COMPUTER (MIS)USE AND THE LAW: WHAT'S WRONG WITH THE CMA?

KRISTOPHER WILSON
Jesus College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy
Trinity 2019

ABSTRACT

A series of justifications accompany the introduction of any new criminal law. The *Computer Misuse Act 1990* ('CMA') section 1 offence was justified on the basis that acts that might otherwise be characterised as *digital trespass* represented a new form of criminally wrongful conduct: such acts compromised the integrity of a computer, program, or system. 'Hackers' and 'hacking', those that seek 'unauthorised access' to computers or data and the tools and techniques that enable that access, were to be deterred. This deterrence was to be achieved, in part, by the intentionally broad operation of the CMA's section 1 offence. The offence exhibits the features of inchoate mode drafting; it does not criminalise obtaining access to a computer. Instead, it criminalises the 'causing of a computer to perform a function'. In casting the offence broadly, and in an effort for it to be *technology-neutral* and *future-proof,* key terms, like 'computer' were also left undefined. The question of whether a given 'access' is 'unauthorised', is to be determined by reference to any consent provided by the owner of the computer.

However, computers are not the same as physical property. There is a much broader scope for delimiting the authorisation of a particular user to *specific data*, in a way that was not envisaged by the Law Commission when recommending the adoption of the section 1 offence to respond to harms to the integrity of *the computer*. The result, as this thesis argues, is that in practice the section 1 offence may instead operate to provide criminal law protection to data and information in a way not otherwise contemplated by the general criminal law. Further, the use of 'terms of service' agreements and internal policies as the means of delimiting 'authorisation' now criminalises what would otherwise be a breach of a civil law right, merely because it is carried out by way of a computer. The offence operates to presume criminally wrongful behaviour, even in circumstances where the use of a computer was tangential to the result an accused intended. These concerns are further compounded by the evolving nature of computing technologies, with the increasingly common approach of applying those technologies to ever more facets of daily life.

This thesis aims to revisit the initial justifications set out to support the creation of the CMA and its five offences. Focus then shifts to the drafting, application, and policy orientation of the section 1 offence. The thesis argues that the offence, as structured, is over-inclusive and exhibits an increasingly high degree of overlap with both general criminal offences, the other offences within the CMA, and those contained in, for example, data protection frameworks. While the section 1 offence was conceived to serve a *supplementary* role to these broader offences, this thesis contends that, as a result of shifts in computing technologies and their uses, the section 1 offences' breadth and low evidence burden may instead be operating in practice to *supplant* those offences. This thesis considers those initial justifications in the context of examples of newer technologies, and through the application of broader criminological and cyber security approaches to computer-related crime.

ACKNOWLEDGEMENTS

This thesis was not necessarily planned in the form that it takes. In being offered and accepting a place in the Centre for Doctoral Training in Cybersecurity, I was exposed to the work of technical specialists (computer scientists, engineers): predominantly non-lawyers. Having already been aware of the *Computer Misuse Act 1990* ('CMA'), there was always something that didn't quite feel right with the apparent breadth of the offence. It was through many conversations with fellow students and staff in the CDT that I began to get a better sense of what that feeling related to. I am grateful for those conversations over the years we worked together.

I first began considering the CMA in the form of a 'mini-project' undertaken in the first year of the CDT's programme. That project, which would ultimately inform chapter 6 of this thesis, was brought about by 'cold-emailing' Dr Rebecca Williams as I searched for a potential supervisor for that project. Becca enthusiastically accepted, ultimately agreeing to be the supervisor for this thesis. My thanks for her continued support in letting me explore this topic, often in my own haphazard way.

The journey has been long. Mainly because I have a habit of over-committing and travelling too much. However, a massive thanks go to the 'Oxbridge Mob' who kept me sane, and the Cowley Road crew who helped make Oxford a home. Thanks also to the friends in various cities around the world (Adelaide, Melbourne, Sydney, New York, San Francisco, Toronto) for lending me your ears (and your couches).

Statistically, it's unlikely I should have ever ended up at the University of Oxford. I was born in remote South Australia to a large, lower working-class Aboriginal family. My great-great-grandparents were the product of a *socially complicated* marriage: a proud Arabunna women and first-generation Australian-born Scotsman. As a result of this, their children, and the following generation of my grandparents, were denied comprehensive education. They were instead taught by missionaries at Finnis Springs Mission to act more 'white' and to become 'civilised' through Christianity. Even when my father was born, real educational opportunities were scarce. Neither of my parents and few in my broader family ever finished school. But they made damn well sure I did. I am unbelievably grateful for the opportunities I have had today which arise only because of the strength, tenacity, and perseverance of those before me.

I'm also exceedingly grateful for those who helped me pay for it: international study is not cheap! My deepest gratitude to the Roberta Sykes Foundation, the Charlie Perkins Trust, and the University of Technology Sydney who all, along with financial support from the British Foreign and Commonwealth Office and the Australian Government, contributed to me being able to pursue this work.

TABLE OF CONTENTS

TABLE OF CASES

UNITED KINGDOM

AUSTRALIA

UNITED STATES

NEW ZEALAND

CANADA

TABLE OF STATUTES

UNITED KINGDOM

AUSTRALIA

UNITED STATES

INTRODUCTION

I OVERVIEW

In its essence, the *Computer Misuse Act 1990* (the 'CMA') section 1 offence criminalises *digital trespass*. The 'unauthorised access to computer material' offence proscribes any attempt by an individual to interfere with a computer, program, or data under another's control. The drafting of the offence adopts language crafted to be *technology-neutral*, with the key term 'computer' left undefined in order to encompass new technologies as they develop. This approach was part of an attempt to *future-proof* the offence.[1] The term 'computer' is to be interpreted and applied in a non-restrictive fashion.

[1] See, eg, Malcolm Highfield, 'The Computer Misuse Act 1990: Understanding and Applying the Law' (2005) 5(2) *Information Security Technical Report* 51, 53.

Despite the offence being devised with the intention that it be flexible, adaptable and effective in responding to rapidly expanding uses of computing technology, in the initial period following its introduction the offence was misunderstood and misapplied consistently. This misunderstanding resulted in an apparent lack of successful prosecutions as there was a perception that there remained an absence of any applicable specific and targeted legislation.[2] As a result, the CMA has been amended and expanded over time to now include five offences that criminalise various forms of misusing computing technologies. But, the section 1 offence remains in the same form as when it was introduced, save a dramatic increase in the available sentences, now an unlimited fine and up to two-year's imprisonment.

The CMA was created in response to the outcome of a small number of high-profile prosecutions in the 1980s that involved, to varying degrees, the misuse of computing technologies.[3] The underlying facts in those cases posed issues for the criminal law, with general criminal offences, or 'non-computer-specific offences', being interpreted and expanded to apply successfully in only a few cases.[4] The challenge in each of these cases was the need to address the broader question of whether the operation of computing technologies (as a *medium*, or means of facilitating conduct) acted as a disruption to establishing criminal culpability. The proposed solution was to treat the 'misuse' of computing technology in and of itself as criminal conduct through the operation of the CMA.[5]

At the time the boundaries of the criminal law in respect to computing technology were first being explored, such technology was still specialised, cumbersome, and

---

[2] See, eg, Marc Goodman and Susan Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 10(2) *International Journal of Law and Information Technology* 139, 141-3; John Worthy and Martin Fanning, 'Denial-of-Service: Plugging the legal loopholes?' (2007) 23 *Computer Law & Security Report* 194.

[3] *Cox v Riley* (1986) 83 Cr App R 54; *R v Gold and Anor* [1988] 2 All ER 186.

[4] Martin Wasik, 'The Law Commission Working Paper on Computer Misuse' (1989) 5 *Computer Law and Security Report* 2. *Cf* Peter Alldridge, 'Computer Misuse Act 1990' (1990) 9(6) *International Banking Law* 339.

[5] See, Colin Tapper, 'Computer crime: Scotch mist?' (1987) (Jan) *Criminal Law Review* 4; Andrew 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.

expensive, and left mainly to corporations, academia and computer enthusiasts.[6] The range of uses (and misuses) of that technology was limited, and the scale of potential future uses, and misuses, of computing technology was difficult to foresee. Debate was thus focused on whether computing technology presented opportunities for new *types* of crime, or merely new ways of committing existing crimes.[7] The tensions underpinning these positions were necessary for lawmakers to confront in determining what approach to adopt to ensure the criminal law could 'keep up' with developments in computing technology. Lawmakers could create new crimes, amend existing crimes, or take a structured and comprehensive approach to do both.[8]

As part of their review, and in recommending the creation of three new offences, the Law Commission set out four broad justifications to support criminalising computer misuse in the proposed manner.[9] These justifications were based on arguments in respect of the need to deter 'hacking', and that such offences could operate to serve a supplementary role to existing offences by criminalising conduct involving uses of computers that fell beyond their scope. Further, 'hacking' was harmful in that it compromised the integrity of the target computer, and this was a new harm that fell outside the experience of the criminal law. These arguments were supported with reference to the fact that other jurisdictions had enacted similar provisions within their domestic criminal law.

Counterarguments had been made that the general criminal law could indeed respond to the challenges posed by computing technologies through *offence-by-offence*

---

[6] For an introduction to the technology of the time, and those influential in sparking further developments, see Steven Levy, *Hackers: Heroes of the Computer Revolution* (2nd ed, Penguin Books, 2001).

[7] See generally, Martin Wasik, *Crime and the Computer* (Oxford: Clarendon Press, 1991); Susan Brenner, 'Is There Such a Thing as "Virtual Crime"?', (2001) 4(1) *California Criminal Law Review* 3; Donald Ingraham, 'On charging computer crime' (1980) 2(1) *Computer and Law Journal* 429; Frank Easterbrook, 'Cyberspace and the law of the horse' (1996) *University of Chicago Legal Forum* 7; and Lawrence Lessig, 'The law of the horse: what cyberlaw might teach' (1999) 113 *Harvard Law Review* 501.

[8] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [4.1]-[4.7].

[9] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989).

consideration and amendment. These arguments were ultimately rejected.[10] Such an approach would have involved the expansion or amendment of the elements of individual offences such that computing technology could fall within their scope. Examples included suggestions that the definition of 'property' be modified to include 'data' in the relevant provisions dealing with theft[11] and criminal damage.[12] Nevertheless, a degree of incompatibility could remain. Theft, for instance, requires an intention to deprive permanently; this is necessarily absent in the context of copying data where the legitimate owner has not been deprived of that data.[13] However, the Law Commission did suggest that a broad and comprehensive review ought to be undertaken to methodically assess the applicability of other existing criminal laws to conduct involving the use of computers following the introduction of the new criminal offences. That review never occurred.

Lawmakers thus proceeded on the basis that the Law Commission's recommendation for statutory intervention was correct, necessary, and warranted. The CMA would thus make particular uses of computing technology criminal, irrespective of the accused's underlying conduct and whether that may enliven criminal liability under general criminal offences.

The question of whether it was indeed necessary to focus on the use of a computer in the commission of a harm as the basis of criminality in and of itself remains inadequately addressed and too often overlooked. The initial justifications for the adoption of a framework based on computer misuse remain debatable. This debate, however, has mostly been side-lined. Despite subsequent review and multiple amendments, any attention given to the CMA appears to be focused almost entirely

---

[10] Ibid [2.29-2.33] where issues presented by the definition of 'property' and 'damage' for the purpose of criminal damage offences were deemed inappropriate to leave to the common law; Richard Walton, 'The Computer Misuse Act' (2006) 11(1) *Information Security Technical Report* 39, 40.

[11] See, eg, Jonathan Clough, 'Data Theft? Cybercrime and the Increasing Criminalisation of Access to Data' (2011) 22 *Criminal Law Forum* 145.

[12] *R v Whiteley* (1991) 93 Cr App 4 25, explored in chapter 2.

[13] Unless the circumstances were such that the accused simultaneously deleted the files that were to be copied, or where the act of copying resulted in all the value of the information being lost; see, eg, *Lloyd* [1985] QB 829, 836 per Lord Lane CJ; *Oxford v Moss* (1979) 68 Cr App R 183; Anna Louise Christie, 'Should the Law of Theft Extend to Information?' (2005) 69 *Journal of Criminal Law* 349, 350.

within the framework it created, centring on disputes of terminology and scope.[14] Change has been prompted by a desire to see an increase in the number and success of prosecutions under the CMA. Questions have not centred on the operation of the CMA within the broader context of the criminal law. Instead, official efforts to review and amend ask 'is the CMA fit for purpose?' However, what this question is asking is; does the CMA work for police and prosecutors?

Rather than presume the correctness of the CMA's approach, given the rapid pace of change in the capabilities and uses of computing technologies since its implementation 29 years ago, it is necessary to revisit the early debates that informed its formulation. Do the justifications for the offences, and their subsequent amendment, still hold? How do the offences sit vis-à-vis general criminal offences? Does a clear delineation between criminal conduct involving computers and conduct without the use of computers still exist, if it ever did? If so, to what extent?

This thesis argues that the continued evolution of computing technologies, as well as the subsequent, and independent, amendments to general criminal law offences, have resulted in a considerable degree of overlap between those offences and, in particular, the CMA's section 1 offence. While overlap is not of itself necessarily a problem,[15] the section 1 offences' focus on 'unauthorised access' could result in policy inconsistency in respect of penalties and the limits of the criminal law: in many circumstances, an online copyright infringer may find themselves criminally liable for the unauthorised access, but otherwise

[14] See, eg, Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change' (2006) 70 *Journal of Criminal Law* 424, 439-41; Neil MacEwan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (2008) 12 *Criminal Law Review* 995; Audrey Guinchard, 'Crime in virtual worlds: The limits of criminal law' (2010) 24(2) *International Review of Law, Computers & Technology* 175; Mary Wong, 'Cyber-trespass and Unauthorized Access as Legal Mechanisms of Access Control: Lessons from the US Experience' (2007) 15(1) *International Journal of Law and Information* 90.

[15] But overlap gives rise to substantive issues with respect to the role and operation of prosecutorial discretion. See, eg, William Stuntz, 'The Pathological Politics of Criminal Law' (2001) 100 *Michigan Law Review* 505; Darryl Brown, 'Prosecutors and Overcriminalization: Thoughts on Political Dynamics and a Doctrinal Response' (2009) 6 *Ohio State Journal of Criminal Law* 543; Ronald Wright and Marc Miller, 'Honest Opacity in Charge Bargains' (2003) 55(4) *Stanford Law Review* 1409; Sara Sun Beale, 'The Many Faces of Overcriminalization: From Morals and Mattress Tags to Overfederalization' (2005) 54(3) *American University Law Review* 747, at 757 in the context of selective enforcement of statutes proscribing otherwise widespread behaviour.

only civilly liable for the infringement itself.[16] The broad nature of the section 1 offence also permits it to be charged concurrently with general offences that carry higher penalties, leaving a substantial degree of scope for charge bargaining.

While the scale of conduct subject to the CMA has increased, there has been a countervailing change in the seriousness and scale of the associated *risks* and *harms* of various forms of digital trespass. With computing technologies becoming so embedded across all facets of our daily lives and throughout the broader economy, the potential scale of harms often associated with digital trespass has grown. These potential harms now range from mere annoyance, inconvenience or loss of privacy for a targeted individual, small to medium scale economic loss or individuals and companies, and to catastrophic economic losses for companies and governments, and serious personal injury and death.

It is necessary to note, however, that there is a distinction that must be drawn here between the harms that can be caused by mere unauthorised access, or digital trespass, and the harms that can result from the undertaking of further conduct that is enabled by that digital trespass. This 'further conduct' can involve the introduction of malicious software to cause abnormal functioning, or to 'overload' the system with unnecessary requests,[17] or could result in the extraction, modification, or substitution of data for economic, political, or other gains.

In popular parlance and much academic discourse, the distinction between mere digital trespass and the conduct enabled by that trespass is often collapsed under the label 'hacking'. While it is clear the two are interconnected, in that the conduct enabled by digital trespass might not occur without that initial 'mere' digital trespass, the fact that a mere digital trespass occurs does not necessarily mean any further specific or identifiable harm *will* result. However, the section 1 offence treats all forms of digital trespass, that is mere digital trespass and the conduct enabled by that trespass, as if both were criminally

[16] This is an incidental example arising from the operation of Terms of Service agreements, explored in chapter 5.

[17] Such a technique is known as a Denial of Service ('DoS') attack, or, when multiple computers are involved, a Distributed Denial of Service ('DDoS') attack. Discussed in chapters 3 and 6.

wrongful to the same degree. There is then an opportunity to charge additional CMA offences where the conduct enabled by the mere digital trespass could amount to a further criminal offence,[18] or where a subsequent impairment to the computer was made.[19] That is, the response escalates from a presumed uniform base criminality.

This thesis will argue that by ignoring the distinction between digital trespass in and of itself and further conduct that might be carried out due to that access, the operation of the section 1 offence sits uncomfortably within the criminal law. Criminality can arise on the basis of conduct involving a computer that breaches an individual's privacy, contractual obligations, or their intellectual property rights, rather than on the basis of *criminally* wrongful conduct.

The site where criminal law and civil law interact have generally be treated 'as isolated incidents, rather than pieces in a broader puzzle'[20] due to English law having no general theory that provides a clear delineation between criminal law and, in particular, tort law.[21] There are several approaches to identifying the markers of conduct that ought to belong in either category.[22] However, Dyson synthesises these to four 'overlapping and contradictory indicia': the moral description of the wrong, the process of remedying the wrong, the presence of penalty or compensation, and some positivist creation of legal classification and form.[23] These considerations, along with general principles of criminalisation, will inform the work of this thesis in considering the operation of the CMA.

---

[18] *Computer Misuse Act 1990* s 2.

[19] *Computer Misuse Act 1990* s 3.

[20] Matthew Dyson and John Randall, 'England's splendid isolation' in Matthew Dyson (ed), *Comparing Tort and Crime* (Cambridge University Press, 2015) 18, 20.

[21] Matthew Dyson, 'The Timing of Tortious and Criminal Actions for the Same Wrong' (2012) 71(1) *Cambridge Law Journal* 86.

[22] See, eg, Kenneth Simons, 'The Crime/Tort Distinction: Legal Doctrine and Normative Perspectives' (2007-8) 17 *Widener Law Journal* 719.

[23] Matthew Dyson, 'Tortious Apples and Criminal Oranges' in Matthew Dyson, (ed), *Comparing Tort and Crime* (Cambridge University Press, 2015) 416, 419.

II RESEARCH FOCUS

This thesis aims to argue that the justifications employed to support the formulation of the CMA's section 1 offence no longer hold as computing technologies have evolved. The offence has been rendered unacceptably over-inclusive, permitting what might otherwise be described as the contracting out of boundaries of criminal liability, with respect to the use of computers, to private entities.

In support of this argument, the approach adopted in constructing this thesis is informed by four questions:

1. Do the justifications put forward to support the creation of the CMA reflect the current use and misuse of computers?
2. Does the drafting of the *actus reus* of the section 1 offence in the inchoate mode result in an unacceptable degree of over-inclusiveness?
3. If so, does the *mens* rea of the section 1 operate to effectively delimit a justifiable boundary of culpability?
4. How do the offences within the CMA fit with criminological understandings of computer-related crime, cybersecurity concerns, and the applicability of general criminal offences?

III DESIGN

This thesis will address the research questions across six substantive chapters that adopt a broad cross-disciplinary evaluative approach.

Chapter 1 – *Justifying Data Access Offences: Situating the Criminalisation of Computer Misuse* briefly sets out the contested approaches to determining what conduct ought to be considered rightfully criminal. The purpose of this chapter is not to advocate one approach to criminalisation over another. Instead, it surveys the broad principles of criminalisation to define a normative model of what features an appropriately structured 'data access' offence ought to exhibit and be confined by. This model will form the reference point for analysis throughout the thesis.

Chapter 2 – *Defining Computer Misuse: Computer Crime in the 1980s and the Law Commission Working Paper* examines the historical, political, technological, and legal context that shaped the formulation of the CMA. The chapter briefly plots the development of computing technologies from the Second World War until the advent of personal computing in the 1980s that gave way to the first prosecutions for criminal conduct involving computing technologies. The chapter introduces the Law Commission's Working Paper on Computer Misuse and explores how law and policymakers sought to frame and conceptualise the harms of computer misuse and the wrongdoing they identified.

Chapter 3 – *The Computer Misuse Act*: *Structure, Interpretation, and Application* traverses a well-worn path in respect to outlining the ultimate recommendations of the Law Commission and the subsequent introduction of the CMA. It sets out to summarise the key prosecutions that have defined the interpretation of the offences, and plot the subsequent waves of amendments made, including the introduction of the additional offences and the transition of the section 1 offence from a summary offence with little emphasis on custodial sentences, to one that is triable either way with a maximum sentence of two years imprisonment.

Chapter 4 – *'Computers' and 'Access': The Effect of Technology Neutral Drafting'* begins the substantive analysis of the section 1 and the associated section 2 offences. The arguments throughout the chapter centre on the decision to leave the term 'computer' undefined, and to incorporate the use of 'access' operating in both its noun and transitive verb form. The decision to leave 'computer' undefined was inspired by the adoption of a similar approach in the *Police and Criminal Evidence Act 1984* ('PCEA') in respect of computer-produced evidence. While the Law Commission approved the approach in reaching their conclusion with respect to CMA, the provisions under the PCEA would ultimately be repealed due to being impractical and unworkable as a result of procedural over-inclusiveness. The blurred approach to defining 'access' similarly results in potential over-inclusiveness.

Chapter 5 – *Inchoate Drafting: The Heavy Lifting of 'Unauthorised Access'* shifts focus to the section 1 offence's *mens rea* requirement that the accused intend to secure access and

that the access so intended is unauthorised. It is argued that for the breadth of the *actus reus* established in Chapter 4 to be justifiable, the *mens rea* must operate effectively to limit culpability to instances of computer misuse that are indeed criminally wrongful. Adopting Jeremy Horder's categories of inchoate offences, the chapter argues that the requirement that the accused intend to secure unauthorised access is not sufficient to produce a normative change in the character of the accused's conduct in any given case. The over-inclusiveness of the *actus reus* is thus not sufficiently limited. This is illustrated through an analysis of the operation of 'terms of service' agreements concerning 'bug bounty programs' and online media streaming services, where a contravention of the terms of the agreements amounts to conduct falling within the scope of the section 1 offence.

Chapter 6 – *Computer Misuse Within the Broader 'Cyber' Regulatory Framework* explores the operation of the section 1 offence vis-à-vis models that have emerged in criminology to understand computer-related crime. In particular, the idea of the computer as being either the target of criminal conduct, a tool in the commission of criminal conduct, or incidental to the commission of a crime. The chapter argues that the section 1 offence does not effectively draw a distinction on this point, applying in most contexts involving a computer. This contention is examined in respect of the European Union Agency for Network and Information Security's 2018 Cyber Threat Landscape Report, where the operation of the CMA's offence is considered, along with general criminal offence applicable to the same underlying conduct. The result is a mapping exercise, culminating with a visual representation of the scope and degree of overlap of the section 1 offence to current identified cyber threats along the 'cyber kill chain'.

The thesis concludes by returning to the normative model established in Chapter 1 and, in addressing the research questions proposed above, makes a number of reform recommendations that are required to delimit the over-inclusive operation of the CMA's section 1 offence.

Chapter 1

JUSTIFYING DATA ACCESS OFFENCES: SITUATING THE CRIMINALISATION OF COMPUTER MISUSE

It is not wisdom, but authority that makes a Law

THOMAS HOBBES [1]

I INTRODUCTION

The availability of new technologies corresponds with changes in the crime landscape: new technologies create new criminal opportunities.[2] However, often these 'new' opportunities merely represent modified versions of existing offences. The language and construction of these existing offences can be flexible enough to encompass the new

[1] Thomas Hobbes, 'A Dialogue Between a Philosopher and a Student, of the Common Laws of England' in Sir William Molesworth, Bart. (ed), *The English Works of Thomas Hobbes of Malmesbury: Now First Collected and Edited by Sir William Molesworth, Bart. Vol VI* (London: Bohn, 1839-45) 5.

[2] David Wall, *Cybercrime: The Transformation of Crime in the Digital Age* (Polity Press, 2007) 2.

method of committing the harm or perceived wrongful act.[3] When given appropriate time, traditional criminal law principles can be expanded by the courts to address new criminal activity involving technology. Alternatively, in a shorter time frame, the legislature can respond to the advent of these new criminal opportunities by passing new criminal statutes that seek to address the underlying behaviour or use of that technology. Lawmakers tasked with deciding on which of these approaches to adopt in respect of a new technology are faced with two challenges relevant to the arguments outlined in this thesis: the *Collingridge dilemma*[4] and the pacing problem.[5] They also ought to be guided by general principles of criminalisation.

From a broad regulatory perspective, when faced with the question of whether new laws in respect of a technology are required, it is incumbent upon lawmakers to first assess whether that technology indeed presents anything *new* or unique.[6] Lawmakers must then consider whether that 'newness' of the technology is itself the catalyst for (re)consideration of legal responses or assumptions, or if there is some new broader legal or regulatory problem that ought to be addressed.[7] To date, much work in the area of technology regulation tends to focus on the perceived *newness* of a technology in the sense that the technology itself is new, not that it necessarily poses a new legal problem. This work also

[3] See, eg, *R v Jheeta* [2007] EWCA 1699. The defendant was charged with, amongst other offences, obtaining sexual intercourse by false pretences contrary to *Sexual Offences Act 1956* s 3 where the sexual intercourse was induced via the sending of coercive and deceptive text messages. Despite the act pre-dating the advent of SMS technology, the law was suitably flexible to respond in that situation: the technological ability to mask the identity of the true sender of the message merely expanded the possible ways in which a defendant could construct 'false pretences'.

[4] David Collingridge, *The Social Control of Technology* (Printer, 1980).

[5] Gary E Marchant, Braden R Allenby and Joseph R Herkert (eds), *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight, vol 7* (International Library of Ethics, Law and Technology, Springer, 2011).

[6] For a discussion on 'newness' as a lens to view 'technology regulation' in its broadest sense see Lyria Bennett Moses, 'How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target' (2013) 5(1) *Law, Innovation and Technology* 1, 6-10.

[7] See, eg, Monroe E Price, 'The Newness of New Technology' (2001) 22 *Cardozo Law Review 1885*.

tends to avoid considering the place and operation of that technology within the broader regulatory landscape, be it civil, administrative, or criminal.[8]

This focus on a technology and its perceived newness creates a risk that the technology itself may be treated as the 'regulatory target', thus resulting in restrictions on, or the prohibition of, specific modes or uses of that technology itself, rather than the social context surrounding it.[9] Further, when the *newness* of the technology inevitably fades away, so too does critical review, consideration, and scholarship on that technology and the associated legal issues.[10]

Concerns surrounding the challenges of focusing on a particular technology as a regulatory target are not new. In 1980, Collingridge expressed concern of two competing regulatory pressures with respect to responding to a technology at different stages of its development, thus coining what would become the *Collingridge dilemma*.[11] At the time lawmakers are first considering a new technology they are likely to be ill-equipped to understand that technology, its use, and its capacity to impact upon the citizenry. They are equally unable to predict how that technology will evolve, and the possible spectrum of harms that might result.[12] Indeed, it is often the case that courts and legislatures lack the necessary 'technical expertise and knowledge … to evaluate the 'workability' of statues' concerning the future use of a given technology.[13] Australian lawyer Philip Argy

---

[8] Bennett Moses (n 6) 2-6, attributes this to the varied approaches to, and definitions of, 'technology'; be it narrowly restricted to 'tools or crafts' or broadly inclusive of all 'means'. Her broader argument is that from the broader standpoint there is very little that separates 'technology regulation' from other forms of regulation: '[a]fter all, most regulation aims to influence a combination of people, things and relationships'. See, also, Roger Brownsword, 'Code, Control, and Choice: Why East is East and West is West' (2005) 25 *Legal Studies* 1.

[9] See, eg, Joseph H Sommer, 'Against Cyberlaw' (2000) 15 *Berkeley Technology Law Journal* 1145; Colin Tapper, 'Computer Crime, Scotch Mist' [1987] *Criminal Law Review* 4.

[10] Bennett Moses (n 6) 6.

[11] Collingridge (n 4).

[12] Marjolein van Asselt, Ellen Voss and Tessa Fox, 'Regulating Technologies and the Uncertainty Paradox' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf, 2010) 259.

[13] John P Dwyer, 'The Pathology of Symbolic Legislation' (1990) 17 *Ecology Law Quarterly* 233, 306.

has gone so far as to joke that 'most lawyers [and judges] wouldn't know the difference between a megabyte and a mozzie bite'.[14]

Alternatively, were lawmakers to wait until the effects of the implementation and use of a technology become clear, they risk socio-behavioural and enforcement challenges. Technologies gain momentum as they grow and become entrenched in the daily lives of citizens: the wider the scope of adoption of the technology, the more resistant that technology becomes to regulatory intervention.[15] Therefore, where lawmakers desire to minimise potential risks and social harms it is important for them to act and intervene early in order to shape both the design and implementation of the technology and the human behaviour and norms associated with its use.[16] But, as noted above, where they act too early, lawmakers risk failing to account for, or to adequately cover, those same risks.

Once a new technology has been both identified as a regulatory target and, in light of the Collingridge dilemma, the enactment of new laws has been considered appropriate, lawmakers face the *pacing problem*. The political and legal process is costly and slow-moving, a direct contrast to the fast-moving development of technology: here, commentators often rely on variations of the 'tortoise and hare' fable.[17] Lawmakers must, therefore, have regard to the risk of under-inclusiveness and the need to manage potential regulatory obsolescence.[18] As such, there can be a tendency to err on the side of over-inclusiveness, with provisions drafted such that possible future developments have the

---

[14] Philip Argy (ed), *Computers for Lawyers* (Longman Professional, 1986). The situation has perhaps only marginally improved, see, eg, the misguided approach in *R v Tsolomitis* [2012] SADC 12.

[15] Thomas Hughes, 'Technological Momentum' in Leo Marx and Merritt Roe Smith (eds), *Does Technology Drive History? The Dilemma of Technological Determinism* (MIT Press, 1994) as cited in Bennett Moses (n 6) 8.

[16] See, Wiebe E Bijker, Thomas P Hughes and Trevor Pinch (eds), The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology (MIT Press, 1987); Wiebe E Bijker, Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change (MIT Press, 1995).

[17] See, Lyria Bennett Moses, 'Agents of Change: How the Law "Copes" with Technological Change' (2011) 20(4) *Griffith Law Review* 763.

