacy of imprisonment as a means of achieving rehabilitation, for example. There are, further, a number of other disposals which can, solely, dispose of a case such as compensation orders, forfeiture orders, and restitution orders. Each of these can meet multiple purposes of

[258] Ibid, 451.

[259] An alternative would be to charge unlawful act manslaughter, which as an offence contrary to common law carries a maximum sentence of life imprisonment. As to the propriety of this, see e.g. *Attorney General's Reference (R. v Dobby)* [2017] EWCA Crim 775.

sentencing. For instance, a forfeiture order can both punish, by depriving the offender of their property, and protect the public, by removing a dangerous article from public circulation.

If a purpose of criminalisation is public protection and incapacitation, while this is usually achieved through incarceration (and therefore requires a high maximum sentence), in the modern sentencing regime it may be possible to reduce the maximum sentence on account of such protection being provided by other, less coercive, means. For instance, a behaviour order may be able to provide state oversight of an offender in the community, ensuring (so far as is possible) that the offender does not reoffend, such that the scale of sentences can be reduced, thereby altering the 'anchoring' point of the severity of sentences for the purposes of cardinal proportionality. Whether one might propose the creation of a new sentencing power rather depends on the analysis of the substantive criminal law and the wrongs being addressed. Here, we simply raise the methodological approach which may prove most useful in the pursuit of a comprehensive reform exercise.

The concept of constructing a sentencing package to meet multiple (and, on Ashworth's view, competing) aims of sentencing is not new. It is most commonly recognised in the sentencing of dangerous offenders, where a court may choose to impose a determinate sentence on a dangerous offender where other measures – such as a sexual harm prevention order – can provide adequate protection.[260] This, we argue, should be a key concern in the reform of any criminal offence, not least in times of austerity and concern about a rising prison population.[261] Any adjustment to the proposed sentences can be made at this stage resulting in – one hopes – a cardinally and ordinally proportionate sentencing regime for the amended (or newly created) offences. Further, one could, when considering the reform of an area of law such as computer misuse, explore the possibility of the creation of a new ancillary order to deal with a particular issue. However, one might think that with the proliferation of ancillary orders in recent years, and the breadth of orders such as the criminal behaviour order,[262] caution should be exercised when considering this as a measure.

As a third step, one must then consider how the proposed regime compares with other offences and offence types. There are two issues here: (a) is the regime ordinally proportionate with other offences and their maximum sentences; and (b) is the regime cardinally proportionate? The former presents problems given the inconsistency of maximum

[260] See Harris and Walker, 'Difficulties with dangerousness: (2) The determination of the appropriate sentence' [2018] *CrimLR* 782.
[261] See Grierson, 'Prison minister calls for more money to build jails in England and Wales' (Guardian Online, 2018).
[262] Criminal behaviour orders may prohibit the offender from doing, or require the offender to do, any specified thing that the court considers will help to prevent the offender from engaging in behaviour that causes or is likely to cause harassment, alarm or distress to any person. Anti-social Behaviour, Crime and Policing Act 2014, s22.

sentences across the criminal law. The road traffic example above serves as an illustration, as does the illogicality of having the same maximum sentence for offences of assault occasioning actual bodily harm and wounding or causing grievous bodily harm.[263] This presents the reformer with a decision: increase or decrease the sentences of the proposed regime to accord with the wider sentencing scheme, ensuring the sentencing regime remains ordinally proportionate, or alternatively, retain the levels on the basis that they are considered to be cardinally proportionate, accepting the inevitable criticism of an incoherent sentencing regime which is ordinally proportionate *inter se* but ordinally disproportionate with the wider scheme.

ORDINAL PROPORTIONALITY

In **Chapter 5**, we focus our discussion on the need for ordinal proportionality *within* the regime of computer misuse offence, asking whether reform is required to maintain coherence at sentencing. We also discuss the role of sentencing guidelines and ancillary orders in maintaining such coherence. This follows a relatively standard approach to assessing a sentencing regime of this kind. What is often neglected but his approach however, providing the focus of this section, is the role of ordinal proportionality *outside* of the specific sentencing regime under discussion; the need to place a set of offences (such as those within the CMA 1990) within their wider sentencing context.