[18] Lyria Bennet Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (2007) 7 *University of Illinois Journal of Law, Technology and Policy* 239.

potential to fall within the scope of any proposed regulatory framework. This approach to drafting is argued to 'future-proof' the provisions, thus managing the need for them to be continuously revisited and updated. The provisions can be considered capable of 'keeping up' with underlying technological developments.[19]

In the criminal law context, techniques to achieve such future-proofing, or *technology neutrality*, include adopting drafting approaches that could be classified as risk-based, preventive, or inchoate-mode drafting, rather than harm or result-based drafting.[20] Offences drafted in this form can thus be broad in the sense that they have the, arguably useful, potential to respond to unforeseen malicious uses of various technologies, but also broad in the sense that they now additionally carry a further unintended potential to capture conduct previously not considered criminal, irrespective of the use of the technology.[21] This broad approach to drafting can also give rise to a misguided sense that the provisions are sufficient and appropriate if they are later observed to respond to new harmful uses of technology as they arise.

But, subsumed within these broader regulatory and practical tensions, when lawmakers seek to enliven the criminal law to respond to a technology, they ought to also have regard to the general principles of the criminal law. This is particularly the case when there is a reliance on ensuring over-inclusiveness to negate the effects of future technological developments: such an approach also needs to be appropriately justified

---

[19] See, Marchant et al (n 5). Not that this has necessarily prevented lawmakers from passing arguably outdated laws in other fields. In 2007 the Australian Parliament introduced a new exception into the *Copyright Act 1968 (Cth)* s 110AA that permitted the private copying of a cinematographic film *only* where that copying involves transferring the film from VHS to a digital format. All other copying for private use remains an infringement.

[20] While not specifically undertaken in response to computer-related crime *per se*, the amendments to the *Fraud Act 2006* involved a redrafting of offences in the inchoate mode: fraud became an offence of objective dishonesty where the accused is subjectively aware that their conduct would be viewed as such, rather than a result-based offence requiring proof of a deception. This shift was taken, at least in part, to ensure coverage of new 'chip and pin' payment technologies where no human was involved in the authorisation of the transaction. The broader effect of this style of drafting has been that the use of any form of technology in the commission of a fraud becomes irrelevant beyond the requirement to establish that the accused's conduct was dishonest.

[21] See, eg, David Omerod, 'The Fraud Act 2006: Criminalising Lying' [2007] *Criminal Law Review* 193; Andrew Ashworth, 'The Criminal Law's Ambivalence About Outcomes' in Rowan Cruft et al (eds) *Crime, Punishment, and Responsibility: The Jurisprudence of Antony Duff* (Oxford University Press, 2011) 159, 162.

within the overarching principles of the criminal law itself. Practical expediency is not sufficient.

Lawmakers engage, from a normative standpoint, in the process of *making* and *arguing* the justifications for a proposed new criminal law. Lacey refers to this as part of the broader process of 'legitimation' of the criminal law.[22] Legitimation occurs at the level of substantive legal doctrine (with appeals to objective and historical legal standards), and through the criminal process.[23] Concerning the criminal process, legitimation is achieved through the incorporation, enactment, and performance of the values of justice, legality, fairness, equality, and privacy, along with broader respect for human rights.[24] The criminalisation of a 'new' opportunity might then be considered appropriate where the construction of the proposed offence addresses and adequately responds to these considerations.

The confines of these broad principles that purport to legitimate or justify criminalisation in any given circumstance remain the subject of debate.[25] A coherent theory of criminalisation remains elusive, especially given the role politics and social perception plays in the legislative process. Indeed, in observing the 'unprincipled

---

[22] Nicola Lacey, 'Legal Constructions of Crime' in M Maguire et al (eds), *The Oxford Handbook of Criminology* (Oxford University Press, 4th ed, 2007) 193; Nicola Lacey, *In Search of Criminal Responsibility: Ideas, Interests, and Institutions* (Oxford University Press, 2016).

[23] See, Simon Bronitt and Bernadette McSherry, *Principles of Criminal Law* (Thomson Reuters, 3rd ed, 2010) 9.

[24] Ibid; Andrew Ashworth and Jeremy Horder, *Principles of Criminal Law* (Oxford University Press, 7th ed, 2013) 32. In respect of human rights, in practice these are those set out in the European Convention on Human Rights: freedom of expression, assembly and association, thought, religion, and a right to be free from discrimination. As Ashworth observes, at 32, all but the right to be free from discrimination are qualified rights, such that the criminal law might curtail these freedoms where 'necessary in a democratic society', referring, in respect of freedom of expression to *DPP v Collins* [2007] 1 Cr App R 5; *DPP v Hammond* [2004] Crim LR 851.

[25] See, eg, Lacey (n 22); RA Duff et al 'Towards a Theory of Criminalization' in RA Duff et al (eds) *Criminalization* (Oxford University Press, 2014) 1; Michael S Moore, 'Liberty's Constraint on What Should be Made Criminal' in Duff et al (eds) *Criminalization* (Oxford University Press, 2014) 182; Lindsay Farmer, *Making the Modern Criminal Law* (Oxford University Press, 2016); Stuart Green, 'Just Deserts in an Unjust Society' in RA Duff and Stuart Green (eds) *Philosophical Foundations of Criminal Law* (Oxford University Press, 2011) ch 16; Victor Tadros, *Wrongs and Crimes* (Oxford University Press, 2016); Deborah R Brock et al, *Criminalization, Representation, Regulation: Thinking Differently About Crime* (University of Toronto Press, 2014); Monique W Morris, *Pushout: The Criminalization of Black Girls in Schools* (The New Press, 2017); Andrew Ashworth, Lucia Zedner and Patrick Tomlin (eds), *Prevention and the Limits of the Criminal Law* (Oxford University Press, 2013).

expansion' of the English criminal law, with apparent disregard to the social significance of creating new crimes, Ashworth posed the rhetorical question of whether the criminal law is a lost cause.[26] This unprincipled expansion is evident in the increased blurring between the civil and criminal law, with Ashworth identifying the feature that distinguishes criminal cases from civil cases as, subject to exceptions, the procedure adopted in response to the conduct, rather than any reference to the content of the law itself.[27]

The apparent unprincipled nature of the criminal law more generally has in recent years received increased scholarly attention, particularly from within the United States. This attention has centred on the notion of *over-criminalisation*, with attention placed on examples of criminal offences that are applied far beyond their initial purview or result in too much conduct falling within their scope.[28] It remains difficult to establish a principled approach to the issue of over-criminalisation when the process of criminalisation itself remains subject to contestation. There is potential, however, for examples of alleged over-criminalisation to inform more detailed arguments in respect of principles of criminalisation.

This chapter sits at the intersection of these issues; the practical challenge of creating technology offences, the tendency to draft in a manner that preferences over-inclusivity in light of the realities of technological development, and the approaches to justifying the resulting offences with regard to the principles of criminalisation. First, this chapter sets out some of the principles identified by commentators that they argue ought to be considered when constructing and imposing criminal offences. The purpose here is not

---

[26] Andrew Ashworth, 'Is the criminal law a lost cause' (2000) 116 *Law Quarterly Review* 225.

[27] Ibid 232.

[28] 'Overcriminalisation' itself remains a contested concept vis-à-vis how it ought to be defined, and more importantly, measured. See, Douglas Husak, *Overcriminalization: The Limits of the Criminal Law* (Oxford University Press, 2007); Lisa H Nicholson, 'Sarbanes-Oxley's Purported Over-Criminalization of Corporate Offenders' (2007) 2 *Journal of Business & Technology Law* 43; Paul Rosenzweig, 'Overcriminalization: An Agenda for Change' (2005) 54 *American University Law Review* 809; Nicola Lacey, *In Search of Criminal Responsibility: Ideas, Interests, and Institutions* (Oxford University Press, 2016) 99-107; Stephen F Smith, 'Overcoming Overcriminalization' (2012) 102(3) *The Journal of Criminal Law & Criminology* 537; Erik Luna, 'The Overcriminalization Phenomenon' (2005) 54 *American University Law Review* 703; Darryl K Brown, 'Criminal Law's Unfortunate Triumph Over Administrative Law' (2011) 7(4) *Journal of Law, Economics and Policy* 657.

to contribute to the broader discussion of the development of these principles, but rather to set a baseline of potential considerations within which the approach *in fact* adopted by the Law Commission and Parliament in establishing the *Computer Misuse Act 1990* (the 'CMA') can be situated.

II GUIDING PRINCIPLES OF CRIMINALISATION

To criminalise a particular form of conduct, according to Ashworth and Horder, is to declare that the conduct constitutes a public wrong, to threaten punishment at the hand of the State to disincentivise that conduct, and to censure those who choose to engage in that conduct.[29] Questions therefore arise as to the nature and content of any limitations within the criminal law on the State's capacity to threaten and impose their power. Put another way, how might any given instance of criminalisation be justified?

In the broadest sense, Ashworth and Horder contend that such a process of justification ought to involve reference to broad democratic principles along with 'sufficient reasons for involving this coercive and censuring machinery'.[30] They go further, lending support to Husak's contention that in a liberal state there exists some form of individual right that might be expressed as 'a right not to be punished'.[31] As such, a given criminal law ought not to be justified 'on balance': a higher burden must necessarily be set.[32] But to what standard are these purported justifications to be measured? How might any limitations be normatively expressed?

---

[29] Ashworth and Horder (n 24) 22.

[30] Ibid.

[31] Husak (n 28) 92-103. Husak's work involves exploring the features that a theory of criminalisation should include, rather than prescribing such a theory. In doing so, he proposes that such a theory should incorporate something akin to a 'right not to be punished' as tool for delimiting situations where the punitive and coercive powers of the State might be appropriately enlivened. Husak adopts a distinction between punishment that 'overrides' or 'infringes' the right of the individual not to be punished (legitimate criminal sanction) from punishment that 'violates' that right (illegitimate criminal sanction). This right not to be punished becomes the benchmark against which Husak's four proposed internal constraints of the criminal law might be measured: that the '[p]enal statute must proscribe a non-trivial harm or evil; hardship and stigma may be imposed only for conduct that is in some sense wrongful; violations of criminal laws must result in punishments that are deserved; and the burden of proof should be placed on those who advocate the imposition of criminal sanctions.'

[32] Ashworth and Horder (n 24) 22.

Duff has described attempts to address these questions as part of the search for the 'master-principles' of criminalisation, noting that there are serious doubts that such principles might be adequately formulated: a principle with precise and determinate meaning tends to be 'under-inclusive', whilst broad principles become vague and thus 'can do no work in guiding or constraining' a decision to criminalise.[33] Thus, a failure suitably to articulate such master-principles results in any consideration of the appropriateness of a particular instance of criminalisation subject to 'piecemeal forms of evaluation'.[34] As will be seen, such a piecemeal approach must necessarily be adopted with respect to the considerations of the CMA set out in later chapters.

Despite these inherent difficulties and a period of avoidance, the issue of framing adequate principles of criminalisation has received renewed attention in recent years.[35] Much of the literature is concerned with considering and articulating limitations as to the type of conduct suitable for criminalisation, and the appropriateness or permissibility of the objectives of lawmakers. Edwards, while terming these the *content* and *reasons* questions respectively, offers a third consideration that he titles the *means* questions: how does the drafting of an offence achieve what was thought proper to criminalise?[36]

A *The Content and Reasons Questions*

The need to articulate principles that can be employed to consider the limits of the criminal law is important given that there is a seeming lack of constraining features inherent in a positivist conception of the criminal law. For the positivist, the criminal law can be understood as a discrete field with principles that can be understood without consideration of moral, political, economic, or other factors.[37] Here, the concept of crime

---

[33] RA Duff, 'Towards a Theory of Criminal Law' (2010) 84(1) *Aristotelian Society Supplementary* 19-20.

[34] James Edwards, 'Uses and Misuses of Criminalisation' (DPhil Thesis, The University of Oxford, 2011) 16.

[35] Nicola Lacey, 'Historicising Criminalisation' (2009) 72 *Modern Law Review* 936.

[36] Edwards (n 34) 10-11.

[37] This is a broad and contradictory claim given that, even for the positivist, the criminal law possesses an inherently political focus on individualism in coming to terms with understanding the principles of *legality* and *rationality*. See, eg, Alan Norrie, *Crime, Reason and History: A Critical Introduction to Criminal Law*

becomes one of name and process. An act becomes a crime because the State names it so, and the response to the commission of that act is punishment through the criminal process in the name of the State.[38] As was observed by Lord Atkin in *Property Articles Trade Association v Attorney-General (Canada)*:

> [T]he domain of criminal jurisprudence can only be ascertained by examining what acts at any particular period are declared by the State to be crimes, and the only common nature they will be found to possess is that they are prohibited by the State and that those who commit them are punished.[39]

This focus on proscription and punishment likely informed Ashworth's view, noted above, that it is the procedure adopted in response to proscribed conduct, rather the content of the law itself, that signifies whether something is to be considered a 'crime'.[40]

The positivist approach eschews questions that would consider the nature of crime or the utility of punishment, or further critique and evaluate the broader criminal justice project.[41] Arguments centre on the principle of legality, or the 'rule of law', tempered with consideration of the liberal notion of individualised justice and fairness. Fairness in this context generally refers to the administration of the criminal law process, not its substance. It does not require consideration of whether a particular form of conduct ought to be criminalised or decriminalised, as the case may be. Instead, it provides for a

(Cambridge University Press, 2014) 35-8. The point here goes to process: the political and moral considerations are left to be debated in chambers of parliament, while the resulting criminal law is to be interpreted and applied without further and additional reference to these considerations. See, further, HLA Heart, *The Concept of Law* (Clarendon Press, 1961); and Ronald Dworkin, *Law's Empire* (Fontana, 1986).

[38] Simon Bronitt and Bernadette McSherry, *Principles of Criminal Law* (Thomson Reuters, 4th ed, 2017) 6-7.

[39] [1931] AC 310, 324.

[40] Ibid 232.

[41] Bronitt and McSherry (n 38) 14-7.

'fair trial according to law'.[42] This view of fairness, as linked to process and procedure, has been supported by empirical evidence.[43]

While fairness is seemingly confined to the operation of the criminal process, work has thus needed to focus on providing a framework upon which the principle of legality can be understood. Legality, as observed by Spears, places a premium on the clarity, rationality and coherence of the criminal law.[44] It also serves as the means by which the broad democratic principles, referenced by Ashworth and Holder as noted above, can be framed. Work towards producing such a framework has centred on proposing principles that, when accepted and applied, serve a dual function: providing guidance to Edwards' *content* and *reason* questions. That is, they address the types of conduct that might properly be criminalised, whilst simultaneously, or inherently, setting out arguments that additionally support the appropriateness of the State criminalising that conduct. The most notable examples here are the *harm principle* and the *wrong principle*.

(a) The harm principle

The harm principle is attributed to Mill's work in political philosophy in the context of seeking to both delimit a community's ability to coerce an individual to behave in a particular way and consider the scope of permissible interference *between* individuals in that community. He observed that

> the only purpose for which power can be rightfully exercised over any member of a civilized community, against his [or her] will, is to prevent harm to others. His [or her] own good, either physical or moral, is not a sufficient warrant. He [or she] cannot rightfully

---

[42] As Gaudron J observed in the Australian High Court in *Dietrich v The Queen* (1991) 17 CLR 292 at 362:

> The expression 'fair trial according to law' is not a tautology. In most cases a trial is fair if conducted according to law, and unfair if not. If our legal processes were perfect that would be so in every case. But the law recognises that sometimes, despite the best efforts of all concerned, a trial may be unfair even though conducted strictly in accordance with the law. Thus, the overriding qualification and universal criterion of fairness.

[43] Even in circumstances where they might disagree with the outcome of a criminal matter, the general public place emphasis on the perception of procedural fairness of the criminal process as asserting confidence in the criminal justice system. See, Andrew Ashworth, 'Crime, Community and Creeping Consequentialism' [1996] *Criminal Law Review* 220, 228, citing Tom Tyle, *Why People Obey the Law* (Yale University Press, 1990).

[44] Donna Spears, 'The Criminal Justice System and the rule of law' (2008) 84 *Precedent* 18.

> be compelled to do or forbear because it will be better for him [or her] to so do, because it will make him [or her] happier, because, in the opinion of others, to so would be wise, or even right.[45]

Mill's position is framed in the negative sense, that is, his concern was to show the kinds of justifications for such interference that he believed were not sufficient or appropriate: the only permissible prohibition of conduct is confined to harmful conduct, rather than immoral conduct that results in no harm to others.[46] Thus, his position rejected paternalistic or moralistic justifications, instead preferring justifications that would go to the defence of an individual from another's harmful conduct.[47] This contention is founded firmly within concepts of liberalism, placing personal liberty, autonomy and individual rights as paramount considerations.[48]

The role and scope of 'harm to others' as a limitation on criminalisation has received substantial attention in both theory and practice[49] regularly being referred to, or regarded as, a 'master principle'.[50] The main difficulty in translating Mill's contention into the context of the criminal law has been creating and maintaining definitions of both 'harm' and 'others'. In respect of harm, is it limited to physical harm, or might it include

---

[45] JS Mill, *On Liberty* (Penguin, 1974) 68.

[46] Joseph Raz, 'Autonomy, Toleration and the Harm Principle', in Ruth Gavison (ed), *Issues in Contemporary Legal Philosophy*: *The Influence of HLA Hart* (Oxford University Press, 1987) 155; Ashworth and Horder (n 24) 28.

[47] Tatjana Hörnle, 'Theories of Criminalization' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 679, 688.

[48] Norrie (n 37) 19.

[49] For a seemingly rare example of theory directly informing practice see, for example, the discussion on approaches to criminalisation of harmful activities from a liberal, paternalist and moralist framework in the appendix of the Law Commission report into consent, albeit disconnected from the substantive discussion: Law Commission, 'Consent in the Criminal Law' (Consultation Paper No 139, 1995) 245-283.

[50] See, eg, Joseph Raz, *The Morality of Freedom* (1986), 418-19; Ashworth and Horder (n 24) ch 2; Husak, (n 28) 65-7; AP Simester and Andreas von Hirsch, *Crimes, Harms, and Wrong: On the Principles of Criminalisation* (Hart Publishing, 2011) 35-88.

psychological or economic harm?[51] Is intent, potential, or risk, of harm sufficient?[52] Must the harm be direct, or does protection from indirect harms justify State intervention?[53] When it comes to the requirement of the 'others', is it a limitation to be construed as against the interests of individuals, or is it sufficient to identify a harm posed at the community or social level?[54]

Feinberg proposed a somewhat broad conception of harm, as a 'setback to a person's interest', particularly welfare interests,[55] which is the result of wrongful conduct against another person.[56] That is, he subsumes a requirement of wrongfulness within the harm principle. Such a framing creates space to criminalise conduct that results in a harm beyond the physical to include other social and economic interests where caused by wrongful conduct: 'criminal prohibitions are legitimate only when they protect individual rights'.[57] It should be noted that Feinberg's position does not appear to have posited an

---

[51] See, eg, arguments as to the types of harms that might justify racial vilification laws in Wojciech Sadurski, 'Racial Vilification, Psychic Harm and Affirmative Action' in Tom Campbell and Wojciech Sadurski (eds), *Freedom of Communication* (Dartmouth, 1994) 77; Aleardo Zanghellini, 'Jurisprudential Foundations for Anti-Vilification Laws: The Relevance of Speech Act and Foucauldian Theory' (2003) 27 *Melbourne University Law Review* 458. See, further, in relation to considering the harm of 'offence'. Joel Feinberg, *Offence to Others* (Oxford University Press, 1988).

[52] See, eg, David Garland, 'The Rise of Risk' in Richard V Ericson and Aaron Doyle (eds) *Risk and Morality* (University of Toronto Press, 2003) 48; Stephen J Schulhofer, 'Harm and Punishment: A Critique of Emphasis on the Results of Conduct in the Criminal Law' (1974) 122 *University of Pennsylvania Law Review* 1497; Claire Finkelstein, 'Is Risk a Harm?' (2003) 151 *University of Pennsylvania Law Review* 963.

[53] See, eg, the interaction of suggested *indirect* harms in the broader context of conflicting public and private interests in arguments in respect of the criminal regulation of pornography in Nicola Lacey, *Unspeakable Subjects* (Hart Publishing, 1998) ch 3; H Potter, *Pornography* (Federation Press, 1996); John Braithwaite and Philip Pettit, *Not Just Deserts: A Republican Theory of Criminal Justice* (Clarendon Press, 1990) 96; Anne Orford, 'Liberty, Equality, Pornography: The Bodies of Women and Human Rights Discourse' (1994) 3 *Australian Feminist Law Journal* 72.

[54] See, eg, Paul H Robinson, 'A Theory of Justification: Societal Harm as a Prerequisite for Criminal Liability' (1975) 23 *University of California Los Angeles Law Review* 266.

[55] See, eg, John Kleinig, 'Crime and the Concept of Harm' (1978) 15(1) *American Philosophical Quarterly* 27, 29-30.

[56] Joel Feinberg, *Harm to Others: The Moral Limits of the Criminal Law* (Oxford University Press, 1987). See, also, Jonathan Schonsheck, *On Criminalisation: An Essay in the Philosophy of the Criminal Law* (Springer, 1994).

[57] Ibid 144. Feinberg appears here to be 'adding on' the consideration of the rights of others to the harm principle, in a similar vein to Mill, (n 45) 83; Husak (n 28) 71. Hörnle (n 47) at 691-2 questions whether it might be that the 'rights of others' consideration substitutes for the harm principle (and the later developed 'offence principle', see below n 58) while highlighting that the concept of 'rights' requires

exclusionary view, rather he observed that 'it is always *a good reason* in support of penal legislation that it would probably be effective in preventing … harm to persons other than the actor'.[58] That is, there may indeed be other reasons that could be relied upon beyond just requiring harm.[59]

The core of this approach has, however, generated considerable disagreement, with Ashworth pointing out that the 'setback to interests' approach does not adequately address the underlying fact that the notion of 'interests' is itself a product of moral, political, and cultural construction and circumstance.[60] Beyond this, Feinberg's position also requires supplementary work in the form of a theory of protected rights and a theory of wrongful conduct, and such work is lacking.[61]

Other scholars have sought to frame the harm principle as requiring a 'non-trivial harm', or noting weaknesses of the harm principle without such a criterion.[62] While arguing the harm principle has had a 'widely-perceived triumph … over legal moralism', Harcourt identified that the lack of a such a criterion, to consider 'non-trivial harms' or guidance as to how to consider competing claims of 'non-trivial harms', has allowed all kinds of arguments to be made in respect of what can be considered a harm suitable to

---

an explanation as to why a given interest is deemed sufficient to warrant the status of a right, and further the focus on rights permits the consequentialist focus of the harm principle to be sidestepped.

[58] Ibid 26 (emphasis added).

[59] See further, RA Duff, 'Harms and Wrongs' (2001) 5 *Buffalo Criminal Law Review* 13. Indeed, in his later work Feinberg supported an additional principle that would make it permissible to criminalise causing serious offence or hurt to other persons: that is, criminalisation is permissible where the conduct cause morally wrongful harm or offence to others. See, Feinberg (n 51). But *cf* AP Simester and Andrew von Hirsch, 'Rethinking the Offence Principle' (2002) 8 *Legal Theory* 269.

[60] Andrew Ashworth, *Principles of Criminal Law* (Oxford University Press, 4th ed, 2003) 33. Indeed, much the same can be said of the concept of harm itself in that the identification and designation of a result as being 'harmful' is shaped by the same considerations, see, Neil MacCormick, *Legal Right and Social Democracy* (Oxford University Press, 1982) 29.

[61] Husak (n 28) 72.

[62] See, Kleinig (n 54); Duff (n 58); Hamish Stewart, 'The Limits of the Harm Principle' (2010) 4(1) *Criminal Law and Philosophy* 17; Bernard Harcourt, 'The Collapse of the Harm Principle' (1999) 90 *Journal of Criminal Law & Criminology* 109; *cf* Alan Wertheimer, 'Victimless Crime' (1977) 87(4) *Ethics* 302 who makes the case that arguments for decriminalisation of crimes without harm are informed by political and policy interests, rather than developing philosophical principles.

justify offence creation.[63] Almost any conduct for which prohibition or sanction is intended can be construed as harmful in some way.[64] That such arguments have been made, accepted, and acted upon renders the harm principle largely ineffective in constraining the criminal law.

On this view, the harm principle became a victim of its own success, ultimately succumbing to the risk, identified by Duff above, that its acceptance and use has rendered it vague and thus not capable of doing any 'work in guiding or constraining' the criminal law.[65] It might be the case that the harm principle operates instead as an exclusionary guide, echoing the negative sense in which Mill framed his contention: it can be useful to identify conduct which ought not to be criminalised, but remains unconvincing as a source of reliance on what conduct should be criminalised. As Lacey, Wells, and Quick conclude, the harm principle might best be viewed as 'neither an ideal nor an explanation but rather as an ideological framework in terms of which policy debate about criminal law is expressed.'[66]

The requirement of some kind of harm is thus relevant but perhaps should receive less weight than has previously been suggested. That being said, Husak appears somewhat less convinced by the growing scepticism of the harm principle, suggesting that if the further work required to underpin Feinberg's view is successful it 'has enormous potential to retard the growth of the criminal law.'[67] In setting forth his overall position, however, Husak places limited reliance on the question of harm in isolation,[68] despite

---

[63] See, Bernard Harcourt, 'The Collapse of the Harm Principle' (1999) 90 *Journal of Criminal Law & Criminology* 109.

[64] See, eg, George Fletcher, *Rethinking Criminal Law* (Little, Brown & Co., 1978); Stephen Smith, 'Is the Harm Principle Illiberal?' (2006) 51 *American Journal of Jurisprudence* 1.

[65] Duff (n 33).

[66] Nicola Lacey, et al., *Reconstructing Criminal Law* (Cambridge University Press, 4th ed, 2010) 10.

[67] Husak (n 28) 72.

[68] Ibid. More broadly, Husak's contribution was to effectively incorporate the essence of the harm principle and the wrong principle into seven constraints on the criminal law. These constraints, he suggests, are split between those that operate within the criminal law itself, and those that ought to be imposed upon them. These constraints invariably concern themselves with both the content and the reason questions. In respect of the content question, Husak argues that offence definitions must target conduct which is both wrongful and deserving of punishment, must advance a legitimate State

arguing that the criminal law must implicitly require that there indeed be a non-trivial harm involved if we are to make sense of the operation of the defences of necessity, consent,[69] or a claim that the accused's conduct in a given case is *de minimis*.[70] Husak discusses these defences as a form of *justification* defences; they operate to justify the accused's harmful conduct where their conduct is the lesser of two harms in the context of necessity, where the harm is negated through consent, or where the conduct does not bring about the harm or does so only to a trivial extent.[71]

At this stage, it is necessary to point out that the discussion thus far has been implicitly premised on conduct that might directly cause harm. The question of whether it is permissible to criminalise conduct that might contribute *indirectly* or *remotely* to the causing of harms has also received considerable attention.[72] This has included consideration of a three-step 'fair imputation of harm' model:

1. is the remote act a 'but for' cause of the harm,
2. is the remote harm somehow normatively involved in the primary harm, or, if the response to either question was no,
3. is the matter of such urgency or the harm so grave that fairness should be set aside to permit the State to intervene.[73]

---

interest, and be no more extensive than is required to give effect to that interest. As to the reasons question, those same offences must be designed to prohibit a non-trivial harm.

[69] See, Peter Westen, *The Logic of Consent* (Ashgate, 2004).

[70] Husak, (n 28) 66-72. See, further, Douglas Husak, 'The De Minimus 'Defence' to Criminal Liability' in RA Duff and Stuart Green (eds) *Philosophical Foundations of Criminal Law* (Oxford University Press, 2011) 328.

[71] Ibid 66-7. On the question of whether or not *de minimus* is really a defence of justification, Husak notes that de minimus infractions might instead be considered as simply not sufficiently wrongful to enliven criminal liability in the first place.

[72] See, eg, above nn 53; Smith (n 63); Robert Mark Simpson, 'Dignity, Harm, and Hate Speech' (2013) 32 *Law and Philosophy* 701; Bryce Ryder, 'The Harms of Child Pornography Law' (2003) 36 *University of British Columbia Law Review* 101. Also see Edward B Royzman and Jonathan Baron 'The Preference for Indirect Harm' (2002) 15(2) *Social Justice Research* 165 for an empirical study on subjects' apparent use of 'directness' as a proxy for moral evaluation, rather than being explained based on intention, resulting harm, or disapproval.

[73] Denis Baker, 'The Moral Limits of Criminalising Remote Harms' (2007) 10(3) *New Criminal Law Review: An International and Interdisciplinary Journal* 370, 375-6.

Similar considerations form the basis of scholarship exploring the proliferation of inchoate and preventive offences, although informed by other considerations as to wrongfulness explored below.[74] There must clearly be some form of evidenced link between the conduct proscribed and an eventual harm that is sought to be minimised by these kinds of offences, but it is necessary to look beyond the harm principle in isolation to find suitable support.[75]

The connected, but seemingly underexplored, question in relation to the harm principle is how it might be appropriately utilised when the underlying conduct identified as 'harmful' actually enables a spectrum of possible harms that range from the trivial to the catastrophic. Such is the effect when the focus is on computer misuse: harms can range from nuisance and minor disruption, to financial loss, and potentially death. The same underlying conduct of interacting with the computer, mediated, however, by the use of different software or hardware tools, can result in any manner of these harms. This is not the same question as approaching indirect or remote harms; *any* given use of a computer could constitute either a direct or indirect harm. Nor is it necessarily the same as considering the risk or prevention of harm: does the mere possession of a computer constitute sufficient risk of harm to the user, either as the perpetrator or a victim? There is perhaps something deeper at play when the focus is on the misuse of computers as the *target* of criminal intervention than can be suitably addressed with reference to the harm principle.

---

[74] See below nn 92-3. See, in the American policing context, Markus Dubber, 'Policing Possession: The War on Crime and the End of Criminal Law' (2001) 91(4) *Journal of Criminal Law & Criminology* 829.

[75] See, eg, Henrique Carvalho, *The Preventive Turn in Criminal Law* (Oxford University Press, 2017); Andrew Ashworth and Lucia Zedner, *Preventive Justice* (Oxford University Press, 2014). At 43, Ashworth and Zedner, while observing the need to subject the harm principle to limitations, usefully explore Mill's testimony to the Royal Commission on the operation of the *Contagious Diseases Act 1866* which established a medical police force to patrol port and garrison towns and were empowered to require suspected prostitutes to undergo forced medical inspections, and provided for their forced detention and treatment. Further, the 1869 act required prostitutes to carry 'registration cards'. The apparent aim of the framework was to safeguard against the harms of contagious diseases, seemingly capable of being supported by Mill's harm principle. Mill, however, became a vocal critic, focusing on considering 'legislative intent' and 'distribution of liberty'. Mill's argued that had Parliament genuinely intended to safeguard against disease men would have been subject to the forced testing and registration, rather than just women.