Beyond the issues of proportionality within the regime there are arguably more fundamental issues stemming from a lack of proportionality with similar or alternative offences. To attempt a comprehensive review of the place of the CMA 1990 in the criminal law of England and Wales would be beyond the scope of this modest appendix. As Kelly argues, this would require a comprehensive and fundamental analysis of every criminal offence, starting from first principles, surely an unenviable task.[264] What is more achievable, however, is a comparison with similar or alternative offences. When offences within a regime have disproportionately low or high maximum sentences in relation to similar or alternative offences this can lead to arbitrary results and disproportionate sentences for certain offenders, depending on the regime under which they are prosecuted. Where the maximum sentences are particularly disproportionate it can lead to a regime rarely being used or prosecuted, simply lying dormant on the statute book, failing to effect any social change. A further issue which arises from the same behaviour being capable of being charged as multiple offences of different types (aside from it being theoretically unsatisfactory) is that it gives rise to a claim that the offender should be dealt with on the most favourable basis.[265] The issues facing the CMA 1990 regime

[263] See the Offences against the Person Act 1861, s20 and s47.
[264] Kelly, 'Reforming maximum sentences and respecting ordinal proportionality' [2018] *CrimLR* 450, 460-461.
[265] See *Bright* [2008] EWCA Crim 462.

are not, perhaps, so severe – it undoubtedly catches behaviour that other offences do not – but the effect of much of the CMA 1990 regime is certainly blunted by its low maximum sentences.

By way of example, many computer misuse offences are committed by way of fraud, unauthorised access to a program or data resulting from the impersonation of another.[266] In contrast to the offences under sections 1 and 2 of CMA 1990, fraud under section 6 of the Fraud Act 2006 carries a maximum sentence of 10 years' imprisonment. This was recognised in *Brown*[267] where the fraudulent access of 152 Barclays bank accounts was charged as offences under section 2 of the CMA (which has maximum sentence of 5 years' imprisonment), rather than as fraud.

The purpose and place of the offence under section 2 of the CMA is particularly confusing due to its low maximum sentence of 5 years. Under section 1 of the Criminal Attempts Act 1981 a person commits an offence if, with intent to commit an indictable offence, they do an act which is more than merely preparatory to the commission of the offence. The maximum sentence for an offence of attempt is the maximum sentence for the offence intended to be committed.[268] Similarly under section 44 of the Serious Crime Act 2007 a person commits an offence if, with intent to assist the commission of an offence, they do an act capable of assisting the commission of an offence. The maximum sentence for an offence under section 44 of the Serious Crime Act 2007 is the maximum sentence for the offence intended to be assisted.[269]

The majority of section 2 CMA 1990 offences could alternatively be tried under either statute. As the offence intended to be committed under section 2 must carry a maximum sentence of more than 5 years' imprisonment, and the maximum sentence for the section 2 offence is only 5 years', invariably the maximum sentence will be greater under either alternative statute. The only offences for which the section 2 offence will be the preferable charging option are those rare offences that do not fall within either statute, such as those where the offence intended is solely an offence in a foreign jurisdiction,[270] or where the action was not, in fact, capable of assisting the commission of the offence or was merely preparatory (i.e. short of attempt) to the offence intended.

[266] See, for example, *Crosskey* [2012] EWCA Crim 1645 where the offender had gained access to Selena Gomez's Facebook account by falsely presenting himself as her step-father who managed the site and was convicted of one count of section 1, and one of section 3.
[267] [2014] EWCA Crim 695.
[268] Criminal Attempts Act 1981, s4.
[269] Serious Crime Act 2007, s58.
[270] By virtue of sections 4(4) and 8 of the CMA 1990.

More generally, there are questions as to why only offences with a maximum sentence of five years' imprisonment or greater engage section 2. Such an approach proceeds on the basis that maximum sentences of imprisonment are a good indicator of offence seriousness whereas, as Kelly argues, in many cases they are not, and often are simply the result of historic accident.[271] The use of a list of specified offences which engage section 2 may perhaps be a more theoretically satisfactory approach, although in practice such an approach in isolation is inevitably a recipe for legislative lacunas and missed offences. It may be that a combined approach would be preferable.