(b) The wrong principle

In the context of defences that operate to 'excuse' an accused's conduct, Horder argued that such defences serve to 'excuse the act or omission amounting to wrongdoing, by shedding favourable moral light on what [the accused] did through a focus on the reasons that [the accused] committed that wrongdoing.'[76] In accepting this premise,[77] Husak argued that '[b]ecause wrongdoing is included in the concept of excusing conditions, it presupposes' that wrongfulness must operate as a constraint on the criminal law.[78] Indeed, for Feinberg, as was noted above, the conduct itself must be *wrongful*: it was not enough that conduct merely resulted in harm.

The concept of wrongfulness could be collapsed or subsumed within the harm principle, as is the case with Feinberg's approach.[79] It is useful, however, to consider them separately, particularly in light of the fact that the harm principle was founded, at least in part, as a liberal effort to escape legal moralism.[80] While there is broad agreement that crime involves some form of wrongful conduct that is of public concern,[81] the question of what constitutes that wrongfulness elicits a spectrum of views. Melissaris has categorised these views as falling within a stream of what might be termed liberal views and moralist views.[82]

The idea that the criminal law serves the function of enforcing morality has been gradually weakened, or has at least required reconceptualisation, as the criminal law has

---

[76] Jeremy Horder, *Excusing Crime* (Oxford University Press, 2004) 8-9.

[77] But not without qualification: see Douglas Husak, 'A Liberal Theory of Excuses' (2005) 3 *Ohio State Journal of Criminal Law* 287.

[78] Husak (n 28) 72.

[79] See, Feinberg (n 56).

[80] Emmanuel Melissaris, 'Theories of Crime and Punishment' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 356.

[81] See, Markus Dubber, 'Criminal Law Between Public and Private Law' in RA Duff et al (eds) *The Boundaries of the Criminal Law* (Oxford University Press, 2010) 191.

[82] Melissaris (n 80) 366-8. It might also be necessary to consider a third 'public interest' or 'community values' category as a compromise point: see, eg, Anthony Mason, 'The Courts as Community Institutions' (1998) 9 *Public Law Review* 83.

'secularised' from the late 18th century.[83] This has involved a move away from the primarily Christian teachings that had provided the normative framework of the criminal law, despite not being eliminated completely.[84] Concepts of morality as a framework for identifying wrongful behaviour within the criminal law also have, over time, perhaps shifted from the view as being a product of the divine to instead being presented on a more populist, secular, and community-minded basis. That is, the morality, or immorality, of conduct, and thus the identification of suitable objects of criminalisation, might be determined by asking the view of 'every right-minded person' within the community.[85] However, the notion of a shared morality, or the attempts to define objective secular values,[86] faces hurdles in a society that is both pluralistic and multicultural.[87] While an appeal to moral values might serve a contributory function in respect of some areas of the criminal law,[88] the discussion here in respect to the criminalisation of computer misuse will proceed on the basis that appeals to the liberal views of constructing wrongfulness provide more fertile ground for consideration. It might be said that computer misuse as a broad category would appear to rest on stronger appeals to individual quasi-proprietary interests, rather than necessarily resting on moral concerns.[89]

---

[83] Jeremy Horder, *Ashworth's Principles of Criminal Law* (Oxford University Press, 8th ed, 2016) 23.

[84] See, Bronitt and McSherry (n 38) 60-61; Patrick Devlin, *The Enforcement of Morals* (Oxford University Press, 1965).

[85] Devlin (n 84) 15.

[86] See, eg, John Finnis, *Natural Law and Natural Rights* (Oxford University Press, 1980).

[87] Moral disagreements abound in respect of issues such as the criminalisation of abortion, euthanasia and drug use to name but a few. This, however, does not preclude moralist perspectives on these issues from contributing to if and how such things are to be criminalised: these perspectives can operate as one of many guiding principles. See, Paul McCutcheon, 'Morality and the Criminal Law: Reflections on Hart-Devlin' (2002) 47 *Criminal Law Quarterly* 15.

[88] Particularly in relation to offences of a sexual nature or in respect of sexuality, where conceptions of morality play a substantial role in shaping the perception across various sections of society, see, eg, Nicholas Bamforth, *Sexuality, Morals and Justice* (Cassell, 1997); Carol Smart, *Law, Crime and Sexuality* (Sage, 1995); Carl Stychin, 'Unmanly Diversions: The Construction of the Homosexual Body (Politic) in English Law' (1994) 32 *Osgoode Hall Law Journal* 503.

[89] This is true in respect of the notion of gaining access to computers or computer materials that belong to another, but the claim is not made here that such a conception necessarily flows to issues surrounding the digitisation and proliferation of specific content that may indeed warrant a consideration of moral views and perceptions. The distinction here is as between a focus on *conduct* and a focus on *content*. Computer misuse assumes the former.

The starting position of the liberal view is that the mere fact that conduct involved a transgression beyond the properly constructed boundaries of individual freedom is wrongful. It is this framing that often results in the linking of the harm and wrong principles together: if the harm principle is satisfied with respect to a particular mode of conduct, thus justifying the imposition of limits by the State on individual autonomy, then any actions in excess of those limits must necessarily be wrongful. On this view, harm is a precondition for wrongfulness, or, more simply, wrongfulness is nothing more than harmfulness.[90] This framing, however, does not prove satisfactory across differing conceptions of harm, or when considered in respect of inchoate, risk-based, or preventive offences where no harm in fact results, appearing to ignore the proper of *mens rea* in favour of *actus reus*. Here, the harm identified to justify the offence might not correlate to the conduct that is, in fact, criminalised. In such cases, the wrongfulness or otherwise of an accused's conduct must necessarily be determined with reference to other factors. Such factors might include the concept of 'ulterior intent', which can serve as a means of signifying wrongdoing that may or may not support criminalisation.[91]

An ulterior intent can operate to render otherwise permissible conduct wrongful where that conduct is engaged in with a view to it playing a role in the commission of a substantive offence.[92] The various approaches to criminalising otherwise lawful conduct engaged in by an accused operating with an 'unlawful' intent have been justified in a

---

[90] Melissaris (n 80) 366.

[91] It is necessary to note, however, that wrongfulness and culpability are not the same thing, thus the use of 'intent' here may appear to cause some confusion or conflation. In the sense of considering wrongfulness, the intent with which an accused may carry out a specific series of conduct can be a relevant factor in determining that their conduct ought to be thought of as wrongful in the objective sense. Whether or not the accused is actually culpable for that wrongful conduct requires consideration of whether they did in fact subjectively possess such an intent and/or was aware of the circumstances.

[92] See, eg, Jeremy Horder, 'Crimes of Ulterior Intent', in Andrew Simester and Tony Smith (eds) *Harm and Culpability* (Oxford University Press, 1996); Peter Asp, 'Preventionism and Criminalization of Nonconsummate Offences' in Andrew Ashworth, Lucia Zedner and Patrick Tomlin (eds) *Prevention and the Limits of Criminal Law*, 23; Douglas Husak, 'The Costs to Criminal Theory of Supposing that Intentions are Irrelevant to Permissibility' (2009) 3(1) *Criminal Law and Philosophy* 51; Peter Westen, 'The Ontological Problem of 'Risk' and 'Endangerment' in Criminal Law' in Duff and Green (n 25) 304, 308; RA Duff, 'Intentions Legal and Philosophical' (1989) 9(1) *Oxford Journal of Legal Studies* 76, 88 where Duff explores the nature of 'ulterior intent' as an intent extending beyond the *actus reus* and its consequences, relying on the interpretation set out in *Jaggard v Dickinson* [1981] QB 527, at 532.

number of contexts.[93] In some cases, conduct might be considered wrongful enough to warrant criminalisation where there are limited, if any, legitimate uses or purposes for the underlying conduct. Those cases should also involve a correspondingly serious harm to protect against. Thus, there may be a presumption of criminal intent, and therefore wrongfulness, from the mere fact the conduct occurred.

The clearest examples of this formulation are possession offences. The possession of instruments for use in forgery[94] or the possession of offensive weapons[95] are perhaps justifiably deemed wrongful because there is no legitimate use case for that possession. An intent to commit a legitimately described non-trivial harm might be presumed from the possession of items for which the only reasonable use of those items would be to achieve that harm.[96] Outside these specifically proscribed cases, mere possession is generally not sufficiently wrongful where there may be an innocent explanation. Instead, wrongfulness arises where the accused's criminal intention affects the normative significance of their conduct, thus transforming conduct that might not, absent that intent, be wrongful.[97]

---

[93] See, eg, Law Commission, 'Conspiracy and Attempts' (Law Com No 318, 2009); JJ Child, 'The Structure, Coherence and Limits of inchoate liability: the new ulterior element' (2014) 34(4) *Legal Studies* 537; JJ Child and A Hunt, 'Mens rea and the general inchoate offences: another new culpability framework' (2012) *NI Legal Q* 245; Ian Leader-Elliot, 'Benthamite reflections on codification of the general principles of criminal liability: towards the panopticon' (2005) 9 *Buffalo Criminal Law Review* 391; Bernadette McSherry, 'Expanding the boundaries of inchoate crimes: the growing reliance on preparatory offences' in Bernadette McSherry et al (eds) *Regulating Deviance – The redirection of Criminalisation and the Futures of Criminal Law* (Hart Publishing, 2009) 141; GR Sullivan, 'Bad thoughts and bad acts' (1990) *Criminal Law Review* 559; Paul H Robinson, 'A functional analysis of criminal law' (1994) 88 *Northwestern University Law Review* 857; RA Duff *Criminal Attempts* (Oxford University Press, 1996); Michael T Cahill, 'Inchoate Crimes' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 513. For a discussion on Action Theory as applied to defining criminal conduct, see, eg, Leo Zaibert, 'Philosophy' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 132, 133-8; Gideon Yaffe, *Attempts in the Philosophy of Action and the Criminal Law* (Oxford University Press, 2010).

[94] *Forgery and Counterfeiting Act 1981* s 5(3).

[95] *Prevention of Crime Act 1952* s 1; *R v Jura* [1954] 1 QB 503; and *Williamson* [1978] 67 Cr App R 35.

[96] *Cf* Douglas Husak, 'Reasonable Risk Creation and Overinclusive Legislation' (1998) 1 *Buffalo Criminal Law Review* 599, 618.

[97] Horder (n 92) 157.

Consider, for instance, possession of a baseball bat. The mere possession of the bat is not in any way wrongful, nor is transporting that bat. However, an accused who picks up that bat and carries it menacingly while walking to another's property with an intent to swing it and bring it into physical contact so as to cause damage to that property has, even if no damage is in fact caused, changed the normative character of their possession of the bat. From the time the accused's handling of the bat became menacing, it was no longer just a baseball bat, but rather a tool to cause future damage. Having the bat in *that kind of* possession might be considered to have become wrongful.[98] Mere possession was not wrongful, but the accused's development of an ulterior harmful intent in its use changed the character of the possession.[99]

Similar reasoning can be observed in the construction of crimes that have a requirement that the accused engaged in conduct that, while wrongful, would be dealt with by areas of the civil law, such as tort, but for the presence of a further criminal intent. The offence of burglary perhaps most clearly captures such a position. Burglary requires that an accused entered into a building as a trespasser with the intent to either steal, inflict grievous bodily harm, or cause unlawful damage.[100] The offence does not require that there be any actual stealing or actual causing of grievous bodily harm; it is enough that the accused attempted to produce such results.[101] Here, we have conduct of an accused that constitutes a civil wrong, the physical trespass unto the premises, that while itself civilly wrongful, would not otherwise be sufficiently wrongful to warrant a response from the criminal absent that further ulterior intent.

The underlying trespass consideration for the purposes of the civil law would appear to respond to the unlawful interference with the victim's enjoyment of their premises, while burglary responds to the further and additional usurpation of the victim's interest in also controlling and protecting their personal property, or bodily integrity,

---

[98] Indeed, such conduct might in fact fall within *Criminal Damage Act 1971* s 3.

[99] See, further, Markus D Dubber, 'The Possession Paradigm: The Special Part and the Police Model of the Criminal Process' in RA Duff and Stuart Green (eds) *Defining Crimes: Essays on The Special Part of the Criminal Law* (Oxford University Press, 2005) 91.

[100] *Theft Act 1968* ss 9(1)(a), 9(2).

[101] Theft Act 1968 s 9(1)(b).

while on that premises. It is these additional qualities that might be said to justify rendering the accused's conduct sufficiently wrongful to warrant criminal sanction.[102]

But, the acceptance of the position that an ulterior intent can change the character of otherwise lawful conduct also broadens the scope of what might be deemed to constitute that trespass for the purpose of the offence beyond what may have been contemplated in its civil form. Consider, for example, circumstances where the accused might otherwise have a general authority to enter a building. The character of the accused's presence in the building could be 'cast in a new light' where an ulterior intent was operational: the intention to steal, or cause injury or damage, renders their otherwise authorised physical presence beyond the scope of the authorisation they may have had.[103] Thus, a customer who has an implied authority to enter a store to browse and purchase goods can be deemed a trespasser for the purpose of the offence of burglary where their entrance and presence in the store was influenced by a pre-existing or operational intention to steal: their implied authority is conditional.[104] While this example is not necessarily objectionable, it is evident that the degree of wrongfulness in a given course of conduct is important for delimiting between wrongs that might fall within the civil law from those within the criminal law,[105] and that this should be carefully constructed and considered when there is space for the criminal law to extend its reach.[106]

---

[102] *Cf* Arthur Ripstein, 'Beyond the Harm Principle' (2006) 34(3) *Philosophy & Public Affairs* 215, who, at 218-24, sets out consideration of the harm principle in respect to a 'harmless trespass' scenario. Here, however, alternative and separate means of constructing wrongdoing are not explored, instead the argument highlights the weaknesses in a sole reliance on the harm principle as outlined earlier in this chapter.

[103] See, eg, *R v Jones and Smith* (1976) 3 All ER 54; *Barker v R* (1983) 7 ALJR 425, 429; but *cf Collins* [1972] 2 All ER 1105; *Byrne v Kinematography Renters Society Ltd* [1958] 2 All ER 579.

[104] *R v Jones and Smith* (1976) 3 All ER 54, 59.

[105] See, eg, Matthew Dyson, 'The Timing of Tortious and Criminal Actions for the Same Wrong' (2012) 71(1) *Cambridge Law Journal* 86; Kenneth Simons, 'The Crime/Tort Distinction: Legal Doctrine and Normative Perspectives' (2007-8) 17 *Widener Law Journal* 719; Matthew Dyson, 'Tortious Apples and Criminal Oranges' in Matthew Dyson (ed), *Comparing Tort and Crime* (Cambridge University Press, 2015) 416.

[106] For a discussion on attempting to frame the criminal-civil distinction more generally, see Paul H Robinson, 'The Criminal-Civil Distinction and the Utility of Desert' (1996) 76 *Boston University Law Review* 201.

While the existence of an intent to inflict some additional form of harm might work to characterise conduct as perhaps sufficiently wrongful in the above examples, the same cannot be said for the other challenge to conceptions of wrongfulness: strict and absolute liability offences. Such offences seek to dispense with a *mens rea* requirement: that is, the conduct is criminal without resort to considering whether the accused had any intent or, perhaps, any knowledge that their conduct was contrary to the law. Thus, in contrast to the examples above, there is no mechanism to assess the character of the conduct in light of any specific intention on the part of the accused, harmful or otherwise. On this point, Husak suggests that arguments that such offences are unjust might be explained as being a product of the offences not requiring *enough* wrongdoing on the part of the accused.[107] Or, that any perceived wrongdoing is disproportionate to the punishment imposed.[108] Any judgement on the wrongfulness of conduct, however, remains controversial, especially without further theoretical support.[109]

Despite this, the practice of criminalising conduct that may be construed as wrongful in the senses described above have proliferated in recent times in an *ad hoc* manner. Horder, for instance, observes that it is a crime to possess a shotgun with the intent to endanger life, but no such crime exists for the possession of a poison held with the same intent.[110] Both might be thought of as similarly wrongful. Horder's position is not necessarily to admonish the criminalisation of those wrongs, but rather to respond to, and further develop, arguments first set out by Glazebrook in the context of exploring the operation of the inchoate crime of attempts,[111] that Parliament ought to 'painstakingly

---

[107] Husak (n 28) 74. For other views on how some strict liability offences might be justified see, RA Duff, *Punishment, Communication, and Community* (Oxford University Press, 2001) 56-66, 79-82; Andrew von Hirsch, *Censure and Sanctions* (Oxford University Press, 1993) ch 2; Alan Michaels, 'Constitutional Innocence', (1999) 112 *Harvard Law Review* 828; Jeremy Horder, 'A Critique of the Correspondence Principle in Criminal Law', (1995) *Criminal Law Review* 770; Jeremy Horder, 'How Culpability Can, and Cannot, Be Denied in Under-age Sex Crimes' (2001) *Criminal Law Review* 15.

[108] Douglas Husak, 'Strict Liability, Justice, and Proportionality' in Andrew Simester (ed) *Appraising Strict Liability* (Oxford University Press, 2005) 81.

[109] See, eg, Richard Singer and Douglas Husak, 'Of Innocence and Innocents: The Supreme Court and *Mens Rea* Since Herbert Packer' (1999) 2 *Buffalo Criminal Law Review* 859.

[110] Horder (n 92) 155. Unless the 'poison' in question is a controlled substance, in which case possession of the 'poison' may itself constitute an offence; see, *Misuse of Drugs Act 1971* s 5(1).

[111] See, Peter Glazebrook, 'Should We Have a Law of Attempted Crime?' (1969) 85 *Law Quarterly Review* 28.

… prohibit all the specific kinds of conduct worthy of condemnation as criminal, when done with the intention to commit the crime'.[112] These observations, however, become less about determining what conduct is sufficiently wrongful to warrant criminal sanction, but rather how the graduated criminalisation of conduct across a logic sequence or chain of wrongfulness (from initiating the conduct to the resulting harm) might be better structured and organised.[113]

In respect of computer misuse, the physical conduct of possessing, interacting with, and using a computer would appear to have limited distinguishing features between legitimate and wrongful conduct. The physical acts of the accused become mediated by different software and hardware. While the *type* of software used might serve as an indicator of wrongfulness, any effort at criminalisation ought to involve the incorporation of a clear intent, or ulterior intent, requirement that can be relied upon as the basis to consider a given instance of computer misuse as wrongful. That is, there ought to be some intent mechanism that enables the conclusion that an accused's otherwise lawful conduct involving a computer has been normatively transformed into wrongful conduct.

B The Means Question

While the harm and wrong principles are of some assistance in addressing the content question and the reasons question, there is a need to consider Edward's third category: the *means* question.[114] That is, after considering the *what* and *why* of a criminal offence, attention should focus on the *how*.[115] The means question thus requires attention to how the State went about achieving a particular objective. That objective might itself be justified, for instance, by reference to the harm and wrong principle, but the mechanism actually imposed by the State in giving effect to that objective may itself not

---

[112] Horder (n 92) 157.

[113] Horder and Glazebrook's broader argument for clearly defined graduated offences also relied on references to the principle of parsimony in offence definition and that such offences would support maximum certainty or fair warning. See, further, Peter Alldridge, 'Making Criminal Law Known' in Stephen Shute and Andrew Simester (eds) *Criminal Law Theory: Doctrines of the General Part* (Oxford University Press, 2002) 103; Ashworth (n 60) 80-2.

[114] Edwards (n 34) 10-11.

[115] Ibid.

be justified by the same arguments. Not only do lawmakers make a decision as to whether the criminal law ought to be employed to achieve their objective rather than the civil law, but also they decide how the 'design and presentation' of a criminal offence will be defined.[116]

In highlighting the need to explore questions around what approaches to designing and defining crimes might be legitimate, Edwards observes that there may be examples where lawmakers have sought to

> prohibit behaviour which does some trivial harm to others without any intention that potential offenders advert to the prohibition, intending only that the prohibition assist officials in prosecuting those thought to have caused this (or a more serious) harm. The intention need not even be that the trivial harm be *reduced*; it may simply be that the prosecutions thereby facilitated will reduce the incidence of other, more serious harms. This is enough to show that the question of means is *not* resolved by our answers to the content and reasons questions.[117]

This argument suggests that while the principles briefly explored above may play a role in providing legitimation for enlivening the criminal law, those principles cannot be understood as supplying sufficient legitimacy to the way lawmakers in fact did so. It may instead be the case that lawmakers, as Edwards argues, have misused their power to criminalise where the definitions for, and application and enforcement of, specific crimes exceed available justifications.[118]

Such an alleged misuse of power to criminalise may not always be the product of any specific intention of lawmakers to do so.[119] The criminal process engages multiple stakeholders and institutions: the police, who decide how to allocate investigative resources; prosecutors, who operate with discretion as to which charges to pursue; and

---

[116] Ibid 18.

[117] Ibid 17.

[118] Ibid.

[119] There are of course arguments to be made in respect of being able to discern a clear intention in an act of Parliament in the first place, given the deliberative nature of the process and the involvement of a vast number of individuals. Suffice to say, much of what has been described so far in this chapter cannot be understood but for the assumption that a criminal law can exhibit an identifiable objective. See, eg, Husak (n 28) 133-4; Edwards (n 34) 23-4.

the Courts, who are tasked with interpreting the confines of the crime and determining whether a given defendant ought to be convicted and sentenced.[120] Beyond this, it may also be the case that the underlying factual matrix of the conduct lawmakers initially envisaged in constructing the offence may fundamentally change or evolve. This could be due to changing behaviour, changing technology, or better understandings of risk. An instance of criminalisation may, therefore, result in unintended consequences or be taken in unforeseen directions that do not accord with the initial justifications that supported the creation of that offence.

Edwards develops his approach through the identification of three types of offences that lack convincing justification either under principles of legality or broader principles of governance: 'ouster offences',[121] 'empowering offences',[122] and 'prejudicial offences'.[123]

Ouster offences are those offences where lawmakers have failed, either unintentionally or deliberately, to include the elements of the wrongdoing that justified the creation of the offence in the definition of that offence. That is, the wrongfulness of the conduct and any resulting harms that are sought to be prevented or managed by the State are excluded from the words and structure of the offence itself and therefore excluded from judicial consideration. Thus, this type of offence would achieve what may otherwise be a legitimate objective of the State through a process that denies the accused and the Court the ability to assess the very conduct used to justify the offence. This view is based on the notion that in situations where lawmakers have narrowly defined the legal rights and duties of individuals pursuant to some objective broader than the substance of the offence, the Courts are *ousted* from considering whether the accused before them is a proper target for censure or punishment.[124]

---

[120] Edwards (n 34) 20-1.

[121] Ibid ch 2.

[122] Ibid ch 3.

[123] Ibid ch 7.

[124] Ibid 45.

As an example of this kind of offence, Edwards puts forward the offence of making a statement likely to be understood as indirect encouragement of an act of terrorism.[125] Here, the conduct that justified criminalisation is the incitement of violence, but the resulting offence covers the making of a mere statement that may be construed as indirect encouragement, even where the making of the statement was reckless.[126] The Court is thus ousted from considering whether the accused was directly involved in inciting violence or ought to be sanctioned with the label 'terrorist'. Similar arguments can be made in respect of the criminalisation of sexual conduct between two teenagers under the age of 16.[127] The framing of these offences thus remove judicial hurdles to conviction. Tangible evidence difficulties and prosecutorial expediencies result in offences that deprive the accused and the Court the capacity to *fully* adjudicate on the underlying conduct. This approach raises clear concerns of procedural unfairness and legality.[128]

Empowering offences are offences that fail to provide useful and adequate warning or notice to potential offenders such that the lack of warning corresponds with an increased ability for law enforcement to achieve the objectives of lawmakers through arrest and prosecution.[129] These offences contribute to an increased ability for arrest because they either address conduct that lawmakers had no real intention to prevent entirely,[130] or where the offence is little publicised, or its true scope of potential application is unknown.[131] The content and structure of such offences thus allow lawmakers to achieve their objectives through subverting principles of legality, namely

---

[125] Ibid 40-2. See, *Terrorism Act 2006* s 1(2)

[126] See further, Joint Committee on Human Rights, *Third Report of Session 2005-6, Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters* (2005-06, HC 561-I) 17-8.

[127] Edwards (n 34) 42. See, *Sexual Offences Act 2003* ss 9, 13.

[128] Ibid ch 2. Specifically, additional concerns arise here as to the principle of fair labelling. See, James Chalmers and Fiona Leverick, 'Fair Labelling in Criminal Law' (2008) 71(2) *Modern Law Review* 55.

[129] Ibid ch 3.

[130] Ibid 88-91. See *Fraud Act 2006* s 2(1) where Edwards argues there was clearly no intention to fully prevent the making of a misleading state in pursuit of benefit.

[131] Ibid 91-2. Edwards uses the example of threatened prosecutions against individuals wearing 'Bollocks to Blair' T-Shirts pursuant to *Public Order Act 1986* s 5(1) which, subject to criteria, makes it an offence to display abusive or insulting writing.

the principles of fair warning.[132] For this style of offences, the net is 'cast wide', with the effect that the power to determine the confines of what is or is not criminal behaviour is delegated to police and prosecutors: their discretion, resource allocation, and internal policies become the criminal law by default.[133]

Prejudicial offences are those offences that seek to either directly or implicitly imbue a particular assumption about the *class* of persons likely to commit a particular wrong as the *class* who will, therefore, be guilty of committing such a wrong.[134] The effect is that the conduct of members of that class is prejudged as criminal by the mere fact of their membership. The ability for such offences to be contemplated, that is as a law that targets a minority group or class, is arguably a product of the majoritarian nature of legislative institutions, amongst other socio-political phenomena.[135] Such offences, according to Edwards, cannot be justified because a government which enacts such offences does not warrant the trust of their citizenry.[136] Again referencing the terrorist offences mentioned above, amongst others, Edwards highlights that such offences inherently assume that the type of people suspected of 'terrorist activities' will be the ones guilty of terrorist acts.

In light of these considerations, and in returning to the subject of criminalising computer misuse, any attempt to grapple with the challenges in respect of the spectrum of possible harms of computer misuse (from the trivial to the most serious) and the ability to categorise the underlying physical use and interaction of computers as wrongful, as identified above, ought to be further constrained so as to avoid, as far as possible, the features identified as constituting ouster, empowering, or prejudicial offences. Thus, any

---

[132] Ibid ch 7.

[133] See, eg, William J Stuntz, 'The Pathological Politics of Criminal Law' (2001) 100(3) *Michigan Law Review* 505; Celesta A Albonetti, 'Prosecutorial Discretion: The Effects of Uncertainty' (1987) 21(2) *Law & Society Review* 291; Robert L Milsner, 'Recasting Prosecutorial Discretion' (1996) 86(3) *Journal of Criminal Law and Criminology* 717; William F Baxter, 'Separation of Powers, Prosecutorial Discretion, and the "Common Law" Nature of Antitrust Law' (1981-2) 60 *Texas Law Review* 661.

[134] Edwards (n 34) ch 7.

[135] This is also present, at least implicitly, in the liberal view of wrongfulness in that while attempting to separate itself from religion centred moral concepts has seemingly adopted a quasi-majoritarian secular form of morality. See, above nn 84-7.

[136] Edwards (n 34) ch 7.

offences proscribing computer misuse ought to be constructed, as far as is reasonable and justifiable, so as not to remove the consideration of the identified harms and their risk from the construction of the definitions within the offence itself. The drafting of the offence should provide clear and adequate guidance as to the forms of computer use that will justifiably elicit an arrest or prosecution. Any offences should avoid becoming imbued with any notion or assumptions as to type or class of persons who might engage in computer misuse.

III CONCLUSION

This chapter laid the foundation for a discussion of the construction and operation of the CMA in respect of both the broad regulatory challenges presented by technology and the existence of internal and external constraints of the criminal law: select principles within criminalisation theory. It began with the identification of the Collingridge dilemma and the pacing problem. Lawmakers are faced with having to balance on the one hand the potential pitfalls of early intervention in an attempt to address the risks and harms posed by a 'new' technology where such risks and harms might not be foreseeable, and on the other hand intervening too late to have a meaningful impact on the development of the culture, capabilities, and uses of that 'new' technology. Assuming, of course, that the technology indeed represents anything new.

When recourse is sought within the criminal law, the creation of any offence ought to have regard to whether the subject matter of the offence justifies the exercise of the State's power to criminalise. That is, can a suitable harm or risk of harm be identified that enlivens the State interest in protecting and defending the interests of individuals, and can that conduct be suitably identified and considered criminally wrongful? If so, the construction of any offence ought to then be such that the definitions of conduct and culpability within the offence are commensurate with the harm or risk of harm that was identified. The offence ought not to presuppose wrongdoing, nor should it be constructed and applied such that those subject to that prohibition are unaware, or inadequately informed, of its scope.

The degree to which the offences within the CMA have been successful in navigating these constraints and considerations, in particular the unauthorised access to

data offence as proscribed by section 1, substantially informs the discussion throughout the rest of the chapters of this thesis, beginning first with introducing the content and scope of the Law Commission Working Paper[137] and their Final Report on Computer Misuse.[138] Chapter 2, therefore, will seek to explore how law and policymakers sought to frame and conceptualise the harms of computer misuse and the forms of wrongdoing they identified.

[137] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988).

[138] Law Commission, 'Criminal Law: Computer Misuse' (Report No 186 Cm 819, 1989).

Chapter 2

Defining Computer Misuse: Computer Crime in the 1980s and the Law Commission Working Paper

---

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. The appellants' conduct amounted … to dishonestly gaining access … by trick. That is not a criminal offence.

Lord Lane CJ [1]

I Introduction

When faced with having to decide on whether a new criminal offence in respect of a technology is required, it was observed in Chapter 1 that consideration ought to be placed on whether that technology presents anything new in respect of the substantive criminal law. Often, however, the decisions of law and policymakers are shaped not only

[1] *R v Gold; R v Schifreen* [1987] 3 All ER 618, 622-3. This quote has been misattributed, perhaps surprisingly too often, to Lord Brandon of Oakbrook who, in writing the opinion unanimously endorsed in the subsequent appeal to the House of Lords, merely quoted the Court of Appeal judge's observation; *R v Gold and Anor* [1988] 2 All ER 186, 191.

by matters of substance and principle but also by politics and perception. Despite this, it was suggested that any proposal for a new offence ought to attempt to provide a clear rationale for its creation and implementation, along with justificatory support by reference to at least some form of identifiable harm resulting from a definably wrongful and causatively connected act or course of conduct. The structure and definition of any such offence should balance the legitimate interests of the State with individual autonomy. Further, the actual drafting of the offence ought to be capable of being supported by the same claims made in proposing it.

In assuming that this position is broadly correct, this chapter sets out to contextualise how law and policymakers in fact approached and rationalised these considerations in the work that would ultimately contribute to the formulation of the *Computer Misuse Act 1990* (the 'CMA'). The chapter will begin first with a brief introduction to the techno-political context surrounding the push to investigate, name, and criminalise computer misuse. This will involve considering the nature and use of computing technologies as they existed and operated up to and including the late 1980s, along with the high profile 'hacking' cases and resulting attention given to computers by both the popular media and the courts. The chapter then moves to set out the initial positions proposed by the Law Commission's Working Paper on Computer Misuse, released for consultation in September 1988.[2]

II PUBLIC ATTENTION, CRIMINAL CONCERN

The criminal law has consistently grappled with new forms of technology: in that sense, computers are not unique. What makes computers particularly challenging, however, is their ability to, in a sense, intermediate conduct, making possible a wide variety of results from a core set of interactions. The computer as an *intermediate* thus creates separation, or dissonance, between the precise act of an accused (for example, typing keys on a keyboard) and the effect of that conduct (any resultant technical, economic, or physical harm). The resulting effect of the conduct is mediated by the design and capabilities of the software operated. This separation between a given computer-

[2] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988).

mediated act and the experienced effect necessitates serious consideration of the target and focus of criminality.

A focus on specifically criminalising the act of making *use* of a computer could result in proscribing otherwise benign conduct and possibly require the need for constant revision and amendment. A focus on criminalising the *effect* produced by such use might not sufficiently disincentivise risky or harmful behaviour. Further, this might result in reliance on general (or pre-existing) offences to prosecute behaviour, only to have those prosecutions fail due to the rigidity of definitional interpretations constructed and conceived by both the legislature and the Courts in the absence of computers. This latter possibility was the problem that in fact arose during attempts to prosecute individuals who had 'caused damage' to computers,[3] or had obtained the use of a network subscription service by use of another's access credentials (passwords).[4] By the time these incidents came to a head in the 1980s, computing technologies had evolved from their military and research origins tobecome mass-market consumer products.

A *The Development of Computing Technologies*

Conceived in 1937, John Atanasoff at the Iowa State College (later University), along with his graduate student Clifford Berry, built the first electronic computer capable of solving linear equations as a proof of concept prototype in 1939. They completed a successful test phase of a full-scale version in 1942 before work was abandoned to refocus efforts during World War II.[5] Mechanical 'computing' devices had been devised much earlier,[6] but the Atanasoff-Berry Computer was the first to conceive and implement a

---

[3] *Cox v Riley* (1986) 83 Cr App R 54; *R v Whiteley* (1991) 93 Cr App R 25.

[4] *R v Gold and Anor* [1988] 2 All ER 186.

[5] See, Clark R Mollenhoff, *Atanasoff: Forgotten Father of the Computer* (Iowa State University Press,1988); Jane Smiley, *The Man Who Invented the Computer* (Doubleday, 2010); Alice Rowe Burks, *Who Invented the Computer? The Legal Battle that Changed History* (Prometheus Press, 2003).

[6] See, Tom Wheeler, *From Guttenberg to Google: The History of Our Future* (Brookings Institution Press, 2018) 121-3. For example, Charles Babbage's Analytical Engine, designed in 1834, and the Difference Engine No 2, designed between 1847-9, but remaining unbuilt until 2002. The Difference Engine No 2 comprises 8000 parts and is 11 feet long, weighing in at five tons. In his work, Babbage conceived of many of the core components and functions of what we recognise in computers today, describing them in the language available in the 19th century with the ultimate descriptor that the Analytical Engine was a 'locomotive that lays down its own railway'.

binary digital system facilitated by the on/off states of electricity flowing through a controlled circuit.[7] Their achievement went unrecognised until 'rediscovered' during a patent dispute in relation to the Electronic Numerical Integrator and Computer ('ENIAC') which is generally regarded as the first 'general-purpose computer.[8] ENIAC was built in 1945 and designed by John Presper Eckert and Joh Mauchly to compute artillery firing tables for the United States Army Ballistics Research Laboratory. But, at around the same time the United Kingdom had, in secret, built and operated a set of computers at Bletchley Park[9] named 'Colossus': the first of which was operational in December 1943, and in active use in 1944. Colossus was designed and used to break the *Lorenz SZ-40* cypher, then in use by the German High Command, allowing the Allied forces to intercept high-level German military intelligence. Due to the immense secrecy surrounding the operation, this achievement was not publicly acknowledged until 1974.[10]

Those involved in these and similar computing projects during the war would go on to be influential in the continued development of computing technologies. In 1948, for example, Norbert Weiner published his book *Cybernetics*, both coining the phrase 'cybernetic' and providing an influential contribution to the future development of artificial intelligence research. His experimental work involved the development of anti-aircraft systems that attempted to use data from radar to predict and plot enemy flight

[7] Ibid 120.

[8] See, Burks (n 5).

[9] It would be remiss to mention Bletchley Park and fail to highlight the contributions to both computing and the war effort made by Alan Turing. Despite his contributions to computing during and after the war, Turing was excluded from work at the renamed Government Communication Headquarters (GCHQ) due to a policy of 'known homosexuals' being ineligible for security clearances, a product of the alliance and closer cooperation with the United States. Turing was later arrested in Manchester in 1952 for having a sexual relationship with another man but, rather than a prison sentence, Turing agreed to receive oestrogen injections. He is believed to have committed suicide by ingesting cyanide in 1954. See Andrew Hodges, *Alan Turing: The Enigma* (Princeton University Press, 2014).

[10] See, Frederick William Winterbotham, *The Ultra Secret: Inside the Story of Operation Ultra, Bletchley Park and Enigma* (Orion Books, 2000). Winterbotham, at the time of the War a member of MI6, had been appointed to head and train 'Special Liaison Units' who had the responsibility of distributing and communicating the contents of the decoded German intelligence from Bletchley Park to the relevant field commanders without arousing suspicion. His book, originally published in 1974, was his personal account of the time and was also the first book (in English) to discuss Bletchley Park and Colossus publicly.

paths.[11] The first computer that could store a program in memory was built at the University of Cambridge in 1949 by a team led by Maurice Wilkes who, three years earlier, had attended a public lecture series at the University of Pennsylvania focusing on ENIAC.[12] In the same year, British born Trevor Pacey, who had abandoned his doctoral studies in physics at Imperial College London to join the Air Defence Research Development Establishment during the war before emigrating to Australia in 1945, had, independently of the work in the United Kingdom, designed and built the Commonwealth Scientific and Industrial Research Automatic Computer ('CSIRAC') in Sydney, before it was relocated to the University of Melbourne in 1956. CSIRAC, the fourth operational stored-program computer in the world, was the first to be built outside the United States or the United Kingdom and is now the oldest surviving electronic computer.[13]

With military and academic approaches continuing to influence the design and application of emerging computing technologies, the ability to use and interact with computers remained a highly skilled and specialised endeavour. This began to change when John Presper Eckert and John Mauchly, designers of ENIAC, produced and sold the first commercially produced computer in the United States, the Universal Automatic Computer I ('UNIVAC I').[14] The first of the UNIVAC I series was purchased by the United States Census Bureau in March 1951. The fifth UNIVAC I sold, built for the United States Atomic Energy Commission, was used by the CBS radio and television network to predict the results of the 1952 presidential election. Based only on a sample of data from 1% of voters, UNIVAC successfully predicted, contrary to available polling

[11] Norbert Weiner, *Cybernetics: Or Control and Communication in the Animal and the Machine* (MIT Press, 2nd ed, 1965). Weiner adopted cybernetic, with the prefix 'cyber' later adopted widely with respect to computers, from the ancient Greek word *kubernḗtēs* (or κῠβερνήτης) which meant 'helmsman' or 'steersman'.

[12] See Maurice Wilkes, *Memoirs of a Computer Pioneer* (MIT Press, 1985); Simon Lavington, *Early British Computers*, (Digital Press, 1980) Ch 6.

[13] See, 'CSIRAC Chronology', *University of Melbourne* (Web Page) <https://cis.unimelb.edu.au/about/csirac/chron.html>.

[14] John Presper Eckert et al, 'The UNIVAC System' (Conference Paper, 1951 International Workshop on Managing Requirements Knowledge, 10 December 1951) 6.

data, a landslide for Eisenhower.[15] None of this would have been possible, however, without the vital work of mathematician Grace Hopper who designed A-0, a program that allowed users to provide instructions to UNIVAC in English, rather than using numbers.[16] A-0 was one of the first versions of what today is known as a compiler, the bedrock of modern computer programming and a major leap forward in the development of computing technologies.

The 1950s also saw the development of the first computer games. Australian John Bennett, an employee of British computing firm Ferranti, designed an electronic version of 'Nimrod', a simple game where players take turns removing matchsticks from a pile intending to be the player who takes the last match. Ferranti built the game and showcased it at the Festival of Britain in 1951.[17] In 1952, Alexander Douglas designed OXO, an electronic version of 'naughts and crosses', while a PhD student the University of Cambridge,[18] and Christopher Strachey designed and played a simulated game of draughts.[19] 'Tennis-for-Two' came as another innovation later 'rediscovered' during a patent lawsuit, which had been designed in New York in 1958 and, as the name implies, allowed two players to play tennis on a Donner Model 30 analogue computer connected to an oscilloscope display.[20]

---

[15] Stephen Feinberg, 'Memories of Election Night Predictions Past: Psephologists and Statisticians at Work' (2007) 20(4) *CHANCE* 8, 10-1.

[16] Grace Hopper would go on to further refine this approach, producing MATH-MATIC in 1957, with her earlier work leading the development of the first English-language business data compiler B-0 (FLOW-MATIC) also released in 1957. See, Kurt Beyer, *Grace Hopper and the Invention of the Information Age* (MIT Press, 2012); Kathleen Broome Williams and James C Bradford, *Grace Hopper: Admiral of the Cyber Sea* (Naval Institute Press, 2013).

[17] See, Tristan Donovan, *Replay: The History of Video Games* (Yellow Ant, 2010) 1-9.

[18] Ibid.

[19] Ibid. See, further, Siobhan Roberts, 'Christopher Strachey's Nineteen-Fifties Love Machine', *The New Yorker – Annals of Technology* (14 February 2017) <https://www.newyorker.com/tech/annals-of-technology/christopher-stracheys-nineteen-fifties-love-machine>.

[20] *Magnavox Co. v Activision, Inc.*, 848 F.2d 1244 (May 09, 1988). Tennis-for-two was largely forgotten, having been design for a three-day public exhibition before being dismantled. Re-discovery of the game was relied on in attempts to invalidate patents held in respect of the game Pong and its operation on televisions by way of a gaming console.

Throughout the 1960s innovations, both technical and commercial, continued. Supercomputers were designed and built by Universities and manufacturers, and large computing systems (mainframe systems) were designed and sold to businesses. Notably, the introduction of IBM's System/360 series of mainframes in 1964 and, in the same year, the launch of the SABRE electronic reservation system initially designed for American Airlines.[21] SABRE involved the linking of over 2000 terminals (access devices) across 65 cities in the United States to a pair of IBM 7090 systems and was capable of delivering flight data through telephone lines in under 3 seconds. Even today, SABRE remains the basis of many travel reservation platforms.

But while computing technologies were gaining traction in the commercial and industrial space, popular culture had not forgotten the wartime and military roots of computing technologies. The premiere of *Star Trek* in 1967 and Stanley Kubrick's *2001: A Space Odyssey* in 1968 thrust the potential for, and dangers of, computing technologies into the public consciousness at a scale not seen previously. This continued with the release of the film *Westworld,* written and directed by Michael Crichton and the highest-grossing film for MGM in 1973, which includes one of the earliest known references to a 'computer virus', and the later film *War Games* which was released in 1983 and set firmly in the context of the Cold War. War Games centred on a high school student who had 'hacked' into a computer in search of games to play only to discover the computer in question had control of the United States missile launchers, and he had accidentally triggered a first strike against the Soviet Union. These representations of 'hackers' would play a substantial role in shaping the discourse around computer-related crimes.[22]

It was in the context of the earlier of these films that the first 'micro-computers' were released to the public. The IBM SCAMP was a proto-type personal computer developed in 1973: a computer in an enclosure the size of a briefcase (if still too heavy to transport), which would ultimately lead to IBM's first publicly available personal

[21] See, eg, Duncan G Copeland and James L McKenney, 'Airline Reservation Systems: Lessons from History' (1988) 12(3) *Management Information Systems Quarterly* 353, 354-6.

[22] See, eg, Debora Halbert, 'Discourses of Danger and the Computer Hacker' (1997) 13(4) *The Information Society* 361, 362-4; Steven Levy, *Hackers: Heroes of the Computer Revolution* (O'Reilly Media, 2010); and Helen Nissenbaum, 'Hackers and the Contested Ontology of Cyberspace' (2004) 6(2) *New Media & Society* 195, 199-200.

computer, or PC as they would be known, the Model 5150 in 1981. The 5150 was designed to run MS-DOS developed by Bill Gates and Microsoft. Later IBM developments would incorporate the Windows operating system. Prior to this, the Xerox PARC Alto had been released in 1974 as the first commercial attempt to provide a graphical user interface, dramatically increasing the ease of use and providing the design inspiration for Apple's Lynda and later Macintosh operating systems.

Throughout the 1960s and 1970s, computing technologies had been cost-prohibitive, remaining, therefore, predominantly in the hands of large companies, researchers and defence research facilities. The rise of personal computing in the 1980s drastically changed this. Costs decreased, and efforts were made to increase awareness of the capabilities and utility of computers for the average person. In the United Kingdom, the BBC as part of their *BBC Computer Literacy Project* partnered with the Acorn Computer Company to produce a series of micro-computers, the *BBC Micro*, that was launched initially in December 1981. In 1982 *The Computer Programme* began airing on BBC 2, allowing those at home, and the students of the 80% of total schools who had purchased one of the devices, to learn how to use the micro-computer by following along at home or school.[23] The devices acted as a terminal to access information via a Viewdata service, which allowed users to access and retrieve data held centrally, a precursor to the Internet.[24] In the following years, Apple released the first Macintosh in 1984, and in 1986 Compaq released the first PC using hardware capable of utilising the new graphical user interfaces implemented into Windows operating systems, coming in just ahead of IBM.

Despite the rise of these micro and personal computers in the 1980s, the bulk of computing technologies in commerce and industry remained large and cumbersome. But the increasing reliance by businesses and the State on their secure and continued

---

[23] See, BBC, 'The Computer Literacy Project Archive' (27 June 2018) <https://computer-literacy-project.pilots.bbcconnectedstudio.co.uk>.

[24] At this time, networking technologies (the ability for a computer to connect to other computers to share data and operations) operated either across existing telecommunications infrastructure or through dedicated connections. There were no widely accepted and implemented standard protocols in the form we would recognise as the 'Internet'. This despite the launch of what would ultimately become the Internet began in 1983, initially as an experiment to link governmental computers in the United States. The Internet would later incorporate the work of Tim Berners-Lee who proposed the foundations of the 'world wide web' in 1989 while at the European Organization for Nuclear Research ('CERN') in Switzerland. CERN, at the time, was the largest internet 'node' in Europe.

operation began to shift attention to the potential risks of that reliance, heightened by concerns over an increasingly wide level of access to computing devices that could communicate across fledgeling networks. This concern had been evidenced by the behaviour of those working within a business reliant on such proper functioning, as well as the conduct of those outside.

B *Early Experiences of Malicious Computer-Assisted Conduct*

While examples of sabotage and manipulation of computers can be identified as early as the 1960s,[25] particularly the phenomenon of 'phreaking' which provided much of the initial curiosity of teenagers in computers and sparked the foundations of the 'hacking' sub-culture,[26] it was not until the 1970s that crimes of fraud would be identified as computer-related. These crimes sparked the first wave of consideration of, and research into, crimes that might be, or that had been, facilitated by computers.[27] One such high profile example in the United States was an elaborate fraud undertaken by the founders of the *Equity Funding Corporation of America* ('EFCA') uncovered in 1973. The conduct at issue was not reliant on the computers; in some senses, it was the same as any other typical form of financial fraud. What the use of computers enabled, however, was a dramatic uplift in the scale of the fraud, as well as exposing weaknesses in the approach adopted by financial auditors in relying on computer-produced records.

1 *The first 'computer crime': Equity Funding*

EFCA was a financial services and life assurance company who, as agents for a suite of companies, marketed and sold shares in various mutual funds as well as life insurance products. The founders of EFCA identified that if they were to operate their own mutual

---

[25] See, eg, Jussi Parikka, *Digital Contagions A Media Archaeology of Computer Viruses* (Peter Lang Publishing, 2007); Peter J Denning, 'Computer Viruses', *NASA Research Institute for Advanced Computer Sciences* (21 March 1988) <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19890017050.pdf>.

[26] Kevin Steinmetz, *Hacked: A Radical Approach to Hacker Culture and Crime* (New York University Press, 2016) 14-6. 'Phreaking' (a portmanteau of 'phone' and 'freak') was the term applied to individuals who reverse-engineered the sound tones used to route long-distance telephone calls, allowing free telephone calls to be made.

[27] See, Thomas Whiteside, *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud* (Ty Crowell Co, 4th ed, 1978); Levy (n 22).

fund and own their own insurance company, they could construct 'packages' for customers in such a way that they could effectively be paid commission twice on every dollar spent. In 1966 EFCA acquired four insurance companies, renaming one the Equity Funding Life Insurance Company ('EFLIC'), ousted its management team, replacing them with EFLIC's own people, and formed a mutual fund. Exploiting the human weakness to fear death and to thus seek a form of secondary consolation (in the form of unaffordable insurance), EFCA developed a package whereby customers could, typically every year for a ten year period, purchase shares in the mutual fund and use the equity in the shares to borrow money from EFCA to pay their annual life insurance premiums to EFLIC, who would then charge commission at either end of the transaction. From the consumer's perspective, assuming the value of the mutual fund continued to grow enough to balance the value of the loan repayments, the sale of the shares at the end of their commitment at the increased value would be enough to cover the amount lent to pay the insurance premiums.[28]

This was, of course, never going to happen. The mutual fund, and by extension, the stock market in which it was invested, would need an exceptional run of growth even to allow customers to break even. The insurance premium was 6% per year of the total amount the customer elected to be covered, and the interest rate on any loan used to pay that premium was 10%. As Woolf observed, the only aspect guaranteed in these packages was the 'two commissions received by the salesman'.[29] Thus, there was a broad incentive for EFCA to ensure the appearance that the company was performing well, allowing the illusion that these packages represented good value for consumers buying in, and a specific incentive for EFLIC to achieve the same.

In what would be publicised at the time as the 'crime of the century' and the first case considered publicly and academically as a 'computer crime',[30] EFLIC management utilised techniques to manipulate the digital records processed on their IBM System

[28] Emile Woolf, 'The Equity Funding Story', in Emile Woolf and Moira Hindson, *Audit and Accountancy Pitfalls: A Casebook for Practicing Accountants, Lawyers and Insurers* (Wiley, 2015) 294, 295.

[29] Ibid.

[30] See, eg, Susan Hubbell Nycum, 'Legal Problems of Computer Abuse' [1977] *Washington University Law Quarterly* 527.

370/145 mainframe. Each company for which EFCA acted for as an agent in selling their mutual fund and life insurance products had access to the mainframe and a series of codes were used when recording the details of the sale of services to customers in order to link policy details to the relevant company. The system would store the details of the policies and their holders, which could then be used to run accounting and billing procedures as well as provide the necessary data for auditing purposes. Each subsidiary company had access to the mainframe, including EFLIC. The mainframe itself was physically very large and was kept in an insecure open office environment where anyone could access it and the master files.

Staff from EFLIC gained such access and reprogrammed the mainframe so that when a policy was tagged with the code '99', which would have been meaningless to any staff, it would be 'skipped' when the system calculated and compiled the monthly account billings. EFLIC was thus able to lodge non-existent policies, undetected, which were effectively 'validated' to staff and other companies merely by their existence in the mainframe's master file. Later, EFLIC would then have these policies 're-insured' to other unsuspecting companies (sometimes multiple times for the same fake policy), with those companies paying a fee in return for the expectation of future premiums when they had fallen due. Further, as the policies were not real, EFLIC did not have to pay a commission to their own sales staff on receipt of these payments. To top it off, to prevent having to pass on those insurance premiums, EFLIC produced forged death certificates for the non-existent policyholders and passed these on to the associated companies. As many as 64,000 fake policies had been entered into the mainframe by 1972.[31]

Even when auditors had requested evidence to support the non-existent policies, the time granted to EFLIC to locate the supporting documentation for the requested 'policies' allowed ample time for fraudulent documents to be produced. That such action was required on their part was immediately notified to them by the use of the code '99'. Even where the technical staff tasked with directly managing the mainframe became suspicious of gaps in the master file's sequence of policy numbers, they did not report it, preferring instead to attribute possible inconsistencies merely to the fact so many

[31] Woolf (n 28).

companies were interacting with it. EFCA, as the parent company, was involved in other fraudulent activity itself, particularly in respect of forging securities, and when later investigated by auditors Stanley Goldblum, the head of EFCA, had all their calls to divisional managers diverted to his phone where he would put on accents and confirm the values at issue.[32]

While this type of fraud did not specifically require the use of a computer, the use and manipulation of the data processed by the mainframe drastically increased the possible scale of the fraud. Similarly, the reliance on the mainframe allowed the degree of fraud to escalate and continue undetected for a substantial period of time. Ultimately, when the fraud was uncovered, incidentally by a participant who had been fired by Goldblum and turned whistle-blower, 19 individuals were charged with 105 fraud and other financial offences, each pleading guilty and receiving varying prison sentences.[33]

This case, along with similar incidents in Europe, including the forced liquidation of *Bankhaus Herstatt* in Germany in June 1974,[34] brought the potential for computers to facilitate and enable criminal conduct to the forefront of popular and political consciousness. In the aftermath of such events, the United States Senate Governmental Affairs Committee held hearings on the need for specific computer crime legislation in 1976.[35] Attempts to establish any legislation initially failed at the Federal level.

---

[32] Ibid.

[33] New York Times, 'Goldblum Among 6 Sentenced to Jail in Equity Funding Case (Online Archive, 19 March 1975) <http://www.nytimes.com/1975/03/19/archives/goldblum-among-6-sentenced-to-jail-in-equity-funding-case.html?_r=o>.

[34] The collapse of *Bankhaus Herstatt* is generally discussed only in relation to 'settlement risk' (the risks associated with transactions between banks that operate across different time zones, referred to within the finance industry now as '*Herstatt risk*') given the ensuing international banking crisis was a result of a number of operations with banks in New York failing to occur as the bank was closed at the end of the day Frankfurt - the start of the working day in New York. However, a key contributor to the collapse of the bank was the techniques employed to mask its risky foreign currency trading practices from regulators. This involved the creation of a 'cancel button' ('*Abbruchtaste*') on their computer system which when activated would result in a trade not being recorded in the daily list of operations produced by the bank's mainframe, thus excluded from audits. The use of this function permitted the foreign currency division of the bank to exceed regulated limits by up to USD$750 million at a given time. See, Emmanuel Mourlon-Droul, ''Trust is good, control is better': The 1974 Herstatt Bank Crisis and its Implications for International Regulatory Reform' (2015) 57(2) *Business History* 311.

[35] See, US Senate Governmental Affairs Committee, *Problems Associated with Computer Technology in Federal Programs and Private Industry* (18 June 1976).

Meanwhile, the success of early prosecutions for conduct involving computers at the State level was mixed and largely turned on the precise wording of existing legislation in a given state. In cases involving alleged theft, where the accused had accessed but in no way modified any data, they would generally not be liable for theft. [36] Other courts found difficulty in regarding data as property, treating it as 'mere information'.[37]

In response, new statutes would incrementally be introduced at the State level throughout the 1980s and early 1990s to address concerns of the possibility of computer-related crimes going 'unpunished'. These State-based computer-specific criminal offences would ultimately result in the implementation of the Federal Computer Fraud and Abuse Act 18 USC §1030, which came into force in 1984.[38]

2 *Computer Facilitated Crimes in the United Kingdom*

Early examples of criminal conduct involving computers gained similar public attention in the United Kingdom, where similar prosecutorial hurdles began to appear. One difference, however, was that the facts and circumstances underpinning these early prosecutions gained a much higher media profile than some of those in the United States, particularly given the United Kingdom had yet to consider the suitability of the existing criminal laws to address the use of computers. Two such cases, which were ultimately relied on by the Law Commission in their Working Paper and Report, fell on either side of the ledger: a successful prosecution for criminal damage in *Cox v Riley* ('Cox'),[39] and an unsuccessful prosecution for forgery in *R v Gold and Schifreen* ('Gold').[40] *Cox* and the latter

---

[36] See, *Ward v Superior Court of Alameda County*, 3 Computer Law Service Reporter 206 (Cal 1972); *Lund v* Commonwealth, 217 Va 688 (Va 1977); *cf Hancock v Texas*, 402 SW 2d 906 (Tex 1966). See, further, discussion in Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd ed, 2015) 47-50.

[37] See, eg, *US v Brown*, 925 F 2d 1301 (10th Cir. 1991); but *cf* US v Collins 56 F 3d 1416 (DC Cir. 1995) for conversion of government property; and *State v Schwartz,* 173 Ore App 301 (Or. Ct App. 2001) with respect to password files.

[38] See, eg, Florida Computer Crimes Act (Chapter 815, Florida Statutes). It's also interesting to note that a Senate committee hearing on computer security in the lead up to the Federal Bill being introduced to Congress began by playing a clip from the film *War Games*.

[39] *Cox v Riley* (1986) 83 Cr App R 54.

[40] *R v Gold and Anor* [1988] 2 All ER 186.

case of *R v Whiteley* ('Whiteley')[41] would centre on similar considerations as in the United States cases in respect of the relationship between data, information and property.

(a) Cox v Riley

The first apparent prosecution involving consideration of software manipulation in the United Kingdom involved not a computer *per se*, but rather an industrial saw that was designed to cut pre-programmed patterns as part of a manufacturing process. In that sense, the saw was computerised: it was controlled by software. The accused, after his employment was terminated, gained physical access to the saw and proceeded to erase the software stored on the saw's built-in circuit board. Erasing the software rendered the saw inoperable, decreasing the company's production rate until a technician could attend and re-install a new copy of the software. A prosecution was initiated alleging that the conduct of the accused amounted to criminal damage contrary to section 1 of the *Criminal Damage Act 1971*

> A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.

At first instance, the prosecution was successful but the accused appealed, arguing that as the software stored on the circuit board was not tangible property his actions could not, at law, have amounted to criminal damage; the physical condition and integrity of the saw had not been affected by his actions. In support of this contention, the accused relied on the definition of property as provided in section 10(1) which required 'property of a tangible nature whether real or personal, including money.'[42] The court might then be said to have been presented with the question of whether or not the deletion of software could amount to damage, or, put another way, was computer data or software to be considered 'property' for the purposes of criminal damage.

---

[41] *R v Whiteley* (1991) 93 Cr App R 25.

[42] *Criminal Damage Act 1971* s 10(1).

To address such a question would necessarily require consideration as to the nature of data and its relationship to information. Namely, are they to be regarded as the same thing? In the computing sense, data might be considered discrete electrical impulses that when compiled and executed using particular processes render information in a form that is available and knowable to a user, or merely provides the instructions for the computer so to do. In that sense, data is not information, but rather is a concomitant of how computers handle information. This distinction is important as the criminal law had been reluctant to extend protection to information held in other mediums.[43] The issue, then, is whether the digital conversion of information into data was such that data itself could take on the quality of property, irrespective of the 'information' it might represent.[44]

The question as to the nature of the relationship between data and information, however, was avoided. The court instead chose to focus on constructing the issue around the employer's experience of the damage, rather than the precise nature of the damage *per se*. That is, while the target of the damage needed to be tangible property, it did not necessarily flow that the damage experienced related only to that tangible state of the property, it could also impact considerations as to intangible nature of the use, value, and enjoyment of that property.[45] When approached in this light, the underlying questions became decidedly less novel, allowing Brown LJ to rely on the reasoning set out in the earlier case of *R v Henderson & Battley* ('Henderson').[46]

Henderson involved a defendant who had deposited 30 lorry-loads of waste on an area of land that had been cleared to enable the commencement of a construction project.

---

[43] *Oxford v Moss* (1979) 68 Cr App R 183. A decision endorsed and adopted by courts in Canada, see, *Stewart v The Queen* [1988] 1 SCR 963; and considered the accepted position in the non-criminal code states in Australia.

[44] See the recent New Zealand Supreme Court decision in *Jonathan Dixon v The Queen* [2015] NZSC 147 which in expressly rejecting the view taken in *Oxford v Moss* and observing that the 'digital file' of video footage was property for the purposes of the criminal code because it could not be said that such files were 'pure information'. *Cf Your Response v Datateam Business Media* [2014] EWCA Civ 281, where the Court of Appeal for England and Wales determined that the digital files constituting a database were not property.

[45] A similar approach to the formulation was adopted in Canada in *Re Turner* (1984) 13 CCC (3d) 430 where, in avoiding a restrictive definition of property, Gray J, at 434, instead sought to consider the 'gist of the offence' which was to 'respond to interference with the enjoyment of property'.

[46] *R v Henderson & Battley* (unreported, Court of Appeal (Criminal Division), 29 November 1984).

The defendant was initially convicted for causing damage to the property, which, on appeal, was challenged on the basis that the land underneath the waste had not been physically altered: there was no tangible damage to the land. There was, however, clearly a physical interference with the land which resulted in *injury* to the use and value of the land. The owner of the land had to expend time, labour, and money to rectify the site. Thus, while the court agreed there was, in fact, no damage to the land itself, there was damage to the intangible interests connected to it. This was sufficient at law. The property in question needed to be tangible, but, where damage was the result of physical interference, the damage itself did not need to be 'tangible'.[47]

Applying this in *Cox,* the Court of Appeal held the deletion of the saw's software could, therefore, constitute criminal damage. The saw was tangible property, and the actions of the accused in physically interfering by deleting the software led to an injury to the 'value and usefulness' of the saw which required the employer to expend 'time and labour and money' to rectify.[48] The saw was temporarily inoperable. Thus, the software had merely expanded the means by which the accused could affect damage to the saw.

While the computerised nature of the saw had the potential to raise important considerations, the means and ends of the accused's conduct were capable of being construed so as to fit within the offence of criminal damage. Causing damage to 'something' that might seem intangible is a crime where that damage is the result of some physical injury upon tangible property. While a seemingly logical approach, the failure to address the underlying nature of computer data in this framing posed new questions in the case of *R v Whiteley* ('Whiteley'),[49] the final prosecution that considered the deletion

[47] It has been argued in later cases that perhaps the decision in *R v Henderson & Battley* is an anomaly in not requiring a 'physical derangement', but the better view is that it is fact entirely consistent with other criminal damage cases when considered as requiring a 'physical injury', see, eg, *Grajewski v Director of Public Prosecutions (NSW)* [2019] HCA 8, [35].