Further, as the Law Commission noted in their working paper, and as we have discussed elsewhere in this report, there is an overlap between CMA and data protection offences. Indeed, this was a justification given by the Law Commission for initially recommending that any hacking offence be non-imprisonable.[272] Although this recommendation was not followed and the offence contrary to section 1 of the CMA has been imprisonable since enactment, offences under the Data Protection Act 2018 are non-imprisonable, as were offences under the Data Protection Act 1998.[273] Arguably some prosecutions under section 1 of the CMA are better considered as data protection offences and vice versa.[274] It is hard to see how the much higher maximum sentence for a CMA 1990 offence is theoretically justifiable. The offence under section 170 of the Data Protection Act 2018 is committed only when a person actually obtains or discloses personal data or the information contained in it; it requires a much greater degree of harm than unauthorised access to a computer would seem to. In this case, however, it may be the data protection offences which are disproportionately low; the offence of unlawful interception,[275] which like the CMA 1990 regime requires only unlawful access, is also punishable by a maximum of 2 years' imprisonment. The Justice Committee in 2011 recommended that custodial sentences should be available for data protection offences, citing the significant profits available from data protection offences and the severe harms that can be effected either through improper use of personal data or the trauma that the intrusion can cause.[276]

[271] Kelly, 'Reforming maximum sentences and respecting ordinal proportionality' [2018] *CrimLR* 450, 453.
[272] Law Commission, *Computer Misuse* (Working Paper No 110, 1988) Para 6.38.
[273] See, sections 170 and 196(2) of the Data Protection Act 2018 and section 60(2) of the Data Protection Act 1998. Section 77 of the Criminal Justice and Immigration Act 2008 gave the Secretary of State the power to make an order amending section 55 of the Data Protection Act 1998 so that it became punishable by a maximum of 2 years imprisonment. The Secretary of State could only make such an order following consultation with the Information Commissioner, the media and other interested parties. This power was never exercised. Section 77 of the Criminal Justice Act 2008 was repealed by the Data Protection Act 2018.
[274] See further, 'ICO prosecution results in a first-ever prison sentence' (2018) 19(1) *Privacy & Data Protection* 18, where it was noted that while the ICO frequently prosecutes under the Data Protection Acts they occasionally charge similar actions under CMA to ensure appropriate penalties are available.
[275] Contrary to section 3 of the Investigatory Powers Act 2016.
[276] Justice Committee, 'Referral fees and the theft of personal data' (HC 1473, 2011) Ninth Report of Session 2010-12.

At the other end of the spectrum, in the national security arena, it is interesting to note that the maximum sentence for the section 3ZA offence, in cases involving a risk of serious damage to national security, is life, while the maximum sentence for offences contrary to section 1 of the Official Secrets Act 1911 is 14 years' imprisonment. It is odd that offences contrary to national security, if committed by the unauthorised access of a computer, face a substantially more severe maximum penalty than such offences if committed by traditional spycraft methods. It is true of course that computer systems can themselves be the target of crime and that computer misuse offences can damage the integrity of, and trust placed in, the computer system attacked.[277] However, any spycraft offence is likely to damage the integrity of, and trust placed in, the relevant information system. It is unclear why computers require such greater protection. Moreover, the significance of any harm suffered by the relevant computer system is likely to pale in comparison to the impact of serious harm to national security.

It is important to remember, therefore, that even where ordinal proportionality is achieved within individual sentencing regimes (our focus in **Chapter 5**), broader proportionality inconsistencies remain across and between regimes. This report is not the place to make recommendations as to these more systematic issues at sentencing. However, they do go some way to explain patters within the data (**Appendix B**) that show the relative underuse of CMA 1990 offences within the criminal justice system.

[277] See, Heymann, 'Legislating Computer Crime' (1997) 34 *Harvard Journal on Legislation* 373.