[48] *Cox v Riley* (1986) 83 Cr App R 54, 57-8. See, also, *Samuel v Stubbs* [1972] 4 SASR 200, 203 where the defendant had squashed a policeman's hat; *Hardman v Chief Constable of Avon and Somerset Constabulary* [1986] Crim LR 330 where pavement drawings made in water-soluble paint constituted damage on the basis that the local authority incurred expense in removing them, regardless of the fact that rain would eventually wash them away; and *Roe v Kingerlee* [1986] Crim LR 735 where mud graffiti was considered capable of amounting to criminal damage.

[49] *R v Whiteley* (1991) 93 Cr App R 25.

of data in the context of criminal damage.[50] The accused in *Whiteley* was convicted of four counts of criminal damage after obtaining 'electronic' access, rather than physical, to the hard drives owned by the Queen Mary College and connected to the Joint Academic Network ('JANET') and deleting data stored therein. On appeal, the accused claimed that a distinction needed to be made between the hard drive disks themselves, and the 'intangible information' they stored.

Prima facie, the Court of Appeal was presented with a similar scenario to that in *Cox*. Thus, in adopting the same reasoning, Lord Lane CJ concluded that the accused had indeed committed criminal damage, observing:

> Any alteration to the physical nature of the property concerned may amount to damage within the meaning of the section … where … the interference … amounts to an impairment of the value or usefulness of the [property] to the owner.[51]

Here, the potentially important distinction between computer hardware, the data stored upon it, and information that data represented, became blurred in the Court of Appeal's reasoning, particularly in relation to identifying and considering the 'value and usefulness' of the hard drives. The Court of Appeal focused on the deletion of the data as being the consequence arising from the accused's manipulation of the magnetic storage mechanism of the hard drives, thus rendering the data inaccessible:

> There can be no doubt that the magnetic particles upon the metal discs were part of the discs and if the appellant was proved to have intentionally and without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disc to the owner, there would be damage within the meaning of section 1 [of the Criminal Damage Act].[52]

The Court of Appeal then turned to the impact of the accused's actions as to the *usefulness* of these hard drives to the College, implicitly derived from the integrity of the data they in fact stored. Content to focus on the time, labour, and money needed to be

---

[50] The implementation of the CMA would result in the computer activities being excluded from the scope of the *Criminal Damage Act 1971*.

[51] *R v Whiteley* (1991) 93 Cr App R 25, 29 per Lord Lane CJ.

[52] Ibid 28-9.

expended to place the hard drives in their original configuration, the Court of Appeal noted that damage will:

> depend on the effect that the alteration has on the legitimate operator … If the hacker's actions do not go beyond, for example, mere tinkering with an otherwise 'empty' disc, no damage would be established. Where, on the other hand, the interference with the disc amounts to an impairment of the value or usefulness of the disc to the owner, then the necessary damage is established.[53]

The resulting blurring of hardware, data, and information, alluded to above, comes not from construing the accused's conduct as amounting to a physical injury to the hard drive, other than the overly convoluted focus on its magnetic particles, but rather on identifying the 'value and usefulness' associated with the hard drives and the effect on the owner in a situation where there are distinct forms in which that value and usefulness can manifest.

Hard drives store data. Their value is thus twofold: first, as a data storage medium, and second, the associated value of the data so stored. This associated value is dependent on the nature of the data and any information that might be obtained through the processing of that data. By manipulating the magnetic particles, the accused deleted the data held on the hard drives: thus representing the required 'physical injury'.[54] But the hard drives themselves were not physically damaged, save a possible argument for 'wear and tear' generated from the deletion process (an argument more convoluted than the focus on magnetic particles). Their value, as hard drives, was not affected as they remained operable and capable of continuing to be used to store and process data. The 'value and usefulness' was thus assessed on the separate question of how much the victim relied upon and valued the data itself, rather than the hard drive. It as this point that the apparent conflation of data with information becomes important.

Where data *is* the information, criminal damage arises on the basis of the value of the information and the impact of its loss on the owner as a consequence of the accused's physical manipulation of the hard drive. This interpretation relies on a broad view in

---

[53] Ibid 29.

[54] See, *Grajewski v Director of Public Prosecutions (NSW)* [2019] HCA 8, [35].

identifying the hard drive itself as the *medium* that carried and stored the data/information. While neither case was decided using this framing, the notion of the hard drive as the medium for the information can explain and support the approach in both *Cox* and *Whiteley* in directly considering the impact upon value and usefulness.[55] Further, treating data and information as synonymous when assessing 'value' provided the scope for Lord Lane CJ to describe the empty disc scenario as not amounting to criminal damage. Where an accused obtained access to a hard drive only to find that it was 'empty' it was suggested that no loss of value or usefulness would result.

This might at first reading seem appropriate, but it is an interpretation that sits uncomfortably with the criminal law's caution in providing a response to the protection of information.[56] Here, the very criminality of an accused's conduct seems to be determined on the subjective value and reliance placed by the owner/victim upon that information, and whether or not any information is contained on the hard drive, irrespective of the nature, context and motivation of the accused's interference. While perhaps a questionable qualification, this consideration is arguably a moral luck issue.[57] But, whether attempted damage might be an appropriate charge in such circumstances does not seem to have been considered,[58] and yet it would be because factual impossibility is no defence.[59]

The alternative approach might be to reconstruct this reasoning on the basis that data and information are distinct. In this framing, the hard drive is the medium that stores the data and the data itself acts as an *additional* medium that stores information. Criminal damage might then be constructed vis-à-vis the hard drive and data without recourse to the value and usefulness of the information. Under this framing, the physical

---

[55] An additional way to frame this question would be to consider what the *target* of the conduct of the accused was, and from that base to consider whether the computer was the target in itself, or rather was it a tool used to target something else. This will be explored further in chapters 4 and 5.

[56] *Oxford v Moss* (1979) 68 Cr App R 183.

[57] See, eg, Nir Eisikovits, 'Moral Luck and the Criminal Law' in Joseph Campbell et al (eds) *Law and Social Justice* (2005, MIT Press) 105.

[58] *Criminal Attempts Act 1981* s 1.

[59] See, eg, *R v Shivpuri* [1986] 2 All ER 334.

injury remains the interference with the hard drive, and the resulting damage is the disruption of the data itself, not the loss of information. The data is a physical component of the hard drives separate to information it can convey: here, the data could be considered to have a quasi-property status.

Revisiting Lord Lane CJ's empty disc scenario, this approach to data as distinct from information permits incorporation of the fact that any access to a hard drive, regardless of whether it is 'empty', involves a modification of the magnetic or electronic 'particles' and receipt of a response from the hard drive's firmware (the software that facilitates its operation as a hard drive). Post manufacture and formatting there are no 'empty discs', just ones that do not contain *additional* user data. Any interaction with a hard drive involves some resulting modification of data. But approaching this modification or deletion of data independently of the value of information could render assessing the data's 'value and usefulness' for the purpose of proving the offence immaterial. This is especially the case where the data itself is treated as property. Any interference that alters, harms, impairs or deteriorates the quality of the data would be capable of amounting to criminal damage in and of itself. This construction might be impermissibly wide, but it perhaps more fully addresses the realities of the underlying conduct and could provide guidance for targeted amendment. This, however, would not be the case, with the dominant view continuing to conflate data with information.

The decisions in both *Cox* and *Whiteley* were later described as 'more ingenious than practical'.[60] This view has been based on the courts' attempts to fit offences designed to address damage to property to apply to computing technologies. The manner in which they did so required a high degree of complexity in constructing a chain of resulting damage arising from the 'intangible' nature of property. This arose from the need to establish a physical interaction with hardware despite the resulting damage being to data and information. Few observers have considered that these difficulties arose from the implicit assumption that data was 'mere information', thus relegating data as an issue to

[60] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd ed, 2015) 112, citing the Model Criminal Code Officers Committee, *Chapter 4: Damage and computer offences*, Final Report (2001) 159.

be dealt with outside the criminal law.[61] But, such was the context that would inform the work of the Law Commission at the time. Data was to be treated as information, and while prosecutions for criminal damage were possible, there were inherent difficulties in explaining the intricate operation of computers, hardware, and software, to judge and jury.

(b) R v Gold; R v Schifreen

The case that put the potential risks of computing technologies at the forefront of the public consciousness in the United Kingdom arose from the conduct of a pair of who now might be referred to as the first 'bug hunters'.[62] The actions of Mr Gold and Mr Schifreen occurred around the same time that media attention was focused on the first 'computer virus' that affected IBM computers: the Brain Virus.[63] Such attention by the media was similarly heightened by the Hollywood portrayals introduced above, particularly the film *War Games*.

Instead of hacking into a military-controlled computer, however, Mr Gold and Mr Schifreen exploited security weaknesses in the Prestel Viewdata service,[64] at the time owned and operated by British Telecom ('BT'). The pair were computer enthusiasts and would discuss and test new computing equipment together. Mr Schifreen was testing a

---

[61] While highlighted throughout the remaining work of the chapter, the subject of 'data' vs 'information' will be briefly considered in Chapter 4.

[62] Bug hunters are those individuals who inspect the structure and code of software to find errors or ways in which the security mechanisms can be overcome due to mistakes. This information is then passed back to the creators to enable them to rectify the problems in the code. Such activities are often 'sponsored' by companies, manufacturers, and developers through 'bug bounty programs' where individuals receive a financial reward in return for notifying the companies. Other contexts include participation in the development of 'open source' software, that is software that is the product of community contributors and is free to use. See, eg, Sandeep Krishnamurthy and Arvind K Tripathi, 'Bounty Programmes in Free/Libre/Open Source Software' in Jürgen Bitzer and Philipp JH Schröder (eds) *The Economics of Open Source Software Development* (Elsevier, 2006) 165, 170-4.

[63] Designed by two brothers in Pakistan, the virus replicated and spread around the world. The Brain Virus infected computers in the UK, erasing and damaging data and significantly impacting usability and performance. See, Jason Kersten, 'How Two Pakistani Brothers Created the First PC Virus, *Mental Floss* (2 November 2013) <http://mentalfloss.com/article/12462/going-viral-how-two-pakastani-brothers-created-first-pc-virus>.

[64] See, eg, Tom Lean, 'Prestel: The British Internet That Never Was?', *History Today* (23 August 2016) <http://www.historytoday.com/tom-lean/prestel-british-internet-never-was>.

new modem in 1984 and was entering in random numbers to see whether or not they would work. Very soon he stumbled across a live account for the Prestel network, account no. '2222222222' and password '1234'. This, however, was not a customer account, but a staff account that contained the connection information for a mainframe used for testing and maintenance. After trying to connect on and off for a few months, eventually, the pair were able to get access to the test mainframe, where they found an unprotected page that provided the system administrator account details for the test mainframe.

Unfortunately, BT had made a cardinal cybersecurity error in that the system administrator passwords for the test mainframe were identical to those for the live network. Thus, Mr Gold and Mr Schifreen had administrator access to everything on the main network, including user message accounts, and the services provided by other companies. The pair managed to modify Financial Times Stock Exchange news, access confidential information stored at a stock brokerage firm, and accessed the email account of the Duke of Edinburgh and sent an email from his account. The pair had attempted to notify BT consistently of the issues they had found but were not taken seriously. To prove their point, after another unsuccessful call, Mr Schifreen altered the title of the network's main database page from 'INDEX' to 'IDNEX' and called back. At last, BT took him seriously, but instead of immediately rectifying the issues, BT contacted Scotland Yard's newly formed Computer Crime Unit who launched a criminal investigation.

The report and the subsequent police investigation sparked widespread media interest. A series of television reports, news articles, and magazine exposés were immediately forthcoming.[65] The reports typically included examples of methods for gaining access to computer systems, often coupled with assertions that the critical systems underpinning banking and nuclear research could be similarly infiltrated. Rumours also persisted that the Prestel service operated as a backup control system for the military, adding a further *War Games* dynamic to public perceptions of the risks. Of course, there was no evidence to substantiate many of the claims, and despite the actions of Mr Gold and Mr Schifreen in reporting the security flaw to BT, and the earnestness with which

[65] Much material from the time has been preserved and is on display at the National Museum of Computing at Bletchley Park.

they appeared to do so, the media portrayed them as hackers who presented a serious threat, with unique skills and abilities to spy and manipulate.[66]

Following the investigation, relying on the evidence collected by BT, it was decided that the pair would be charged with forgery. Police and prosecutors had no recourse to offences for 'hacking', and it was thought that forgery presented the best chance of success. The alternative route would have been to pursue a charge under various fraud offences that, as they existed at the time, all required proof of deception. It was believed that as the network was itself authenticating users in response to the entered access credentials, rather than a human, deception would not be able to be established. The applicable definition of 'deception' was provided in the *Theft Act 1968* s 15(4):[67]

> Any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of a person using the deception or any other person.

The view that a person needed to be the subject of the deception arose from the discussion in the case of *Davies v Flackett* ('Davies').[68] While not directly decided on this point, and thus merely an observation in obiter by Bridge J, *Davies* involved a prosecution for 'obtaining a pecuniary advantage by deception'[69] in relation to a group of friends who had manually lifted the boom gate at an automated car park and driven through without paying the required parking fee. The defendant, the driver, was acquitted at first instance, with the verdict at trial suggesting that the system in use at the carpark, like a computer, had no mind and could therefore not be deceived. The Crown appealed to the Divisional Court who upheld the acquittal. The reasons provided by the Divisional Court, however, did not directly consider whether the car park system could at law be deceived, instead finding that the prosecution had failed to produce evidence that the accused had entered the car park with the intention not to pay: his non-payment was opportunistic and at the end of the transaction, rather than a motivating and operating inducement upon gaining

---

[66] Tom Lean, *Electronic Dreams: How 1980s Britain Learned to Love the Computer* (Bloomsbury Sigma, 2016) 158.

[67] The *Theft Act 1968* and *Theft Act 1978* would ultimately be repealed and replaced by the Fraud Act 2006.

[68] *Davies v Flackett* [1973] RTR 8.

[69] *Theft Act 1968* s 16.

access to the car park. In respect of the automated system, any consideration became purely academic, with Bridge J expressing doubt that a machine could, in fact, be deceived, while Ackner J did not want to foreclose the possibility.[70]

These observations would later be relied on in submission in *Holmes v Governor of Brixton Prison* ('Holmes').[71] Again, while determined on other grounds, the case involved consideration of whether or not a computer could be deceived. The accused in *Holmes* was facing extradition to Germany for varies fraudulent bank transactions, resulting in consideration of the offence of 'obtaining a money transfer by deception'.[72] One small aspect of the case centred on the misuse of passwords belonging to bank employees that were used to authorise the money transfers. Once authorised in the system by use of the employee access credentials, the system would automatically validate and proceed with the transaction. On this point, while noting that *Davies* was not binding authority, Burnton J observed that 'we nonetheless accept that "the prevailing opinion is that it is not possible in law to deceive a machine."'[73]

In accepting that this would be the likely response of the court in a prosecution against Mr Gold and Mr Schifreen for an offence requiring deception, despite providing the first clear opportunity to decide the issue directly, the pair were charged with nine counts of forgery under the *Forgery and Counterfeiting Act 1981* s 1(1):

> A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice.

---

[70] *Davies v Flackett* [1973] RTR 8, 11.

[71] *Holmes v Governor of Brixton Prison* [2005] 1 All ER 490.

[72] *Theft Act 1968* s 15A, later repealed and replaced by *Fraud Act 2006* s 14(1)(3).

[73] *Holmes v Governor of Brixton Prison* [2005] 1 All ER 490, [12]. The court referred to views set out in John Smith, *The Law of Theft* (Oxford University Press, 8th ed, 1997) [4.12]; and Edward Griew, *The Theft Acts* (Sweet & Maxwell, 7th ed, 1995) [8.12]-[8.13]. They went a step further, also supporting the view of Professor Griew that it was 'regrettable' that the misuse of passwords and account details was not a substantive offence of theft or a cognate offence, before noting that the conduct could likely be framed as an offence contrary to section 2 of the *Computer Misuse Act 1990*.

At first instance, both were convicted. Subsequently they petitioned the Court of Appeal to consider the meaning of 'false instrument'. At trial, there seemed to be a high degree of confusion as to what the alleged 'false instrument' upon which the forgery could be based in fact was, with its identification ultimately left up to the jury.[74] The appeal centred on the argument that the use of otherwise valid access credentials that were stored temporarily by the network's authentication system could not amount to a false instrument. The Court of Appeal, therefore, had to consider the meaning of 'instrument' and whether it could be extended in the sense accepted at trial to cover the conduct of Mr Gold and Mr Schifreen.

Arguments on appeal centred on the 'user segment' of the network: the log-in mechanism. 'Instrument' had been provided with a definition in the Act which included 'any disc, tape, sound track or other device on or in which information is recorded or stored'.[75] Thus the Court of Appeal had to determine whether the process of transmitting the access credentials across the network had the necessary qualities of being 'recorded or stored'. Given the electronic nature of the transmission and that the validation of the authenticity of the credentials occurred instantaneously before being erased, the access credentials could not be considered either recorded or stored. In quashing the convictions, Lord Lane CJ stated:

> 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 … to dishonestly gaining access to the relevant Prestel data bank by trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts.[76]

An appeal was lodged by the Crown to the House of Lords, alleging that the Court of Appeal had erred in its interpretation of 'recorded or stored'. In supporting the view of Lord Lane CJ, Lord Brandon applied the ordinary meaning of the words 'recorded or stored' to the operation of the 'user segment'. That meaning connoted 'the preservation of the thing … for an appreciable time with the object of subsequent retrieval or

---

[74] *R v Gold; R v Schifreen* [1987] 3 All ER 618, 621.

[75] *Forgery and Counterfeiting Act 1981* s 8(1)(d).

[76] *R v Gold; R v Schifreen* [1987] 3 All ER 618, 622-3.

recovery.[77] The mechanism the system used to handle the verification of access credentials did not fit this construction: the details were held temporarily before becoming inaccessible. The process took mere seconds, and there was no recording or storing. As a matter of law there could be no false instrument. The House of Lords upheld the quashing of the convictions.

The fact that Mr Gold and Mr Schifreen escaped conviction, along with the perceived complications of pursuing other possible avenues (the issue of proving deception discussed above), served as a key motivator for considering the introduction of new computer offences. *Gold* has since been the subject of much discussion, used largely as a contextual focal point to frame the 'problem' that the criminal law faced at the time.[78] Lloyd would later claim that '[c]overage of cases such as *R v Gold*, although interesting and valuable … has lost much of its relevance because of the passage of the Computer Misuse Act'.[79] But none of that coverage seems to critically question the identification of the charges, nor the socio-political context of the time. *Gold* will be revisited in chapter 5 in the context of identifying the role of a computer in the commission of a crime. For now, *Gold* sparked the political push to investigate creating computer offences, with the apparent approval of the Courts of the need to do so. It was not long, therefore, before the Law Commission turned their attention to the issue.

III THE WORK OF THE LAW COMMISSION

The Law Commission turned their attention to the challenges posed to the criminal law by the use of computers after the completion of their broad review of the offence of conspiracy to defraud, noting that the dishonest manipulation of computers was a major consideration in assessing the appropriateness of the structure and operation of that

[77] *R v Gold and Anor* [1988] 2 All ER 186, 192.

[78] See, eg, Neil MacEwan, 'The Computer Misuse Act 1990: Lessons from its Past, Predictions for its Future' (2008) 12 *Criminal Law Review* 955; Richard Walton, 'The Computer Misuse Act' (2006) 11(1) *Information Security Technical Report* 39; Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change' (2006) 70 *Journal of Criminal Law* 424; Martin Wasik, 'The Computer Misuse Act 1990' (1990) (Nov) *Criminal Law Review* 767.

[79] Ian Lloyd, 'Crime and the Computer Book Review' (1992) 6(1) *International Review of Law, Computers & Technology* 225, 244.

offence into the future.[80] In those observations, the Law Commission further observed that while the review was necessarily limited to the consideration of fraud, it was clear that a comprehensive review of the broader criminal law would be necessary. Thus, after waiting for the conclusion of the appeal to the House of Lords in *Gold*, in September 1988 the Law Commission released their Working Paper for public consultation on the need for new computer offences.[81] This was followed by the release of their Final Report in October 1989, which will be discussed in Chapter 3.[82]

A *The Working Paper*

Given the broader context, the Working Paper was presented as a measured document that sought to provide a clear basis of terminology and understanding to the phenomena of 'computer misuse', noting that the Commission's work was to be carried out in the context of widespread media coverage and heightened public interest.[83] It sought considered contributions from interested parties as to the extent, if any, the criminal law needed amendment to account for the use of computers, while displaying a level of scepticism that such recourse was necessary in the form of a 'computer crime statute' save a new offence for 'hacking'.[84] Nevertheless, the Working Paper provided comment on the creation of such a computer crime statute in a suite of proposed possible reform options.

1 *Terminology and Framing*

The Working Paper rejected the use of the term 'computer crime', instead preferring the adoption of 'computer misuse'. Computer crime was thought to both 'prejudge the conduct in question' and lack the ability to distinguish clearly the type of

---

[80] Law Commission, 'Conspiracy to Defraud' (Working Paper No 104, Cm 228, 1987) [4.9]-[4.11], [10.3]-[10.9].

[81] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988). Scotland had undertaken a similar process in the year prior, and the Working Paper drew heavily from their work. See, Scottish Law Commission, 'Report on Computer Crime' (Report No 106, Cm 174, 1987).

[82] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989).

[83] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [1.4].

[84] Ibid viii.

conduct involved, noting that conduct, even when unauthorised, does not 'become unlawful simply because a computer is involved'.[85] On the latter point, the Working Paper set out an analogy with the unauthorised use of a neighbour's lawnmower which 'is not a crime … so long as it is returned undamaged.'[86] Further, clear consideration should be placed on identifying conduct involving computers analogous to other forms of conduct that were not criminalised at the time: observing here that 'it is not an offence to obtain unauthorised access to information' and that this would be a relevant consideration into considering 'hacking'.[87] 'Computer misuse', then, provided flexibility to identify the various types of conduct that could be either enabled by computers and unique to computers.

Drawing on definitions settled upon in the Scottish Law Commission's Consultative Memorandum on Computer Crime, the Working Paper described a computer as 'a device for storing and processing data, by which is meant information of any kind'.[88] Again, naming data as information. The Working Paper then set out the basic operation of networks, at the time being a network that was operated from a centrally controlled mainframe, describing the usefulness of computers as dependant on 'users being able to contact the central computer from remote locations.'[89] This framing of networks as being connected to a 'central computer' was a product of the proprietary and corporate nature of networking that existed at the time.[90] The Working Paper thus noted that any use of the term 'access' did not mean physical access.[91]

---

[85] Ibid [1.5].

[86] Ibid.

[87] Ibid [1.6].

[88] Ibid [1.12]-[1.13].

[89] Ibid [1.15].

[90] This framing no longer holds true with respect to the structure and operation of the internet, but still holds some truth for some forms of corporate networks, although today more complex and not located on 'one' central computer.

[91] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [1.15]-[1.16].

In focusing predominantly on 'hacking', the Working Paper defined the issue as both the 'unauthorised obtaining of information from a computer' and the 'unauthorised obtaining of access to a computer'. Further issues were defined as the 'unauthorised alteration or destruction of information stored on a computer', the denial of access to a computer by an authorised user, and the 'unauthorised removal of information stored on a computer'.[92]

2 *Recourse to the Criminal Law?*

The Working Paper noted that proposals for the creation of new criminal offences required justification.[93] Rather than turn to criminal law theory to find those avenues of justification, the guiding principles contained in a Home Office consultation paper were reiterated.[94] First, that the conduct was harmful to the degree that remediation on the basis of compensation as between individuals would not be sufficient, and that redress of that conduct was a concern of public interest. Second, criminal sanctions should only be introduced where other 'means of control would be ineffective, impractical or insufficient'.[95] Finally, any new offence would need to be enforceable, and thus provide a clear definition of its scope and effect.

As to the first and second consideration, the Working Paper would later consider the suitability of the civil law to provide a remedy for 'hacking'.[96] Again linking data to information through using the terms interchangeably, it was suggested that any such action would require the legitimate owner of the 'information' proceeding against anyone who had obtained that information through unauthorised access, or where the data had been destroyed or corrupted.[97] It was thus concluded that action would lie only in a potential breach of confidence action, where the information was capable of being

---

[92] Ibid [2.1].

[93] Ibid [1.11].

[94] See, Home Office, 'Trespass in Residential Premises' (1982) [18]-[20].

[95] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [1.11].

[96] Ibid [6.4].

[97] Ibid.

considered confidential, or in an action in negligence in the rare cases damage to data was inadvertently caused by hacking.[98] The Working Paper then set out the provisional view that 'the civil law (whether reformed or not) could only rarely provide an effective remedy. We would welcome comments on this conclusion.'[99]

The identification of data and information as one and the same appears to have resulted in the foreclosing of consideration of the tort of trespass, despite the framing of hacking as 'unauthorised access to a computer' providing a clear analogy. That the civil law had, and continues to provide, only minimal protection for 'information' seems to have added weight to arguments in support of a new criminal offence. Indeed, following consultation and in setting out the responses, the Final Report would make no mention of the civil law.

3 *Reform Options*

The Working Paper framed possible reform as falling within three approaches: creating a dedicated computer crime statute,[100] the 'limited reform' option,[101] and the 'half-way approach'.[102] A dedicated crime statute would involve the creation of specific new offences for all conduct involving computers; for instance, the creation of a specific offence of 'computer fraud' and 'criminal damage to a computer'. The Commission did not favour this option, referring to the underlying rationale of the *Theft Act 1968* and the *Criminal Damage Act 1971* as being:

> to create "broad band" offences which are so defined that they include a range of conduct and factual circumstances, and to dispense with distinctions based on the kind of property stolen or damaged.

---

[98] Ibid [6.5].

[99] Ibid [6.6].

[100] Ibid [4.3].

[101] Ibid [4.4].

[102] Ibid [4.5]-[4.7].

The limited-reform option would involve taking no action in respect of computers as a category, but rather addressing the issues presented by computers as another aspect of consideration during the reform process of other general offences. That is, if it were thought necessary to introduce a new offence of theft in relation to computers, such an assessment would be best left to those considering the structure and role of theft offences as a whole.[103]

The 'half-way approach' would reject the whole-scale creation of new computer versions of offences and instead would focus efforts on the widening of existing offences in order to ensure computers would fall within their scope. This would leave the option to create computer-specific offences where necessary to 'fill the gaps'. The Commission was of the view that this would be the most appropriate option, accepting that there was clear scope to expand existing offence such as fraud.[104] While it was noted specifically that 'hacking' was not covered by the existing criminal law, the creation of such an offence would be suitable if it could be appropriately justified. That being said, it was also suggested that reforms to the definition and structure of other general offences might suitably cover 'hacking'.[105]

Having expressed a preference for the half-way approach, the Working Paper set out four proposed models of how a 'hacking' offence might be shaped; an offence with respect to unauthorised access to certain categories of information (Option A), an offence of unauthorised access to a computer with the intention to inspect information (Option B), an offence of unauthorised access that results in damage to the computer (Option C), or a broad offence of obtaining unauthorised access to a computer (Option D).

---

[103] Despite ultimately recommending the creation of an 'unauthorised access' offence is Scotland, this appeared to be the favourite approach of the Scottish Law Commission in relation to the substantive criminal law. See, Scottish Law Commission, 'Report on Computer Crime' (Report No 106, Cm 174, 1987) [3.15]-[3.20].

[104] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [4.7].

[105] Ibid.

(a) Option A

Option A proposed the construction of an offence that would be limited to an individual who gained unauthorised access to a computer that contained certain categories of information.[106] An offence of this nature would turn on the contents of any computer so accessed: for instance, an offence would not be committed where an individual knowingly gained unauthorised access to a computer that did not have any information that fell within the protected categories of personal or corporate information.[107] The construction of harm to be addressed by this model could be considered the loss in value of the information, any resulting financial or reputational damage, and the invasion of privacy. Thus, the harm was not 'hacking' *per se*.

The Working Paper noted that this model would not be appropriate if the accepted purpose of a new offence would be to 'cover all cases of hacking, irrespective of the information at risk.'[108] The preference to cover all cases of hacking might be argued to support and promote reliance and confidence in the safety and security of computers more generally: the criminalisation of access to only certain kinds of information would do little to achieve this. However, this model would operate neatly alongside emerging data protection frameworks.[109]

(b) Option B

Option B would be an offence of unauthorised access to a computer in order to inspect stored information.[110] This model would thus focus on the access to information stored on the computer, rather than the computer itself. While the *actus reus* in this model is constructed more broadly than that in Option A given it would cover any unauthorised access regardless of the qualities of the information inspected, the *mens rea* requirement is

---

[106] Ibid [6.25].

[107] Ibid.

[108] Ibid [6.27].

[109] The concept of 'personal information' for the purpose of Option A was drawn from the recently implemented *Data Protection Ac 1984*.

[110] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [6.27].

focussed narrowly. Thus, in any prosecution, it would need to be established that the accused had an intention to access and inspect the specific information stored upon it. Further limiting features might also be considered in respect of whether such an offence ought to be limited to circumstances where there was an intention on the part of the 'hacker' to gain some form of advantage or to cause damage to another's interests.[111]

An offence structured in this form would not cover all forms of hacking, particularly those instances where the access was achieved merely to fulfil the challenge of overcoming security mechanisms, or the thrill of solving the puzzle, rather than accessing information.[112] But, this model would have the capacity to clearly limit the scope of the offence to those circumstances that represented more serious interference with computers.

(c) Option C

Option C proposed an offence of unauthorised access that causes damage to the computer. An offence in this form would be based substantially on the existing offences within the *Criminal Damage Act 1971* but would resolve the complications that had arisen in *Cox* and *Whiteley*. Unauthorised access would attract criminal sanction only where there was resulting damage to the operation and utility of the computer and any information contained therein. The offence would be constructed as one of strict liability in respect of the resulting damage: the intention of the accused would be irrelevant.[113] However, it would still need to be established that the accused intended to gain the initial unauthorised access that caused the damage.[114]

The benefit of this approach is that the offence does not depend on the nature of the information stored, but the requirement of damage would prevent its application to the many instances of 'hacking' that result in no such damage. It thus would not respond

[111] Ibid [6.29].

[112] Ibid [6.12].

[113] Ibid [6.32].

[114] Ibid [6.34].

to circumstances where unauthorised access was a mere intrusion, or where the access was not used to disrupt the operation of the computer.

(d) Option D

Option D would be a general offence of obtaining unauthorised access. Such an offence would criminalise the mere obtaining of unauthorised access to a computer, with no further conditions as to the information contained therein, nor a requirement that there be any resulting damage. This model most clearly reflected a trespass formulation: the unauthorised interference with a computer, where the computer itself is deemed the focus of protection, along with all data contained therein. It thus had the capacity to respond to all instances of hacking, regardless of the underlying intention informing the access that was obtained. The criminalisation of conduct would thus turn on whether a given 'access' was unauthorised and that the individual had knowledge that the access they obtained was unauthorised.

An offence constructed this broadly would have the effect of criminalising benign conduct, with the Commission offering the hypothetical scenario of an individual who obtains unauthorised access to a database that contained the timetables for a British Railways service. Such access would pose no risk of harm or damage but would clearly fall within the scope of the offence.[115]

4 *Possible Justifications*

The selection of which of the above models was to be preferred, and to be informed by the consultation process, would depend on the clear identification of the harms to be responded to, along with the broader aims of having such an offence. The Working Paper proposed a number of considerations including; deterrence, supplementing existing offences, risks to the normal operation of computing systems, hacking as criminogenic, and that other jurisdictions, by that time, had created similar offences.

[115] Ibid [6.37].

(a) Deterrence

It was suggested that the lack of a specific offence against hacking was capable of inhibiting users from making full use of their computers out of a fear their device would be targeted and damaged. Given the increased prevalence and importance of computers to society, it was in the public interest that hacking is deterred.[116] This would promote confidence in the reliability and security of computers and networks, thus encouraging an environment of experimentation and investment in computing technologies. The creation of an offence would also serve a signalling function by specifically naming and targeting hacking. It would declare the boundaries of appropriate computer conduct and would signal society's disapproval of those who breach computer norms, and serve to 'reject the claim that hacking is a harmless intellectual pastime'.[117]

The Working Paper also argued that aside from providing an avenue for successful prosecutions in a way that described the specific conduct and harm at issue, a specific hacking offence would also deter the sharing of information surrounding techniques and potential targets on 'bulletin boards' and message boards, dissuade teachers from permitting their pupils to learn computer skills, and disincentivise existing hackers from presenting their efforts to the media. Such deterrent effects would thereby reduce and ultimately prevent the encouragement of other hackers.[118]

(b) Supplement existing offences

The creation of a hacking offence would serve a useful supplementary function in support of existing obligations in respect of certain information. The *Data Protection Act 1984* received particular attention in the Working Paper, with a hacking offence suggested to be a seemingly appropriate corollary to the complimentary obligations placed on data controllers to keep personal information secure.[119]

---

[116] Ibid [6.8].

[117] Ibid [6.12].

[118] Ibid.

[119] Ibid [6.9].

(c) Risks to the operation of computers

The resultant harm of hacking was ultimately identified as the potential risk to the operation of the computer: any form of unauthorised access, regardless of whether it was intentional or not, impacts upon the computer's integrity. Such conduct created a high degree of inconvenience in having to track potential intrusions.[120] The scale of consequential harms could vary greatly depending on the nature of the computer in questions. The hacking of a computer containing important and valuable information or engaged in managing a service (such as air traffic control) could result in serious and catastrophic harm. But while this variation is dependent on the computer itself, the most important element warranting consideration, according to the Working Paper, was that the accessing of *any* system could result in *potential* harms.[121]

(d) Hacking as criminogenic

Citing the cannabis as a 'gateway drug' argument, the Commission noted that a hacking offence might also dissuade the commission of other offences.[122] This is particularly the case where the gaining of unauthorised access might be a required *first step*: computer-assisted fraud, or theft. This would appear to be distinct from the arguments that would support any offence on the basis of providing a supplementary function, like data protection. Here, the arguments are supporting the adoption of an inchoate mode offence: a specifically labelled offence that criminalised conduct that *might* otherwise be considered an attempt. This position was informed, as evident implicitly in the observations above, by the views in public, political and cultural discourses that were engaged in a process of 'othering' hackers. It would appear that this justification implicitly assumes an underlying deviance in the type or class of persons who engage in hacking; thus, permitting the base conduct of 'hacking' would likely lead to, or encourage, an escalation in their deviant behaviour.

---

[120] Ibid [6.11].

[121] Ibid [6.12].

[122] Ibid [6.13]. See the explanation contained in footnote 13 of Part 6 of the Working Paper, where, in respect of cannabis, the Commission stats 'decriminalisation is sometimes said to encourage a progression towards the use of more dangerous drugs.'

(e) The work of other jurisdictions

Finally, the Commission noted that at the time the Working Paper the United States had already passed laws addressing hacking: the Computer Fraud and Abuse Act 18 USC §1030. Similar laws had been implemented in Canada,[123] and the Australian State of Victoria,[124] while the other Australian States were completing reviews of their own criminal legislation.[125] New offences had also been recommended by the Scottish Law Commission in their earlier report on computers and the Scottish criminal law.[126] The Working Paper presented this as an indication that the legitimacy of such criminalisation was widely supported.[127]

(f) Arguments against criminalising?

Despite presenting themselves as not being convinced of the need to amend the criminal law, the Working Paper spent considerably less attention to considering the arguments against the creation of a new criminal law for hacking. The objections noted in the Working Paper can be reduced to four key points. First, that there was no right to privacy recognised in the United Kingdom and such an offence would represent a *de facto* recognition of such. Second, while analogy could be made with the tort of trespass, even then such a claim lies outside the criminal law without an aggravating factor.[128] Third, information is not property and thus outside the bounds of the criminal law's protection.[129] Finally, a hacking offence would be difficult to enforce.[130]

---

[123] *Criminal Law Amendment Act, C 1985*; *Criminal Code,* RSC 1985, s 342.1(1).

[124] *Crimes (Computers) Act 1988 (Vic).*

[125] Tasmanian Law Reform Commission, *Computer Misuse* (Report No 47, 1986).

[126] Scottish Law Commission, 'Report on Computer Crime' (Report No 106, 1987).

[127] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [6.14].

[128] Ibid [6.15].

[129] Ibid [6.16]; *Oxford v Moss* (1979) 68 Cr App R 183.

[130] Ibid [6.18].

It should again be noted that despite drawing the analogy to the tort of trespass here, that discussion was missing in the parts of the Working Paper dealing with the civil law. Further, the conflation of data and information was again clearly evident. As will be set out in chapter 3, none of these considerations against criminalisation featured strongly in submissions received by the Law Commission during their consultation period, resulting in a substantial change in language and approach in the recommendations set out in the Final Report.

IV CONCLUSION

Computing technologies had evolved substantially since the first examples began to take shape in the context of World War II. The later commercialisation of these technologies progressed and contributed to the transition from large, expensive computers, to smaller, cheaper personal computers for the mass market. Networking technologies similarly developed in their capabilities. As the general public began to be introduced to these technologies, media and Hollywood portrayals would play a key role in representing the challenges and risks associated with their adoption. These risks were further emphasised by coverage of large-scale frauds, like those at *Equity Funding* in the US, and coverage of hackers in the UK, particularly in respect of the newly released 'Brain virus' and the case of *R v Gold; R v Schifreen*.

The Law Commission in the UK was then tasked with seeking input on the state of the English criminal law and its ability to respond to uses and misuses of computers. In releasing their Working Paper, the Law Commission framed the issue as being one of determining whether a new 'hacking' offence was required. They set out four possible models of such an offence and sought comment on which, if any, ought to be selected.

Importantly, the Commission specifically identified the need to justify any such offence, by ensuring that the offence would address conduct that is harmful, that no other means would be effective, practical of sufficient, and that it would be enforceable. To substantiate this, the Working Paper suggested that it was the breach of the integrity of the computer that was the harm, coupled with the risk of potential harms that could result from any unauthorised access. They suggested that the civil law would be insufficient to

address the concerns of hacking and that a specific offence would act as a deterrent to both hacking and further criminal activities.

Chapter 3 will now consider the result of the consultation period with a focus on the Law Commission's recommendations in their Final Report and the resulting offences contained in the *Computer Misuse Act 1990*

Chapter 3

THE *COMPUTER MISUSE ACT*: STRUCTURE, INTERPRETATION, AND APPLICATION

Never trust a computer you can't throw out a window.

STEVE WOZNIAK [1]

I INTRODUCTION

Following the consultation period initiated by the release of their Working Paper on Computer Misuse, the Law Commission substantially reappraised their initial view that there was no need for a suite of new criminal offences, albeit having initially been open to suggestions that it might be appropriate to create a new hacking offence. Accompanying a marked change of tone, the Law Commission instead recommended

[1] This quote, like many examples of content found on the internet, is not entirely accurate, having been paraphrased. But, nevertheless, was later endorsed by Wozniak who was happy to take credit for the better phrased version of what he had in fact said. See, Kevin Purdy, 'How Apple Co-Founder Steve Wozniak Gets Things Done', *Lifehacker* (Interview, 23 April 2009) <https://www.lifehacker.com.au/2009/04/how-apple-co-founder-steve-wozniak-gets-things-done/>.

the introduction of three new offences. On the basis of the submissions they had received from interested parties, the Law Commission was satisfied that they had been correct in identifying 'three types of computer misuse [for] which [to] be concerned'; computer-assisted fraud, unauthorised access to a computer (hacking), and the unauthorised alteration or erasure of data.[2]

This chapter sets out the recommendations set out in the Final Report, before exploring the structure of the offences as contained in the resulting framework: the *Computer Misuse Act 1990*. The chapter considers the key cases that developed and provided guidance for the definition and scope of the offences. It also explores the impact of the five subsequent waves of amendments that cumulatively would modify the nature of the offences and increase the maximum available sentences, while also introducing two further new offences.

II THE FINAL REPORT

The Final Report spent a considerable amount of time reflecting on the submissions received during the consultation period to solidify the position that a hacking offence was indeed required and could be appropriately justified. And, instead of adopting the conservative approach flagged in the Working Paper and widely expected, a second more serious offence was recommended for hacking with an ulterior intent.[3] Further, the Law Commission accepted that a third new offence in respect of erasure or alteration of data was warranted to address the complexities that had arisen with respect to applying the

[2] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [1.40]. In respect of computer-assisted fraud, the Commission concluded that no recommendations would be made on the basis that the issue of decisions being made by computers was a relatively rare, noting at [2.5] that 'at present machines comparatively seldom make decisions about the provision of services or the release of liabilities', those decisions remained subject to human consideration and thus would fall within the ambit of existing fraud offences. They further concluded at [2.7] that the issue of not being able to deceive a machine would better be dealt with at a later date as a topic within a review of fraud. Indeed, this would ultimately occur in the 2002 review of Fraud which ultimately resulted in the introduction of the *Fraud Act 2006*. See, Law Commission, 'Fraud' (Report no 276 Cm 5560, 2002). It is interesting to note, however, that the Fraud Report made mention of the Computer Misuse Act 1990 only once and that was limited only to its possible application to the protection of trade secrets, see [4.7].

[3] Geoffrey Brown 'Is there an Ethics of Computing?' (1991) 8 *Journal of Applied Philosophy* 19, 22.

offence of criminal damage to computing technologies.[4] No draft bill was offered in the Final Report, with that task to be left to Parliament. This has been attributed to the speed in which the report was produced and 'because it was thought at the time that this was a matter of urgency'.[5]

A *The Unauthorised Access Offences*

The central question posed by the Law Commission's Working Paper was '[s]hould the obtaining of unauthorised access to a computer be a criminal offence?'[6] The overwhelming view of the submissions received on this point was that 'hacking by unauthorised entry (or attempted entry) is sufficiently widespread to be of major concern to computer system users'.[7] The Working Paper had presented hacking as both a threat to the confidentiality or value of information stored on a computer and a broader threat to the integrity and trust in computer systems.[8] The submissions received were said to have invited the Law Commission to view the issue 'in a somewhat different light',[9] stressing that computer storage involves problems that are 'qualitatively different from manual methods of storage.'[10] Analogy was made to information that is stored on paper, and thus capable of being protected by physical barriers and the laws of burglary and potentially theft (where the paper was physically taken), whereas computers represent different security risks to the information stored given they can be accessed via a network from anywhere and this does not involve a choice on the part of the computer user but is an inherent nature of a computer's design.[11]

---

[4] *Criminal Damage Act 1971* s 1(1).

[5] Peter Alldridge, 'Computer Misuse Act 1990' (1990) 9(6) *International Banking Law* 339.

[6] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [8.4].

[7] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [2.10].

[8] See discussion in Chapter 2, above 68-71, 77.

[9] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [2.11].

[10] Ibid [2.12].

[11] Ibid.

While noting that this 'difference', still involving a conflation of data with information, would not in itself necessarily justify the creation of a new offence, the risks presented to the integrity and trust in computer systems was sufficient. That these offences would involve indirect protection of information was deemed to not 'milita[te] against the creation of such an offence if, as we are persuaded, there are other and strong grounds for taking that step'.[12] These other justifications were; first, that the harms of hacking were the actual losses and costs incurred by computer owners; second, that hacking may be undertaken as a preliminary step to committing further general offences; and third, that the permissibility of any form of hacking would result in a feeling of 'insecurity' by computer owners.[13] The deterrence of such conduct would thus be a legitimate public goal.[14]

The Law Commission further rejected arguments that the activity of hackers could be beneficial to improving the security of computer systems, where the designers and operators of those systems are notified of security issues in the systems 'defences'. Taking a property-based conception of ownership of the system, the Law Commission argued that '[i]t is for those operators to decide how their system shall be tested. If they *invite* outside attack … that is irrelevant to the uninvited and unauthorised intrusions with which most system owners are concerned'.[15] No consideration appears to have been placed on the difference between 'ownership' of hardware and 'ownership' of software, the ownership of the former being transferred at purchase, with ownership of the latter remaining with the creator with a transfer of a *license* to use the software being created.

Questions over the enforcement of any such offence were also set aside. The Law Commission was convinced that with full cooperation by the owners of 'victim' computers, law enforcement would face a relatively simple task in identifying the source of an incoming connection. This could be achieved by requesting call logs and connection details from the relevant telecommunications company, with such investigatory

[12] Ibid [2.13].

[13] Ibid [2.14].

[14] Ibid [2.15].

[15] Ibid [2.17].

techniques already being suitably provided for.[16] This would provide the line number used to 'dial' the computer and, from there, it would be straightforward to identify the relevant individual.[17] Active enforcement would thus remove 'the present aura, if not of acceptability then at least of fun, that surrounds hacking'[18] which would work to persuade 'young people not to enter into, or to be instructed in, hacking'.[19] The efficacy of this view and approach was supported by 'informants' from police forces and industry.[20] While they did at least acknowledge that there would be some cases of hacking that would go undetected,[21] the absurdities inherent in the Law Commission's assertions will be explored in Chapter 4.

The Law Commission thus concluded that an offence of unauthorised access was both justified and necessary, and while it would not totally eliminate hacking, it would go a long way towards reducing the overall incidence of such conduct and thus increase confidence in the integrity of computer systems.[22] They recommended that an offence be adopted in the form set out in the Working Paper as Option D, which based on the submissions received during their consultation was the strong favourite.[23] They went further, however, also recommending the introduction of a second new offence where the hacking was undertaken with an intent to commit a further serious crime.

The purpose of the proposed creation of two offences was considered in light of the recommendations made by the Scottish Law Commission in their review of computer misuse, and a proposal was put forward by Emma Nicholson MP to criminalise

---

[16] Ibid [2.20], highlighting the operation of *Telecommunications Act 1984* ss 45(1)(b) and 45(2)(a) which permitted telecommunications companies to provide information to law enforcement for the prevention and detection of criminal activity.

[17] Ibid [2.22].

[18] Ibid [2.23].

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Ibid [2.24].

[23] Ibid [2.25].

'unauthorised entry' to a computer.[24] The Scottish Law Commission had recommended the creation of an offence that would have criminalised circumstances where a person:

> without authorisation to do so, [obtains] access to a program or data stored in a computer in order to inspect or otherwise to acquire knowledge of the program or the data or to add to, alter or corrupt any such data or program for the purpose of –
> (a) obtaining an advantage for himself or another person, or
> (b) damaging another person's interests.[25]

This framing was the product of the Scottish Law Commission concluding that an offence that merely required unauthorised access would produce uncertainties as to guiding appropriate sentences given that the consequences of a given instance of unauthorised access range from minimal interference to substantial losses. The specificity in the framing of the offence, adopting a fraud-based formulation, was also said to be necessary to substantiate the proposed maximum sentence available for the offence which was recommended to be set as an imprisonment term of up to five years. The Nicholson proposal involved the creation of an offence of 'unauthorised entry into a computer system' with no requirement of damage or harm punishable by up to ten years' imprisonment.

In relation to considering suitable proposals for reform to the criminal law in England and Wales, the Law Commission took issue with the ulterior intent requirement of the Scottish formulation, focusing on the evidential difficulties that arise when such requirements limit offences to proven cases of fraud, dishonesty or malicious damage. Where such a limitation is effective, 'there will be problems of proof and the law will also fail to impose sanctions on the casual hacker'.[26] But where the limitations are not interpreted in a strict sense, such that they operate in practice to cover most or all acts of hacking, there is a danger that severe penalties could be applied to less serious instances.[27]

---

[24] See, Brown (n 3) 22-3.

[25] Scottish Law Commission, 'Report on Computer Crime' (Report No 106, Cm 174, 1987) [4.12].

[26] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.9].

[27] Ibid.

While the intention of the Scottish formulation was that such requirements would be interpreted strictly in order to justify the seriousness of the sentence available, the Law Commission believed a broad offence with a 'comparatively moderate penalty' would serve the broad aims of deterring all forms hacking, with an additional offence for those who hack in furtherance of an intention to commit a general offence, which would carry a more serious sentence.[28] The Law Commission thus recommended a hierarchical approach to dealing with hacking: a summary offence to deal with 'general mischief', and an indictable offence for hacking with ulterior intent.[29]

Despite recommending the creation of these two new offences, the Report contained no suggested formulation or potential draft of their content. Instead, recommendations were made as to what should broadly be considered in constructing such offences. In relation to the 'basic access offence', the Law Commission was of the view that such an offence should require that the person 'caused a computer to perform any function with intent to secure access to or obtain information about a program or data held on the computer'. Further, the accused must know that the access so intended was, in fact, unauthorised.[30] To explain how such an offence ought to work in practice, the Report provided a three-stage example of an individual attempting to log-in to a computer. At stage one, the person enters their username and password. At stage two, the computer completes a verification process. At stage three, access is either granted or refused by the system. Where an unauthorised person was attempting the same, the Law Commission observed the following:

> At stage three the user unquestionable secures access to a program or data held in a computer. That person is guilty of an offence (subject to *mens rea*). At stage two, the user has caused the computer to perform a function (for example displaying a menu or a blank screen) and he is guilty of an offence (subject to *mens rea*) because he intended thereby to obtain information (from the menu or welcome screen) … This leaves the user at stage one. Under our proposals he would be guilty of the offence if (subject to *mens rea*) he causes a computer to perform a function (viz. check his identification combination) with intent to obtain information in respect of any program or data held in the computer. He will obtain information about a program or data stored in the computer by finding out whether or not the identification combination that he presents is recognised as valid … he will be guilty

[28] Ibid [3.10].

[29] Ibid [3.11].

[30] Ibid [3.14].

> whether or not he succeeds in gaining the information, whether or not its factually possible to gain that information and whether his aim is to obtain information … or merely explore the system.[31]

The potential breadth of this offence was not of concern to the Law Commission who noted that cases involving a hacker who does not, in fact, reach stage three would be rare as they would likely not be detected. But they went further, arguing that if the offence required successfully gaining access, rather than attempting to, an accused who was in fact detected at stage one 'might claim that he was only interested in testing the system's defences … That claim might be hard to disprove …[but they] would still in our view be someone whom the law should seek to discourage.'[32] The Law Commission further justified this position on the basis of wishing to avoid placing the courts in the position of having to determine which kinds of computer use would be 'more than merely preparatory' for the purpose of establishing whether an attempt of the access offence had been made.[33] This is, of course, an odd justification to offer considering the proposal was to create a *summary offence* for which prosecution as an attempt would not be possible,[34] albeit relevant to the more serious ulterior intent formulation of the second proposed offence. The Law Commission was also of the view that the *mens rea* requirement of intent to gain access would serve a suitable limiting function, provided care was taken so as exclude the possibility of recklessness being sufficient.[35]

The construction of criminality in this form also seems to be predominantly based on the idea of unauthorised information exchange. The crux of why an individual who enters invalid credentials into a system, which will reject those same credentials, warrants criminal sanction has been constructed to be the fact they are obtaining 'information' from the computer and that the credentials are in fact not valid. Having earlier settled on the view that the harm to be addressed was that as against the integrity of a computer system, it does not seem to follow that the framing of the structure of the offence should

---

[31] Ibid [3.17].

[32] Ibid [3.18].

[33] Ibid [3.18].

[34] *Criminal Attempts Act 1981* s 1(4).

[35] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.27].

then be linked to the snippets of information gleaned by processes that indicate that there has been no injury to the integrity of the system.

Indeed, a computer's integrity was a key concept upon which the construction of 'access' was recommended to be based, with the Law Commission arguing that the structure of the offence should make plain that it was not intended to cover physical print-outs of the computer information or other modes of access not requiring interaction with the computer. The harm was to the integrity of the computer; thus, only electronic hacking could be the proper focus.[36] Thus requiring the 'causing of a computer to perform a function' would negate the possible inclusion of acts of physical access or mere inspection of data displayed on another's screen.[37]

In considering the construction of 'authorisation', the Law Commission noted that while it would be clear that a remote access by an outsider would clearly fall within the scope of any hacking offence, so too should the conduct of employees of a company who have some degree of authority to access and use a computer but who nevertheless exceeds that authority consciously and deliberately.[38] Where the harm to be addressed centres on the integrity of a computer, there is no reason why employees or similarly situated 'insiders' should be excluded. Their conduct ought only to be captured, however, where there was 'a deliberate act of disobedience … and not merely carelessness, stupidity or inattention'.[39] In such circumstances, the burden should be on the prosecution to prove that the employee had knowledge of the extent of their authority and this would be the case where the employer had 'clearly defined limits' which 'should be laid down as a matter of good management practices'.[40] Thus the Law Commission recommended what would essentially be an incentive for computer owners to create a clear chain of authority, supported by policy and other internal documents, that could provide adequate notice to

[36] Ibid [3.24].

[37] Ibid [3.26].

[38] Ibid [3.35].

[39] Ibid [3.36].

[40] Ibid [3.37].

employees of acceptable computer use. Such a requirement was deemed sufficient to negate suggestions that it might be prudent to introduce a defence of honest belief.[41]

The Law Commission then turned to the connected issue of an authorised use for an unauthorised purpose, that is where an individual does not exceed their scope of authorisation in respect to accessing the computer but instead undertakes conduct which would fall outside their normal duties. Here, the recommendation was made that such conduct should not fall within the scope of the offence noting that

> there is nothing to distinguish the misuse of an employer's computer from the misuse of the office photocopier or typewriter, and that it is therefore inappropriate to invoke the criminal law to punish conduct more appropriately dealt with by disciplinary procedures.[42]

The final observations made in respect of the basic access offence were to confirm that the term 'computer' should be left undefined, noting that the submissions received agreed that it would be unnecessary to attempt to define it. Elsewhere, attempted definitions had been complex and unruly in an attempt to be all-encompassing, which could result in confusion for those involved in prosecutions, and there was little 'enthusiasm for the *tertium quid* of definition by partial exclusion' approach.[43] It was then recommended that the offence would be triable summarily only with a maximum penalty of three months' imprisonment, a fine up to Level 4 on the scale, or both.[44] While initially considering a six-month maximum, the Law Commission was concerned to avoid the impression that the basic offence would be so serious as to warrant a custodial sentence in *most cases.*[45]

The ulterior intent formulation of the second proposed new offence, that is where an individual commits the basic access offence intending to use that access to facilitate

---

[41] Ibid.

[42] Ibid [3.38].

[43] Ibid [3.39].

[44] Ibid [3.45].

[45] Ibid.

the commission of a further serious offence, was justified on the basis that it would be both difficult and unlikely that a prosecution for an attempt of the intended general offence could be satisfied merely by evidencing unauthorised access to a computer system. Using the example of the unauthorised transferring of funds from an electronic bank account, the Law Commission was of the view that an attempt to gain access to the Bank's computing system would probably not amount to conduct that was beyond merely preparatory to complete the intended theft.[46] Thus, the Law Commission recommended that the second proposed offence ought to draw on the general construction of the offence of attempts (including applying to circumstances where the further offence was factually impossible), but be limited to use of a computer and only in respect to further offences with sentences of five years or more.[47]

The Law Commission concluded by recommending that such an ulterior intent offence should carry a maximum five-year term of imprisonment, and should operate as a lesser-included offence with respect of the basic access offence. Where charged on indictment, the basic access offence should be available where a further intent on the part of the accused cannot be proven.[48]

B *An Unauthorised Data Erasure and Alteration Offence*

In turning to the difficulties with respect to applying the offence of criminal damage to the computing context, the Law Commission further recommended the creation of an offence that would criminalise the unauthorised modification to the contents of a computer. This was proposed as causing:

> an unauthorised modification of the contents of any computer's memory or the contents of any computer storage medium, with intent thereby to impair the operation of any computer or computer program, or to destroy, or to impair the reliability of accessibility of, any data stored or otherwise held in any computer.[49]

---

[46] Ibid [3.52]. See, eg, *R v Thompson* [1984] 3 All ER 565.

[47] Ibid [3.56]-3.58].

[48] Ibid [3.59]-[3.60].

[49] Ibid [3.64].

It was noted that a number of submissions received during consultation indicated that it might be suitable to amend that definition of property within the *Criminal Damage Act 1971* so as to include 'data' and 'computer programs'.[50] The Law Commission was not convinced, arguing that 'damage' still carried a meaning that necessitated 'physical injury' and thus non-physical interferences with computer programmes or data remain ill-suited.[51] Concern was also raised as to the general criminal damage offence extending to reckless conduct, with the preference in respect of computer misuse to be limited only to intentional acts.[52]

The Law Commission proposed that 'modification' be provided further definitional guidance to ensure that it included; causing a program or data to be erased from, or stored or 'held' in, a computer,[53] actions with respect to computer storage mediums (hard drives and other aspects of computer hardware responsible for storing and processing data etc), and interference with a program already so stored.[54] It was also intended that such an offence would include conduct involved in the distribution and circulation of computer viruses, intending that the conduct should be criminalised at the moment the virus is copied to a storage medium, regardless of how the virus was ultimately distributed, where the individual intended at the time that it was distributed to cause *some* form of modification. On this point the Law Commission provided the example of the distribution of a virus on 'floppy disk' passed through innocent agents:

---

[50] Ibid [3.62]. See, eg, Hugo Cornwall (alias Peter Sommer), 'Hacking away at computer law reform' (1988) 138 *New Law Journal* 702; David Bainbridge, 'Hacking – the unauthorised access of computer systems: the legal implications' (1989) 52 *Modern Law Review* 236, 245. *Cf* Confederation of British Industry, 'Submission to the Law Commission on Working Paper No. 110 on Computer Misuse--The CBI Submission Part II' (1990) 6(2) *Computer Law and Security Report* 23, 24.

[51] Despite contemplating a change to the definition of property, it does not appear to have been thought that 'damage' might similarly benefit from the insertion of guidance with respect to computers – linking it specifically to circumstances involving the erasure or impairment of data.

[52] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.62].

[53] Ostensibly, this was to respond to the issue in *R v Gold and Anor* [1988] 2 All ER 186 where it was held that the temporary nature of the data transmission rendered it incapable of being considered an 'instrument'. It is unclear why this was necessarily warranted given there was no further definitional requirement of permanence set out, either expressly or impliedly, in the structure of the proposed offence.

[54] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.67].

> If X in London gives a disk that he knows to be infected to an innocent agent Y, who does not use it but gives it to Z in Newcastle, who does not use it but gives it to V in Plymouth, who copies the contents of the floppy disk including the virus on to his own hard disk and thereby has his data files corrupted then, provided that X intended when he gave Y the disk that a computer's memory etc. should be impaired, it matter not that X did not know the identity of the target computer.[55]

The *mens rea* requirement of a general 'intent to impair' was selected on the basis that the Law Commission wanted to ensure coverage of the above example while also avoiding having the offence apply to circumstances where the unauthorised modification improved or was otherwise neutral in its effect on the system, leaving these circumstances to be dealt with by the basic offence.[56] That the earlier proposed access with ulterior intent offence might also apply to such a circumstance seems to have escaped consideration.[57] Impairment to the proper operation of a computer was also deemed to be a suitable corollary to the 'physical damage' requirement of the criminal damage offence.

The final recommendations in relation to this proposed offence were that it should be made clear that the *Criminal Damage Act 1971* should not be deemed to no longer apply to computer systems and data, thus reversing the decision in *Cox v Riley*.[58] It was further recommended that the offence be triable either way and punishable on conviction on indictment for a maximum five years' imprisonment.[59]

C *The Recommendations in the Context of the Normative Model*

It is prudent at this point to consider the normative model established in chapter 1. There it was suggested that the creation of new criminal offences ought to have regard to identifying a suitable harm or risk of harm that gives rise to the legitimate use of the State's interest in protecting and defending individuals. The construction of the offences

---

[55] Ibid [3.70].

[56] Ibid [3.72].

[57] And yet it could, as the Law Commission had already noted that such an offence would be drafted to be clear that factual impossibility would be no defence.

[58] *Cox v Riley* (1986) 83 Cr App R 54.

[59] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.78]-[3.79].

should be enforceable, and the definitions of those offences ought to be such that the conduct that is criminalised is commensurate with the harms identified. The offence should also not presuppose wrongdoing on the part of a particular class or group and should not be constructed and applied where those subject to it are unaware of its scope.

While substantive attention will be placed on these considerations in the context of the final form of the CMA in Chapters 4, 5 and 6, some initial observations can be made, particularly in respect of the Law Commission's final identification of the relevant harm, their approach to 'hackers' as a group warranting the attention of the criminal law, and the effect this has had on the structure of the offences they proposed.

In respect to the harm of hacking, the Law Commission appeared to identify the main harm as being the compromise of a computer system's integrity. While acknowledging that there were consequential harms beyond this, the focus remained on deterring conduct that would, in fact, breach a system's integrity with the resulting cost of rectifying that breach, and broader damage to public confidence in the security and reliability of computing technologies. This would appear a suitably clear identification of a real and tangible harm of public concern. The failing, however, appears to be in the recommending a broad offence that criminalises conduct on the basis of obtaining information from a system, rather than redressing a resulting breach of a computer's integrity. Now it might be that the risks associated with 'hacking' were substantial enough that this departure in focus is ultimately justifiable, but such a position is inherently weakened by the confusion and conflation of concepts like 'data' and 'information'.

The apparent preference for adopting a broad offence that ensures all forms of hacking were captured requires similar reflection. The analysis provided by the Law Commission appears to have been based on the assumption that all 'hacking' leads to crime, thus anyone who engages in activities that require a high-level computing skill set are criminals in the waiting and the criminal law ought to be engaged so as to provide a sufficient deterrent in order to prevent the 'downward slide'. This view is perhaps evident in the discussion of discouraging 'youth' and the creation of networks for sharing

'hacking' information,[60] and the presupposition that 'hackers' had nothing to offer in respect of the 'legitimate' work of the law in protecting computer security.[61] This focus on 'hackers' occurred even despite the Law Commission explicitly referencing throughout the Final Report a number of surveys that indicated that the most common forms of computer misuse were actually committed by employees and insiders.[62]

As will be explored now as the chapter shifts its attention to the resulting Act, similar views were expressed and relied upon by lawmakers as the proposal moved through the House of Commons and the House of Lords.

III THE COMPUTER MISUSE ACT

Following the delivery of the Law Commission's Final Report, it was expected by many commentators, and the media, that the government of the day would incorporate the introduction of the recommended offences into their legislative agenda.[63] However, the relevant Secretary of State, Nicholas Ridley, did not present Government legislation. It was hoped that Emma Nicholson MP, who had made criminalising hacking a key personal priority, would put forth a private members bill incorporating the Law Commission's recommendations (with her previous work on drafting a criminal offence against 'hacking') and that it would ballot sufficiently high enough that debate could proceed with the backing of the Government.[64] The bill that was ultimately introduced, however, was one introduced as a private members bill in the name of Michael Colvin MP. With government backing, the Bill navigated the House of Commons and the House of Lords relatively smoothly, with a number of amendments proposed at the Standing

[60] Ibid [2.23].

[61] Ibid [2.17].

[62] Ibid [2.3], [3.35].

[63] See, eg, Alldridge (n 5).

[64] Ibid.

Committee stage.[65] It contained the three offences recommended by the Law Commission while also providing additional provisions to deal with jurisdictional issues.

The need for the offences, or the suitability of their framing (as protection of computer integrity) was not seriously challenged during the debate. Instead, MPs tended to focus on making plain the perceived impact of computer misuse upon industry and commerce, expressing further views that the criminal law was ill-suited to respond. This included noting that as at April 1990 '270 cases [had] been verified … as involving computer misuse of the past five years, [but] only six were brought to court … and only three … were successfully prosecuted.'[66] The circumstances of the other 264 cases do not seem to have been critically explored, with emphasis seemingly just being placed on the contrast between the numbers: 270 incidents and three convictions.

Some contributions to the debate were considerably less useful. The suggestion above that the Law Commission appeared to be identifying and treating 'hackers' as a *class* from which criminality could be expected, lost all veneer of respectability when discussed on the floor of the House. Hackers were described as members of 'a twisted culture that the Bill is trying to stamp out'.[67] This culture was suggested to include those 'who spend all night hacking, and lose their job because of poor performance, or they might have been sacked for hacking whilst at work … consequently they are often poor',[68] although according to other contributions hacking was lucrative because '[t]hey make a great deal of money out it and the German hackers, at any rate, support a drug-based lifestyle on their activities' and 'because drugs are expensive, hackers need to make a great

[65] Notably the proposal to introduce a defence to the section 1 offence where it could be established that the owner of the computer had not taken 'such care as in all the circumstances, was reasonably required to prevent the access in question'. This would effectively be making contributory negligence a defence to a criminal charge, and the amendment was ultimately withdrawn on that basis. This would, however, have brought the section 1 into line with the data protection principles in the *Data Protection Act 1984*. See, further, Stefan Fafinski, 'Computer Use and Misuse: The Constellation of Control' (PhD Thesis, University of Leeds, September 2008) 39.

[66] HC Deb 9 February 1990, vol 166, col 1134.

[67] HC Deb 9 February 1990, vol 166, col 1137.

[68] HC Deb 9 February 1990, vol 166, col 1177.

deal of money'.[69] It was further lamented that '[a]t one time, computers were used only by a few professors and very disciplined professionals, but the tremendous growth in microcomputing has meant the entry into the arena of the unspeakable'.[70] These *unspeakables* were not apparently only drug addicts with poor time management skills, but their alleged behaviour was even said to be motivated by 'a profound sexual inadequacy'.[71]

Unsurprisingly, then, the Bill was passed, and the *Computer Misuse Act 1990* ('CMA') came into force on 29 August 1990. This was despite the decision in *R v Whiteley,* discussed in chapter 2, having been delivered and indicating that criminal damage offences could be successfully prosecuted.[72] MacEwan would later observe that the Government should have adopted a 'holding pattern' such that more care could be taken in the creation of the new offence, especially given the relative speed of progress.[73] Such pause might have given the opportunity for lawmakers to anticipate the dramatic changes in technology just around the corner. 'Instead, the CMA suffered a premature birth, which left it weak and vulnerable when the internet, as we know it, arrived.'[74]

This section will explore the offences as originally enacted, before moving to consider subsequent amendments that sought to respond as computing technologies continued to evolve.

A The Offences as Originally Passed

The CMA was structured to contain three offences, reflecting the recommendations put forth by the Law Commission. Section 1 would provide for the

---

[69] HC Deb 9 February 1990, vol 166, col 1154.

[70] HC Deb 9 February 1990, vol 166, col 1151.

[71] HC Deb 9 February 1990, vol 166, col 1156.

[72] (1991) 93 Cr App R 25.

[73] Neil MacEwan, 'The Computer Misuse Act 1990: Lessons from its Past, Predictions for its Future' (2008) 12 *Criminal Law Review* 955.

[74] Ibid 956.

basic access offence, titled 'obtaining unauthorised access'. Section 2 set out the ulterior intent access offence, titled 'obtaining unauthorised access with intent to commit or facilitate a further offence'. The section 3 offence would criminalise the unauthorised modification of computer material.

1 *Obtaining Unauthorised Access – CMA section 1*

The basic access offence was constructed in line with the recommendations of the Law Commission, incorporating the focus on 'causing a computer to perform a function' when undertaken with an 'intent to secure access' where the accused 'knows' that the access would be unauthorised. Section 1 thus provided:

> (1) A person is guilty of an offence if –
> (a) he causes a computer to perform a function with intent to secure access to any program or data held in a computer;
> (b) the access he intends to secure is unauthorised; and
> (c) he knows at the time when he causes the computer to perform the function that this is the case
>
> (2) The intent a person has to have to commit the offence under this section need not be directed at:
> (a) any particular program or data;
> (b) a program or data of any particular kind; or
> (c) a program or data held in any particular computer.

However, while the Law Commission had recommended a maximum sentence on summary conviction of three months, a fine fixed at Level 4 of the standard scale, or both, which was intended to reflect and balance the likely application of the offence to relatively minor conduct, the offence as implemented provided for a maximum sentence of six months, a fine fixed at Level 5 of the standard scale, or both.[75] The offence retained its summary nature and was to operate as a lesser-alternative-offence for both sections 2 and 3.[76] While the other offences within the CMA were to have a limitations period of three years from the commission of the offence,[77] prosecutions under section 1 were possible

[75] *Computer Misuse Act 1990* s 1(3) [as originally enacted].

[76] *Computer Misuse Act 1990* s 12 [as originally enacted].

[77] *Computer Misuse Act 1990* s 11(3) [as originally enacted].

within six months of evidence of the offence becoming known to prosecutors, subject to the three-year maximum.[78]

2 *Unauthorised Access with an Ulterior Intent – CMA section 2*

The ulterior intent offence, as proposed by the Law Commission, would operate as an aggravated form of the basic access offence in section 1. With the offence in section 1 operating as a lesser-alternative-offence, the structure of the section 2 offence builds on that of section 1 with the further provision that the accused committed that offence with an intent to facilitate or commit a further general offence. Section 2 thus provides:

> (1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent –
> (a) to commit an offence to which this section applies; or
> (b) to facilitate the commission of such an offence (whether by himself or by another person);
> and the offence he intends to commit of facilitate is referred to below in this section as the further offence.
>
> (2) This section applies to offences –
> (a) for which the sentence is fixed by law; or
> (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years.

The offence is triable either way, with a maximum sentence for conviction on indictment for five years' imprisonment, the maximum statutory fine, or both.[79] Incorporating the further recommendations of the Law Commission, the offence is available even where the further intended offence was factually impossible,[80] but further, it was irrelevant whether the further offence was temporally correlated:[81] that is, it would not be necessary to establish that the access and the further offence were part of the same transaction. Mere preparation in the form of obtaining unauthorised access in order to give *later* effect to an ulterior criminal intent would thus be within scope. Importantly, the section 2 offence remains available even where the further offence has been completed.

---

[78] *Computer Misuse Act 1990* s 11(2) [as originally enacted].

[79] *Computer Misuse Act 1990* s 2(5)(b). On summary conviction, per s 2(5)(a), a maximum sentence of six months, the maximum fine, or both would be available.

[80] *Computer Misuse Act 1990* s 2(4).

[81] *Computer Misuse Act 1990* s 2(3).

That is, a prosecution can proceed on the basis of the section 2 offence *and* the completed offence.[82]

3 *Unauthorised Modification – CMA section 3*

The offence in section 3 enacted the Law Commission's recommendation that an offence be created to respond to the unauthorised modification of computer programs or data. It was further provided that the section 3 offence would work to the exclusion of the *Criminal Damage Act 1971* if the modification did not impair the computer's physical condition.[83] Section 3 thus provided:

> (1) A person is guilty of an offence if –
> (a) he does an act which causes an unauthorised modification of the contents of any computer; and
> (b) at the time when he does the act he has the requisite intent and the requisite knowledge.
>
> (2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause modification of the contents of any computer and by so doing –
> (a) to impair the operation of any computer;
> (b) to prevent or hinder access to any program or the reliability of any such data; or
> (c) to impair the operation of any such program or the reliability of any such data.
>
> (3) The intent need not be directed at –
> (a) any particular computer;
> (b) any particular program or data or a program or data of any particular kind; or
> (c) any particular modification or a modification of any particular kind.
>
> (4) For the purposes of subsection 1(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.
>
> (5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

An individual found guilty of an offence under section 3 was liable on conviction on indictment for a maximum five years' imprisonment, the maximum statutory fine, or both.[84]

---

[82] See, *R v Skelton* (Unreported, Bradford Crown Court,17 July 2015); *R v Imran Uddin* (Unreported, Birmingham Crown Court, 24 April 2015).

[83] *Computer Misuse Act 1990* s 3(6) [as originally enacted].

[84] *Computer Misuse Act 1990* s 3(7)(b) [as originally enacted]. This offence too would be triable either way, with summary conviction, per s 3(7)(a) accompanied by a maximum sentence of six months, the maximum fine, or both.

4 *Definitions and early interpretation by the Courts*

The CMA provided guidance as to the intended interpretation of the key terms 'access', 'unauthorised', and 'modification'. 'Computer', in accordance with the Law Commission's recommendation, was left undefined. So too were the confines of 'intention' and 'knowledge'.

(a) 'access'

The actual operation of the concept of 'access' within the CMA sits at the intersection of its meaning when used as a noun and its meaning when used as a transitive verb (explored further in Chapter 4). That is, access can be the description of an accused who 'obtains computer access' (describing the end state of their conduct, in noun form), as distinct from the accused 'accessing the computer' (describing the interaction of the accused with the computer, in its verb form). Unhelpfully, the definitions provided in subsections 17(2) and 17(3), which were intended to provide guidance to the interpretation of access, incorporated features of both conceptions. Subsections 17(2) and 17(3) provided:

> (2) A person secures access to any program or data held in a computer if by causing a computer to perform a function he –
> (a) alters or erases the program or data;
> (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
> (c) uses it; or
> (d) has it output from the computer in which it is held (whether by having it displayed or in any other manner)
> and references to access to a program or data (and to an intent to secure such access) shall be read accordingly
>
> (3) For the purpose of subsection (2)(c) above a person uses a program if the function he causes the computer to perform –
> (a) causes the program to be executed; or
> (b) is itself a function of the program.

The framing of 'access' in these broad terms was thus intended to capture any form of unauthorised interaction with a computer. But, in what might be described as departure from the justifications set out by the Law Commission that it is the integrity of the 'computer' that is the legitimate interest being protected, the definitions here appear to address not only the computer 'as a whole' but also individual instances of computer

programs and data. That is, within the framing of subsections 17(2) and 17(3) were the seeds of potential growth in the types of 'access' that could fall within the scope of the CMA's offences.

However, while the potential breadth of the 'access' would begin to be explored in later cases, the very first prosecution to go to trial, *R v Sean Cropp* ('Cropp'),[85] involved the physical *use* of *one* computer, rather than involving conduct as between two computers that was thought to typically be the case in instances of 'hacking'. This presented difficulties for the trial judge in squaring the seemingly broad nature of access in subsection 17(2) with the text of section 1 that could thus be cumulatively read as requiring 'causing *a computer* to perform any function with intent to secure access to *any* program or data held in *any* computer'.[86]

The accused in *Cropp* had returned to a store for which he had been a former employee in order to purchase goods for his new employer. The accused had remembered the necessary codes for use on the point of sale system that would cause the system to apply a discount to purchases. While the system was unattended, these codes were so entered by the accused resulting in a 70% discount on the purchase price of the goods subsequently invoiced to his new employer (representing a discount of £506.36 ex VAT). Upon discovery, the accused was charged with an offence contrary to section 2 of the CMA. After the presentation of the prosecution's case, the accused made a submission of no case to answer, arguing that it must be established that he had used one computer to access another computer. The trial judge agreed and instructed the jury that a second computer must be involved, stating that '[i]t seems to me to be straining language to say that only one computer is necessary when one looks to the actual working of the subsection'.[87]

---

[85] *R v Sean Cropp* (Unreported, Snaresbrook Crown Court, 4 July 1991). While *Cropp* was the first prosecution to go to trial in respect of the section 2 offence, it was not the first case involving an offence contrary to section 2. *R v Ross Pearlstone* (Unreported, Bow Street Magistrates Court, March 1991) involved the guilty plea of a former employee who used their former employer's telephone account to make unauthorised calls to avoid incurring a charge.

[86] Ibid.

[87] Cited in *Attorney General's Reference No 1 of 1991* [1992] 3 All ER 897, 900.

This interpretation might be said to fit with the idea that the access offences were designed to target 'hackers' as outsiders, with incidental coverage of 'insiders' where appropriate. It would thus represent a severe limitation to the scope of the CMA in responding to the concerns of business and industry who had expected that the offences would apply equally to the conduct of their current and former employees.[88] Unsurprisingly, the Attorney General sought the opinion of the Court of Appeal to clarify the proper interpretation by way of an Attorney General's Reference.[89] Giving the opinion of the court in finding the trial judge had erred in directing the jury that two computers were required, Lord Taylor CJ held:

> Mr Lassman argued successfully before the judge, and sought to argue before this court, that the final phrase, 'held in any computer' should really be read as 'held in any other computer' or alternatively should be read 'held in any computer except the computer which performed the function'. To read those words in that way, in our judgment, would be to give them a meaning quite different from their plain and natural meaning … In our judgement there are no grounds whatsoever for implying or importing the word 'other' between 'any' and 'computer' or excepting the computer which is actually used by the offender from the phrase 'any computer'.[90]

The Court of Appeal was also convinced by arguments that to interpret the offence otherwise would result in the 'surprising, and indeed unlikely, lacunae which this Act would have left in the field of interference with computers … there would be nothing in the 1990 Act to meet … industrial espionage.'[91] In so confirming that the offences within the CMA applied to conduct engaged in on a single computer, the Court of Appeal thus permitted the beginning of what would be a continued trend in expansive interpretations of access. Such expansion will be the focus of discussion in Chapter 4.

(b) 'unauthorised'

Guidance as to the interpretation of what type of access might be considered 'unauthorised' is provided in subsection 17(5). Despite the preference of the Law

---

[88] See discussion, above Part II.

[89] *Attorney General's Reference No 1 of 1991* [1992] 3 All ER 897.

[90] Ibid 901.

[91] Ibid.

Commission that such guidance ought to exclude the possibility of applying to situations where 'insiders' gain authorised access but for an unauthorised person, no such limitation was attempted. Instead, subsection 17(5) provides:

> (5) Access of any kind by any person to any program or data held in a computer is unauthorised if—
>
> (a) he is not himself entitled to control access of the kind in question to the program or data; and
>
> (b) he does not have consent to access by him of the kind in question from any person who is so entitled.

This construction gives rise to a number of issues in relation to the way in which 'authorisation' to access data might be granted or restricted, and how the appropriate source of that authorisation might be ascertained. In respect of the latter, does authorisation lie with the owner of the system, the creator of the software, or the 'owner' of the particular data? Additionally, can that authorisation come in the form of verbal instructions, signs, and policy documents, or is to be limited to computer security mechanisms (user accounts and passwords)? Further, given the focus on a 'kind of access', is any authorisation to be limited to the specific authority of the individual to access specific data, or the broader type or 'kind of data' that might be accessible when exercising that level of otherwise authorised access?

Lending further weight to the observations made above in Part II as to the questionable approach of the Law Commission in focusing on 'hackers' as a legitimate danger and suitable target of these offences, the first wave of prosecutions that gave rise to questions of whether or not access was unauthorised centred primarily on employees and 'insiders': specifically, police officers misusing their access to the Police National Computer System.[92] While these early cases involved guilty pleas, the application of the

[92] See, *R v Bennett* (Unreported, Bow Street Magistrates Court, 10 October 1991); *R v Bonnett* (Unreported, Newcastle under Lyme, 3 November 1995) cited in MacEwan (n 70) 958; *R v Begley* (Unreported, Coventry Magistrates Court) see, further, *R (on the application of Begley) v Chief Constable of the West Midlands* [2001] EWCA Civ 1571 for judicial review of the accused's subsequent dismissal for misconduct. The first two cases, *Bennett* involving access to the Police National Computer System to identify the details of his ex-wife's new partner, and *Bonnett* involving similar access to find the details of an owner of a personalised number-plate the accused wished to purchase, resulted in fines of ~£150. *Begley* involved a female police officer who accessed the system to find the details of a woman the officer believed to have had an affair with her boyfriend at the time. Despite her conduct being substantially similar to that in *Bennett*, and granted there was perhaps more awareness of the risks of such conduct and a growing emphasis on higher penalties given the case was heard years later, it is

CMA to conduct involving 'authorised access for an unauthorised purpose' would be considered in *DPP v Bignell* ('Bignell').[93] *Bignell* involved two police officers, a husband and wife, who had instructed an operator of the Police National Computer System to obtain, on their behalf, the details associated with the registration number of two cars owned by Mr Bignell's ex-wife's new partner. When making such requests, officers had to assign a 'Reason Code' that would be stored as an explanation for why the information was sought. The pair thus used a false 'Reason Code' to obtain access to the information. At first instance the pair were convicted of an offence under section 1 of the CMA on the basis that they were not authorised to make use of the computer system in relation to their private lives.

At risk of losing their jobs on the basis of their conviction the pair appealed, arguing that they were authorised to make requests for information from the computer system, they had merely done so for an unauthorised purpose. Given they had authorised access to the 'kind of data' in question, their inappropriate use of that data must necessarily fall outside the bounds of the CMA.[94] This argument was accepted at the Southwark Crown Court and the appeal was allowed, with the Crown launching a further appeal to the Divisional Court. In delivering the majority judgment, Astill J upheld the decision of the Crown Court, having found that as the two police officers were authorised in their normal course of duties to access and request information from the computer system, the use to which they then put that information to was not determinative in respect of constructing authorisation. Astill J further observed, reflecting the position of the Law Commission, that:

> The respondents remain subject to internal disciplines. The use of the computer for an unauthorised purpose involves the use of a false Reason Code and that is a matter subject to disciplinary procedures. In addition the respondents could have been prosecuted under the Data Protection Act 1984.[95]

---

interesting to note that the male defendant in *Bennett* received a fine, but the female defendant in *Begley* received a prison sentence and lost her job.

[93] *DPP v Bignell* [1998] 1 Cr App R 1.

[94] Similar arguments could have been made in the earlier cases against police officers, but these had all involved guilty pleas. See, above nn 89.

[95] *DPP v Bignell* [1998] 1 Cr App R 1, 12.

In coming to this decision, Astill J interpreted the definition of 'unauthorised' as set out in subsection 17(5) as being limited by the kinds of access defined in subsection 17(2) discussed above. Thus, the phrase 'entitled to control access of the kind in question' in subsection 17(5) must be a reference to the possible 'kind of access' listed in subsection 17(2):

> Section 17(2)(a) to (d) sets out four ways in which a person secures access. Section 17(5)(a) and (b) define unauthorised access by reference to access 'of the kind in question'. That refers to the four kinds of access set out in section 17(2)(a) to (d) and the respondents did have authority by reference to section 17(2)(c) and (d) at lease. It, therefore, follows that 'control access of the kind in question' in section 17(5)(a) must apply to the respondents because they were authorised to secure access by section 17(2)(c) and (d).[96]

Because the officers had authorisation to make requests for information from the computer system, that they had exceeded the intended scope of their initial authorisation in using it to gain information they would otherwise not be entitled to obtain was a matter for the organisation to deal with internally. It did not warrant the intervention of the criminal law. This reasoning clearly follows the advice set out by the Law Commission with respect to circumstances of 'authorised access for unauthorised purposes'. The appropriate response to such conduct would be through internal disciplinary processes. However, the Court, in reaching this conclusion, had made a number of errors in statutory interpretation. As a result, the decision in *Bignell* generated wide criticism, both in respect to those errors and in the perceived effect of nullifying the application of the CMA to cases of industrial espionage.[97]

The errors the court made can be attributed to the effect of the failure of the CMA to make a proper distinction between 'access' in its noun and transitive verb form. The reference to 'access' has become a distinct point of confusion, especially as the section 1 and 2 offences do not require the accused to actually 'obtain access'. Gringas observed at the time:

---

[96] Ibid.

[97] See, eg, Andrew Murray, *Information Technology* Law (3rd ed, Oxford University Press, 2016) 363; Zaiton Hamin, 'Insider Cyber-Threats: Problems and Perspectives' (2000) 14(1) *International Review of Law, Computers and Technology* 105, 108-9.

> The offence [in *Bignell*] should have been made out … The Act is drafted in terms of 'causing a computer to perform a function' together with an intention to 'secure unauthorised access to any program or data'. It is therefore an error of law for the court to have provided judgment littered with references to 'accessing a computer'. The Act does not sanction those who access computers; it sanctions those who use computers to secure access to data and programs.[98]

The decision in *Bignell* was not only an error of law in the sense identified by Gringas, but also an error in the effect of the court linking the question of authorisation under subsection 17(5) to the identification of a discrete kind, or 'level' of access under subsection 17(2). Indeed, such linking is inappropriate by virtue of subsections 1(2)(a) to (c) which define the necessary access the accused intended to obtain as not being directed at *any* particular program or data, data of any kind, or data held in any particular computer. The inherent flexibility in the identification of what forms of access can be intended, from the computer itself, to particular programs and data, must necessarily presuppose that the legitimate controller of the data has the capacity to delimit authorisation along the same lines. As Bainbridge observed, 'being entitled to access computer material is not the same as being *entitled to control* access to such material.'[99]

Despite the interpretation of the scope of the CMA in *Bignell* aligning with that recommended by the Law Commission, it did not correspond with the actual drafting of the offences and the interpretative guidance provided. The reasoning in *Bignell* was subsequently disapproved in *R v Bow Street Metropolitan Stipendiary Magistrate and Allison, ex parte United States (No. 2)* ('Allison').[100] *Allison*, another case involving an employee, centred on facts similar to that in *Bignell*. An employee of American Express, Ms Ojomo, used her access to the American Express computer system to obtain the credit card details of customers. Ms Ojomo then provided those details to a number of third parties in the United States, as well as Mr Allison who resided in London. Fraudulent credit cards linked to those accounts would then be created and used to purchase goods.

---

[98] Clive Gringas, 'To be Great is to be Misunderstood: The Computer Misuse Act 1990' (1997) 3 *Computer and Telecommunications Law Review* 213, 215.

[99] David Bainbridge, *Introduction to Information Technology Law* (Longman, 6th ed, 2007) 443 [emphasis added].

[100] *R v Bow Street Metropolitan Stipendiary Magistrate and Allison, ex parte United States (No. 2)* [2000] 2 AC 216.

Allison thus concerned the actions Mr Allison in London; specifically on the issue of whether or not he could be extradited to the United States to face charges on the basis of the unauthorised access to the consumer accounts. The court thus had to determine whether his conduct, his collaboration with Ms Ojomo, fell within the ambit of the CMA. It thus needed to be established that Ms Ojomo was unauthorised to access the customer accounts that she passed on to Mr Allision. This required consideration of the seemingly identical issue to that in *Bignell*: where a person is authorised to access data of the kind in questions (in this case the credit card accounts of customers by an employee whose role it was to deal with those accounts), can they be deemed nevertheless to have obtained unauthorised access where the purpose to which the access is put (the manufacturing of forged credit cards) falls beyond the scope of their authorisation (providing customer service)?

Lord Hobhouse, providing the majority judgement in the House of Lords, disapproved of the view that authorisation was associated to a 'kind of data', rather it was linked to 'specific data' and 'specific purposes':

> [Section 17(5)] therefore has a plain meaning subsidiary to the other provisions of the Act. It simply identifies the two ways in which authority may be acquired – by being oneself the person entitled to authorise and by being a person who has been authorised by a person entitled to authorise. It makes it clear that the authority must relate not simply to the data or programme but also to the actual kind of access secured … It does not introduce any concept that authority to access one piece of data should be treated as authority to access other pieces of data 'of the same kind' notwithstanding that the relevant person did not in fact have authority to access that piece of data. Section 1 refers to the intent to secure unauthorised access to any programme or data. These plain words leave no room for any suggestion that the relevant person may say: 'Yes, I know I was not authorised to access that data but I was authorised to access other data of the same kind'.[101]

The question to be decided, therefore, was not to be construed on the basis of 'authorised access for an unauthorised purpose' as seemed to be the approach in *Bignell* but was rather to be considered by approaching the question of authorisation from first principles. The court applied an approach to authorisation that was substantially similar to that elsewhere in the criminal law.[102] That is, to first identify the specific access

[101] Ibid 224.

[102] *R v Jones and Smith* (1976) 3 All ER 54. This comparison will be explored in more detail in chapter 5.

involved, then consider the circumstances and degree of any authorisation, and then ask whether that degree of authorisation includes the specific action in question.

Here, Ms Ojomo had the authority to access only the credit card accounts for the customers for which she was specifically responsible. The records indicated that 'she accessed 189 accounts that did not fall within the scope of her duties'.[103] On that basis, the purpose of her access became irrelevant: Ms Ojomo's access to the particular customer files was unauthorised by virtue of the policies and practices associated with her position. She did not have a general authority from her employer to access the details of all customers. The offence was thus established.

With respect to how this approach aligned with that adopted in *Bignell*, Lord Hobhouse described the ultimate conclusions of the Divisional Court in *Bignell* as 'probably right', with the negative treatment limited to Astill J's reasoning in coming to an otherwise correct conclusion. On his interpretation of the facts in *Bignell*, Lord Hobhouse observed that:

> It was a possible view of the facts that the role of the defendants had merely been to request another to obtain information by using the computer. The computer operator did not exceed his authority. His authority permitted him to access the data on the computer for the purpose of responding to requests made to him in the proper form by police officers.[104]

On this framing, the question of authorised access for an unauthorised purpose could thus be avoided without explicitly overruling the decision in *Bignell*. The result appears to be that neither decision, either *Bignell* nor *Allison*, can be regarded as providing guidance in respect to the specific question of how to approach the issue of 'authorised access for an unauthorised purpose' directly: *Allison* having been decided on the basis that the specific intended access in that case was, in fact, unauthorised, and the reasoning in *Bignell* on that question having been disapproved. Indeed, the decision in *Allison* seems to centre on the fact that Ms Ojomo accessed the 189 accounts for which she clearly had no authority, without consideration of whether she also accessed the details of accounts for

[103] Ibid 220.

[104] Ibid 225.

which she did have some authority or the alternative where she used only the details of customers for which she was indeed responsible.

All that might be said, at least at this stage, is that the construction of authorisation does not necessarily require consideration of the purpose of the access unless in circumstances where the person entity entitled to control access to the data in question has granted a form of authority that is *conditional* or *circumstantial*. The default position, in the absence of such conditional authority, might then by that authorised access for an unauthorised purpose falls outside the scope of the offence. However, to interpret the decision in *Allison* in this way means that not only that authorisation can, and should, be limited to the specific data in question, but also that a spectrum of conditions can be placed on any 'access' as a *separate* and *additional* consideration. The result is a dramatic expansion of the scope of the offence to potentially apply even to situations where an accused may have authority to access the data, but did so by way of a method that was not itself authorised – that is conditional access provided in a terms of service agreement. The potential for this will be the subject of discussion in Chapter 5.

(c) 'modification'

Applying only in respect of interpreting the section 3 offence, 'modification' was provided interpretative guidance by subsections 17(7) and 17(8):

> (7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer –
> (a) any program or data held in the computer concerned is altered or erased; or
> (b) any program or data is added to its contents; and
>
> and any act which contributes towards causing such a modification shall be regarded as causing it.
>
> (8) Such a modification is unauthorised if –
> (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and
> (b) he does not have consent to the modification from any person who is so entitled.

The first prosecution for an offence of causing an unauthorised modification contrary to section 3 came in *R v Goulden.*[105] The accused was contracted to install security

[105] *R v Goulden* (Unreported, Southwark Crown Court, 10 June 1992).

software on a computer workstation for a printing company. That software required the setting of a password which the accused set and subsequently withheld from the company to act as a 'guarantee' against his claimed service fees totalling £2,275. The printing company was thus unable to operate their computer for a number of days, resulting in an alleged loss of £36,000 in revenue plus a further £1,000 for another contractor to override the password protection. Thus, by setting the password to one of his own choosing, the accused was deemed to have had 'modified' the security software pursuant to subsection 17(7)(b), and he had been given no consent to do so, satisfying both subsections 17(8)(a) and 17(8)(b). He was convicted, with the court imposing a two-year conditional discharge and a fine of £1,650.

Similar conduct would later arise in the context of software designers seeking to implement design features into that software which would allow them to protect their intellectual property rights. In *R v Whitaker*,[106] in the context of a dispute over a software license payment, the accused enacted a function that had been designed into the software that would make it unusable: a 'logic bomb'. The accused argued that pursuant to the conditions in the software license, the intellectual property rights in the software were reserved to himself, and he was thus the person 'entitled to control' the software. The court disagreed, but only with respect to the wording of the particular licensing agreement. Had the agreement expressly included a reference to such a capability, then the accused would have been authorised to protect his interest in the manner in which he did. The court, thus, lent support to the idea that the person 'in control' of a piece of software can remain the developer, even where installed on a computer system owned by another.

The issue of the development and deployment of malicious software (computer viruses and malware) would be first addressed in the case of *R v Pile.*[107] The accused was a self-taught programmer who, working under the online pseudonym the 'Black Baron', created two viruses, Queeg and Pathogen, which he shared on various online chat forums, encouraging others to make use of them. Relying on the expansive construction

[106] *R v Whitaker* (Unreported, Scunthorpe Magistrates Court, 1993).

[107] *R v Pile* (Unreported, Plymouth Crown Court, 15 November 1995).

of 'intent' under subsection 3(3), the court had very little difficulty in finding the accused's conduct was indeed a contravention of the section 3 offence.

While a number of subsequent prosecutions in relation to the creation and distribution of computer viruses and malware were successful,[108] concerns began to arise in relation to the newer phenomenon of 'denial of service' ('DoS') attacks.[109] DoS attacks exist in a number of forms but ultimately involve flooding a computer or server with a high enough volume of access requests that it becomes overloaded and incapable of responding effectively: the target service becomes inaccessible and inoperable. Unlike the operation of computer viruses or malware as being 'added' to the contents of a computer, or enabling direct access to bring about the 'erasure of data', DoS attacks do not result in any change to the contents of the target. Instead, it is akin to parking a car such that it blocks other users from using a driveway. There was thus a risk that such conduct would fall outside the scope of the section 3 offence as drafted.

The first case to test these concerns was *DPP v Lennon* ('Lennon').[110] The accused was a former employee who utilised a technique referred to as 'mail-bombing' against his former employer's email server. This involved the use of software to facilitate the sending in excess of five million emails, thus overloading the email server and impairing its function. At first instance, the court had no issue establishing that the sending of emails constituted a 'modification' as it resulted in the details and content of the email being stored on the employer's server. However, the accused was acquitted on the basis that there was an 'implied' authority to send an email. This was reversed on appeal, with the Divisional Court determining that the totality of the conduct should be assessed, rather than assessing each access or modification individually: thus, while there is an implied authority to send one email, there is no such authority to send five million simultaneously.

---

[108] See, eg, *R v Vallor* [2004] 1 Cr App R 54, a case similar to *Pile*, which involved the creation and distribution of the Gokar, Redesi and Admirer mass-mailing viruses.

[109] Along with the more complicated 'distributed denial of service' ('DDoS') attacks. For a taxonomy of DDoS attacks, see, Jelena Mirkovic and Peter Reiger, 'A Taxonomy of DDoS attacks and DDoS Defence Mechanisms' (2004) 34(2) *ACM SIGCOMM Computer Communication Review* 39.

[110] *DPP v Lennon* [2006] EWHC 1201.

The ultimate success in *Lennon*, however, did not assuage concerns as to the suitability of the structure of the section 3 offence. The conduct of the accused in *Lennon* was only captured because the sending of an email results in it being stored on the target server, thus modifying its contents. No such modification occurs when a DoS attack is carried out by other means. This would ultimately result in substantial changes to the section 3 offence, set out in sub-section 2 below.

(d) 'intention' and 'knowledge'

The *mens rea* requirements that the accused operated both with the 'intention to secure access' and with 'knowledge' that the access they intended to secure was, in fact, unauthorised received no specific definitional guidance in the CMA and was thus left to general principles, save to specify that the intent required on the part of the accused need not be linked to *any* specific computer, program, or data.[111] Thus, with 'intent' not being linked to any specific aspect and the broad definition given to 'access', the operation of 'intent' serves only as a limited restraint on the scope of the offence. The mere intentional act of turning on a computer, clicking the mouse, or typing on a keyboard could be enough to enliven criminal liability. Thus, the 'knowledge' requirement has sufficient work to do.

There is limited guidance as to how the test for knowledge is to be approached: is it, as one would assume, a subjective assessment,[112] or is constructive knowledge sufficient? Many situations would involve circumstances where the accused has clearly been presented with information from which subjective knowledge can be established or inferred: the presentation of a log-in screen for which the accused did not possess the requisite passwords, or, policies, signs or verbal instructions.[113] However, the Court of Appeal in *Lennon*, introduced above, appeared to endorse an objective standard by considering how a person entitled to control the computer, program or data, would

---

[111] *Computer Misuse Act 1990* s 1(2).

[112] See, eg, Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd ed, 2015) 105.

[113] *Ellis v DPP (No. 1)* [2001] EWHC Admin 362.

respond if any access of the kind ultimately obtained was requested 'in the normal course of business'. The Court of Appeal observed:

> If Mr Lennon had telephoned Ms Rhodes and requested consent to send her an e-mail raising a point about the termination of his employment, she would have been puzzled as to why he bothered to ask and said that of course he might. If he had asked if he might send the half million emails he did send, he would have got quite a different answer.[114]

While, as Clough observed, this might be useful in assessing the reasonableness of a subjective belief held on the part of the accused that their conduct was indeed authorised, the core of the test ought to remain subjective.[115] Indeed, consideration of the reasonableness of the belief would present no challenge for the jury in acquitting the accused in the high profile case of *R v Ashford.*[116] The accused, a journalist, was charged with unauthorised access to a stolen smartphone belonging to a public relations ('PR') agent, contrary to the section 1 offence, and possession of criminal property.[117] He testified at trial that he was not aware that the phone the was stolen when given to him by his 'source', a 20-year old who 'had evidence of a celebrity cheating on his partner'. He claimed to have believed that either it was an orchestrated leak on the part of the agent, or that his employer had cleared it with the legal department as they had directed him to the 'source' in question such that he did not turn his mind to the issue. Further, the smartphone was not protected with a passcode. He spent hours exploring its content before being altered to the fact the phone was stolen via a public tweet from the PR agent. The jury was ultimately convinced that he did not know his conduct was unauthorised.[118]

Perhaps the most interesting case to deal with the question of 'intent' was *R v Bedworth,*[119] which, although providing little in the way of interpretive guidance, involved an accused who successfully claimed to have suffered from 'computer tendency

---

[114] Ibid [9].

[115] Clough (n 112).

[116] *R v Ashford* (Unreported, Westminster Magistrates Court, 13 August 2014).

[117] *Proceeds of Crime Act 2002* s 329.

[118] This, and broader questions as to the construction of knowledge will be returned to in Chapter 5.

[119] *R v Bedworth* (Unreported, Southwark Crown Court, 21 May 1993).

syndrome'.[120] The accused was charged with conspiracy to commit offences under both sections 1 and 3 of the CMA for obtaining unauthorised access to a number of computer systems.[121] He pleaded not guilty on the basis that he was a computer addict and thus could not form the necessary intent. His two other co-conspirators pleaded guilty. During the trial defence counsel called an expert psychiatric witness who attested to the nature of the accused's addiction, and he was subsequently acquitted by the jury.

However, given the charge was that of conspiracy, the necessary intent was in relation to the formation of an agreement between the conspirators with the intent that one or more of them should carry out the object of the conspiracy so agreed. This standard is higher than that required by section 1, which merely requires an intention to secure access. Charlesworth has observed that had the accused instead been charged under section 1, which was available to be pursued in its own right, there was a higher likelihood he would have been found guilty.[122]

B *Offences Subsequently Amended or Introduced*

As discussed above, in the years following the introduction of the CMA a number of successful prosecutions were pursued under the section 3 offence in relation to the creation and distribution of computer viruses and malware, and some forms of DoS attacks. However, sufficient concern was expressed with respect to the capacity of the CMA to keep pace with the rapid uptake of the internet and the 'new' ways that legitimate computer use could be impacted upon.[123] As such, the section 3 offence was repealed and replaced in 2006, now making it an offence to 'impair' the function of a computer. A further new offence was added at the same time, section 3A, which specifically

---

[120] Not to be confused with the legitimate 'computer vision syndrome' which is a recognised condition resulting from using electronic displays for extended and uninterrupted periods of time which can result in headaches, blurred vision, eye strain, fatigue and vertigo. See, eg, Esteban Porcar, Alvaro M Pons, and Amalia Lorente, 'Visual and Ocular Effects from the Use of Flat-Panel Displays' (2016) 9(6) *International Journal of Ophthalmology* 881.

[121] Belonging to British Telecom, the European Commission, and the Financial Times, amongst others.

[122] Andrew Charlesworth, 'Legislating Against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990' (1993) 4(1) *Journal of Law and Information Sciences* 80, 91. Charlesworth attributed the acquittal to 'misplaced sympathy' from the jury.

[123] See, eg, John Worthy and Martin Fanning, 'Denial-of-Service: Plugging the Legal Loopholes?' (2007) 23 *Computer Law & Security Review* 194, 195.

criminalised the production and distribution of hacking tools, computer viruses, and malware. In 2015, as part of a suite of new or strengthened terrorism-related offences, a new offence of 'unauthorised acts causing, or creating risk of, serious damage', section 3ZA, was also introduced.

1 *Unauthorised Acts with Intent to Impair – the reformed section 3*

The initial formulation of the section 3 offence required an unauthorised modification: the addition to, or deletion of, the contents of a computer. The revised section 3 offence focussed instead on impairment to the operation of a computer or the prevention or hindrance of legitimate use.[124] Any impairment would need only be temporary,[125] and it would also become an offence to do an act that could enable subsequent impairment until its repeal in 2007 (reflected below).[126] The redrafted section 3 offence provides:

> (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 the reliability of any such data; or
> (c) to impair the operation of any such program or the reliability of any such data.
>
> (3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (c) of subsection (2) above.

Thus, the redrafted form of section 3 removed the requirement that there be an actual 'modification' to a computer and instead operates to criminalise any act done with an accompanying intent to impair the computer or to prevent or hinder legitimate access. Further, contrary to the initial recommendation made by the Law Commission, the redrafting introduced recklessness as a sufficient condition to enliven criminality, bring the offence more into line with the offence of criminal damage.[127] At the same time, the

---

[124] Introduced by virtue of the *Police and Justice Act 2006* s 36.

[125] *Computer Misuse Act 1990* s 3(5)(c).

[126] *Computer Misuse Act 1990* s 3(2)(d), later repealed by the *Serious Crime Act 2007* ss 61(3)(a)(i), 92, 94.

[127] *Criminal Damage Act 1971* s 1(1).

maximum penalty for the commission of this new offence was set at, on conviction on indictment, ten years imprisonment, the maximum statutory fine, or both.[128]

The breadth of the new section 3 offence has resulted in a number of successful prosecutions for DoS and DDoS attacks against high profile institutions and services.[129] The offence continues to provide no defences, a particular concern for security researchers investigating security threats whose conduct and subsequent dissemination of their findings could fall within the scope of 3(3).[130] Concern has also been expressed about the lack of recognition of the use of DoS and DDoS attacks as a form of civil disobedience: albeit that conduct qualifying as civil disobedience necessary requires the individual concerned to accept the consequences of the conduct.[131]

A further consequential amendment to the redrafting of the offence was to amend the guidance to the interpretation of 'modification' in subsections 17(7) and 17(8) outlined above. Whereas their initial form provided guidance on the interpretation of both 'modification' and 'unauthorised', the amended form now only provides for the interpretation of unauthorised with respect to 'an act done in relation to a computer' in a new subsection 17(8):

> (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
>
> In this subsection 'act' includes a series of acts.

[128] *Computer Misuse Act 1990* s 3(6).

[129] See, *R v Weatherhead, Rhodes, Gibson & Burchall* (Unreported, Southwark Crown Court, 24 January 2013).

[130] For instance, work carried out in identifying websites that were running versions of 'OpenSSL' that supported the vulnerable Heartbeat protocol (which allowed passwords, crypto-keys, and other sensitive data to be obtained from the memory of the 'secure' server software) would have contravened section 3. See, eg, John Leydon, 'It may be illegal to run Heartbleed health checks – IT Lawyer', *The Register* (11 April 2014) <http://www.theregister.co.uk/2014/04/11/heartbleed_health_checking_services_may_be_illegal/>.

[131] See, eg, Mathias Klang, 'Virtual Sit-Ins, Civil Disobedience and Cyber Terrorism' in Mathias Klang and Andrew Murray (eds), *Human Rights in a Digital Age* (Routledge, 2005) 135; Molly Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience* (Bloomsbury, 2014).

The effect of this new guidance is to simplify and clarify that the approach to assessing 'authorisation' must necessarily take the form of a consideration as to the nature and scope of any consent the accused may have had in relation to their conduct. In another step to increase clarity, the pre-existing exclusion of the applicability of the *Criminal Damage Act 1971* that was in the original drafting of subsection 3(6) was removed and inserted into the *Criminal Damage Act* itself,[132] although without any impact as to its operation.

2 *Making or Supplying Articles – section 3A*

Also introduced by the *Police and Justice Act 2006*[133] was a series of new connected offences to cover the development, possession and supply of any article (physical or software-based) that could be utilised to commit, or facilitate the commission of, any of the other offences within the CMA. Section 3A was introduced to ensure compliance with Article 6 of the European Cybercrime Convention which requires parties to adopt such 'legislative and other measures as may be necessary' to ensure such conduct was criminalised in domestic law.[134] This was necessary as the amendments to the section 3 offence set out above could potentially result in 'gaps' in respect of prosecuting the creation of computer viruses and malware, although it is not entirely clear why such conduct would not be pursued pursuant to the 'reckless enabling' formulation available pursuant to subsections 3(2)(d) and 3(3).

The aim of section 3A was thus to ensure the criminalisation of the creation, possession and distribution of hacking tools, viruses, and other malicious software. Section 3A provides:

> (1) A person is guilty of an offence if he 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 or 3.

---

[132] *Criminal Damage Act 1971* s 10(5), inserted by *Police and Justice Act 2006* s 53(1), Sch 14[2].

[133] *Police and Justice Act 2006* ss 37, 53, Sch 14.

[134] *European Convention on Cybercrime,* opened for signature 23 November 2001, ETS 185 (entered into force 1 July 2004).

(2) A person is guilty of an offence if he supplies or 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 or 3.

(3) A person is guilty of an offence if he obtains any article with a view to it being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.

(4) In this section 'article' includes any program or data held in electronic form.

Conviction on indictment could attract a maximum term of imprisonment of two years, the statutory maximum fine, or both.[135] These offences are not without controversy, again particularly in relation to the lack of an available defence for computer security researchers. However, a prosecution is only possible where the *mens rea* element of intending, or believing, that the article will be used to commit an access or impairment offence can be established.[136] This, however, provides no shield to the other offences within the CMA.

There have been very few prosecutions under section 3A since its introduction, and those that have been initiated have resulted in guilty pleas.[137] It was observed, however, that a potential 'loop-hole' existed in the structure of subsection 3A(3) in that it was a criminal offence to obtain an article 'with a view to it being supplied'[138] to another, but obtaining such an article for personal use was not an offence. That is, the offence required a third party.[139] As such, a further amendment was required to address this shortcoming.

---

[135] *Computer Misuse Act 1990* s 3A(5)(c). A summary conviction carries a maximum term of imprisonment of 12 months, the maximum statutory fine, or both per s 3A(5)(a).

[136] While there is no exemption for such work, the Crown Prosecution Service prosecution guidelines outline a number of considerations that ought to be factored into a decision to prosecute under section 3A. These include; the primary purpose of the article at issue, whether or not the article is available on a commercial basis, is it widely used for a legitimate purpose, and what is the context in which the article is used. It was widely reported by the media in 2015 that later amendments made by the *Serious Crimes Act 2015* introduced new exemptions for GCHQ, intelligence officers and police to 'hack' without criminal liability, but this was not the case. The consequential amendments to *Computer Misuse Act 1990* s 10 merely clarified the interaction between the use of powers authorised elsewhere (see, eg, *Regulation of Investigatory Powers Act 2000*) and the offences set out in CMA.

[137] *R v McLoughlin* (Unreported, Southwark Crown Court, 13 May 2011); *R v Mangham* [2012] EWCA Crim 973; *R v Martin* (Unreported, Maidstone Crown Court, 16 May 2013).

[138] *Computer Misuse Act 1990* s 3A(3).

[139] See, Home Office, 'Home Office Circular: Serious Crime Act 2015' (March 2015) <https://www.crimeline.info/uploads/docs/seriouscrimeact2015.pdf>.

Such amendment was later provided in the form of sections 42 and 88(1) of the *Serious Crime Act 2015,* which amended the offence in subsection 3A(3) to read:

> (3) A person is guilty of an offence if he obtains any article –
> (a) Intending to use it to commit, or assist in the commission of, an offence under section 1, 3, or 3ZA; or
> (b) with a view to it being supplied for use to commit, or to assist in the commission of, an offence under section 1, 3, or 3ZA.

3 *Unauthorised Acts Causing Serious Damage, or Risk Thereof – section 3ZA*

As evident by the inclusion of a section 3ZA offence in the amended form of subsection 3A(3) above, the *Serious Crime Act 2015* also simultaneously introduced that offence.[140] The section 3ZA offence responds to unauthorised conduct in relation to a computer that results in, or creates significant risk, or serious damage of a 'material kind'. It is primarily aimed at serious 'cyber-attacks' and acts of 'cyber terrorism' against systems considered 'critical infrastructure': power supply, communications, food or fuel distribution, and transportation networks. It represents further recognition of the increasingly important role of, and reliance upon, computer systems. The section 3ZA offence provides:

> (1) A person is guilty of an offence if –
> (a) the person does any unauthorised act in relation to a computer;
> (b) at the time of doing the act the person knows that it is unauthorised;
> (c) the act cause, or creates significant risk or, serious damage of a material kind; and
> (d) the person intends by doing the act to cause serious damage or a material kind or is reckless as to whether the damage is caused.
>
> (2) Damage is of a "material kind" for the purpose of this section if it is –
> (a) damage to human welfare in any place;
> (b) damage to the environment of any place;
> (c) damage to the economy of any country; or
> (d) damage to the national security of any country.
>
> (3) For the purpose of subsection (2)(a) 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.

[140] *Serious Crime Act 2015* ss 42, 88(1). The other offences contained within the *Computer Misuse Act 1990* s 3A were similarly amended to reflect this pursuant to *Serious Crime Act 2015* ss 41(4), 88(1).

Offences contrary to section 3ZA are prosecuted on indictment only and can receive a maximum term of imprisonment of up to 14 years, a fine, or both.[141] But, where the harm caused, or significant risk of harm created, is to human welfare in the form of loss of life or human injury or illness,[142] or where the damage is to 'national security',[143] the accused is liable for life imprisonment, a fine, or both. Crown Prosecution Service prosecution guidelines advise that prosecutions under this offence should be handled only by the Special Crime Counter-Terrorism Division.

This offence is, as yet, untested, and it remains to be seen what scope of conduct would indeed by encompassed, particularly in relation to assessing the creation of a 'significant risk' of harm, and the degree of causal connection required between the unauthorised act on the computer or network and the resulting harm.

4 *Incidental amendments*

The *Police and Justice Act 2006*, while introducing the new section 3 and the offences set out in section 3A, also modified the sentences of available for the section 1 and section 2 offences.

In respect of the section 1 offence, its character was changed from that of a summary offence to an offence triable either way.[144] On summary conviction, the offence now carries a maximum term of imprisonment of 12 months, the statutory maximum fine, or both.[145] On conviction on indictment, the section 1 offence can attract a maximum imprisonment term of two years, the statutory maximum fine, or both.[146] The conversion of the offence from summary to indictable also renders the section 1 offence

---

[141] *Computer Misuse Act 1990* s 3ZA(6).

[142] *Computer Misuse Act 1990* s 3ZA(7)(a).

[143] *Computer Misuse Act 1990* s 3ZA(7)(b).

[144] Amended pursuant to *Police and Justice Act 2006* ss 35(3), 53.

[145] *Computer Misuse Act 1990* s 1(3)(a).

[146] *Computer Misuse Act 1990* s 1(3)(c).

subject the *Criminal Attempts Act 1981*. It is thus now possible to be prosecuted for attempting to cause a computer to perform a function.[147] This despite the Law Commission initially arguing that a custodial sentence should be a last resort, given the design and breadth of the offence was capable of applying to non-serious conduct, and even where justified should have been limited to a term of three months. In respect of the section 2 offence, the maximum penalty for summary conviction was increased from six to 12 months.[148] The penalty for a conviction on indictment remained unchanged at five years.[149]

It should also be noted that as of 2015, the £5,000 limit for fines with respect to the offences under the CMA has been removed as part of broader changes introduced by subsection 85(1) the *Legal Aid, Sentencing and Punishment of Offenders Act 2012*. The offences now carry potentially unlimited fines.

The package of amendments in respect of the CMA contained in the *Police and Justice Act 2006*, including the introduction of both the new section 3 and section 3A offences, were not without some criticism, albeit unheeded at the time. Lord Northesk commented in a written statement to the House of Lords that he was:

> unconvinced that the insertion of these few odd confused clauses … demonstrates either adequate understanding of the complexities of the issues or firm resolve to attend to the whole corpus of internet crime...To be blunt, I fear that ultimately these clauses will create more problems than they solve[150]

While the remainder of this thesis will focus attention on exploring the scope and effect of the problems hinted at by Lord Northesk, it is necessary to first briefly introduce and survey the utilisation of the CMA in practice.

---

[147] *Criminal Attempts Act 1981* ss 1(1), 1(4).

[148] *Computer Misuse Act 1990* s 2(5(a), amended by *Police and Justice Act 2006* ss 52, 53, Sch 14[17].

[149] *Computer Misuse Act 1990* s 2(5)(c).

[150] HL Deb, 11 July 2006, vol 684, cols 607.

IV PROSECUTORIAL TRENDS

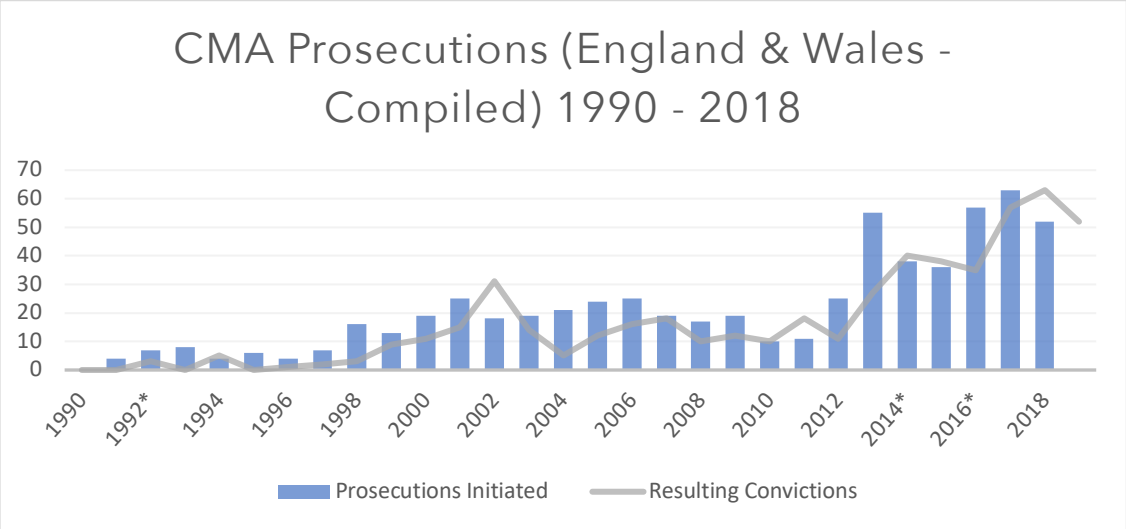
The use of computers in the commission of a more general, non-computer specific, criminal offences may be prosecuted as both that general criminal offence *and* as an offence contrary to the CMA. This results in difficulty in accurately assessing the true scale of prosecutions for conduct that might be considered computer misuse or conduct that relies on or is enabled by unauthorised access. Adding to this difficulty is the practical issue that prosecutions under the CMA have thus far tended to be dealt with entirely in the lower courts, more often than not accompanied by guilty pleas. Consequently, the higher courts have had limited opportunity to consider, define, and provide guidance as to the scope of the offences. A lack in the reporting of cases also increases the difficulty in assessing the necessity of the CMA.

Any attempt to accurately identify prosecutorial trends and the role of computer use *between* prosecutions under the CMA and other non-computer specific criminal offences is also hampered by approaches to record keeping. The Ministry of Justice, for instance, keeps track of prosecutions made under the CMA, but these appear to be limited to cases where a CMA offence is the lead offence charged: that is the first charge listed in the initiating instrument, generally the most serious offence. Thus, for example, an incidence of online fraud could be prosecuted as several alternative offences, and, if the CMA offence was listed second or lower, it does not appear in the Ministry of Justice's 'official' statistics. However, much analysis of the operation of the CMA has centred on these figures. Therefore, the broader question of the interaction *between* types of criminal offences has largely been missed.

The table below sets out the number prosecutions according to the Ministry of Justice statistics publicly released: at the time of writing only available for prosecutions between 1990 and 2013.[151] More recently, Lord Maginnis of Drumglass, in a written question presented in the House of Lords, asked Baroness Williams of Trafford to provide the number of hacking offences relating to customer banking accounts that had been prosecuted throughout the period 2015-17. The answer provided, while noting that the

[151] HC Deb, 26 March 2014, vol 578, cols 275-6W. The figures for the years to 2018 are the result of research undertaken from a variety of sources, with a table of identified cases located in Appendix 1.

Government does not hold data on such incidents specifically, advised that for the period 2015-17, 142 convictions for offences contrary to the CMA were recorded.[152] The 142 figure, having originated from the Ministry of Justice, thus only represents those successful prosecutions where the CMA offence was listed first.



As can be observed in the table above, few offences under the CMA appear to have been pursued during the period immediately following its introduction: 1991-1998. After 1998, prosecutions rose modestly before plateauing with an apparent downward trend beginning in 2006 and subsisting until 2011. The media reported this apparent decline as evidence of the failings of the CMA and the broader law enforcement regime in respect of these kinds of offences.[153] However the period 2011-13 appears to show a substantial increase in prosecutions, coinciding with the adoption of the National Cyber Security Strategy in 2011,[154] and the formation of the National Crime Agency, staffed with specialist 'cyber crime' personnel, who in 2013 would emerge as the National Cyber

[152] HL Debates, 12 November 2018, Bank Services: Hacking: Written question - HL11092.

[153] See, eg, John Leyden, 'UK prosecutions for hacking appear to be dropping', *The Register* (18 May 2012) <https://www.theregister.co.uk/2012/05/18/uk_hacking_prosecutions_decline/>.

[154] Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (London, 2011).

Crime Unit.[155] A new reporting centre, 'ActionFraud', was also established to streamline the process for victims of computer-related crime to report to law enforcement. The years 2011 through 2013 are particularly notable for the apparent spike in CMA prosecutions: this seemingly corresponds to the implementation of 'Operation Tuleta' which began in mid-2011 with six officers working solely on computer misuse cases continuing through to 2013 and accounting for 21 arrests and prosecutions.[156]

While the table above would seem to indicate a slow and steady rise in the number of prosecutions, these figures represent only those prosecutions where the CMA offence was the lead charge. The conclusions drawn by the media and other commentators are thus not entirely made out: the official data does not account for the instances of prosecutions under the CMA *in addition to* more substantial general criminal law offences, such as fraud. The discrepancy in the Ministry of Justice's account of prosecutions under the CMA was made particularly apparent in 2014 when Cordery Legal Compliance submitted a freedom of information request to the Crown Prosecution Service ('CPS') for data relating to CMA prosecutions. In response, the CPS released a tally of the total number of prosecutions for offences under the CMA they had launched between January 2008 and June 2014.[157] While the data provided to Parliament by the Ministry of Justice identified ~137 offences contrary to the CMA had been pursued, the CPS data, however, revealed that prosecutions for 218 offences contrary to the CMA were initiated in 2013 alone, with 702 offences prosecuted across the period January 2008 to June 2014. No information was provided in relation to the number of resulting convictions.

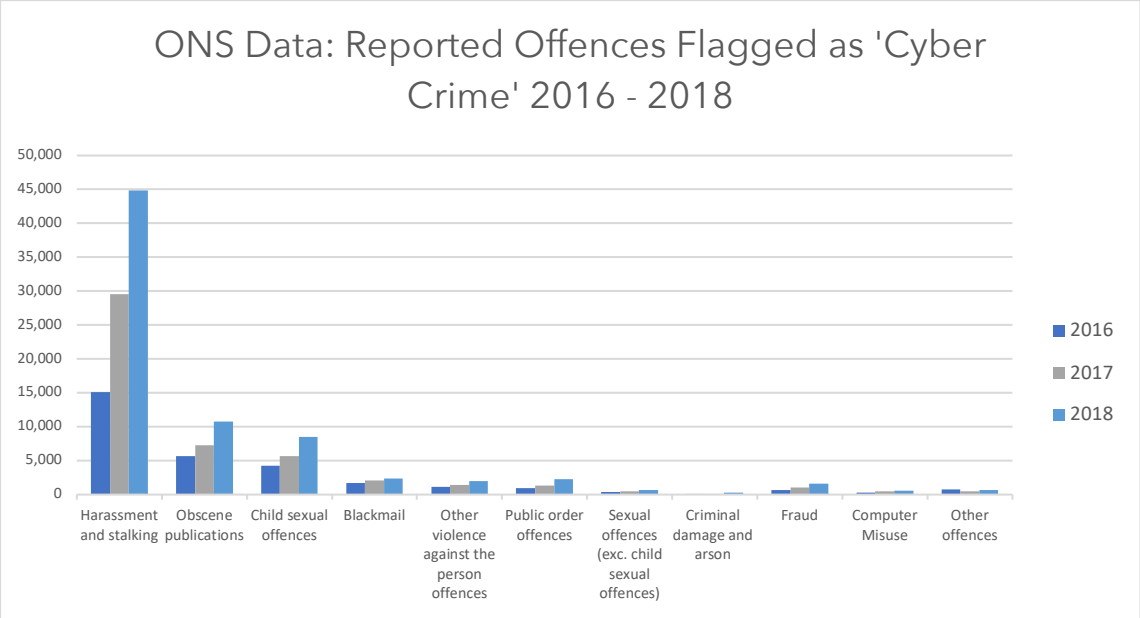
---

[155] Home Office, 'The National Crime Agency: A Plan for the Creation of a National Crime-Fighting Capability' (Cm 8097, 2011); Cabinet Office, 2010-2015 Government Policy: Cyber Security (London, 2013).

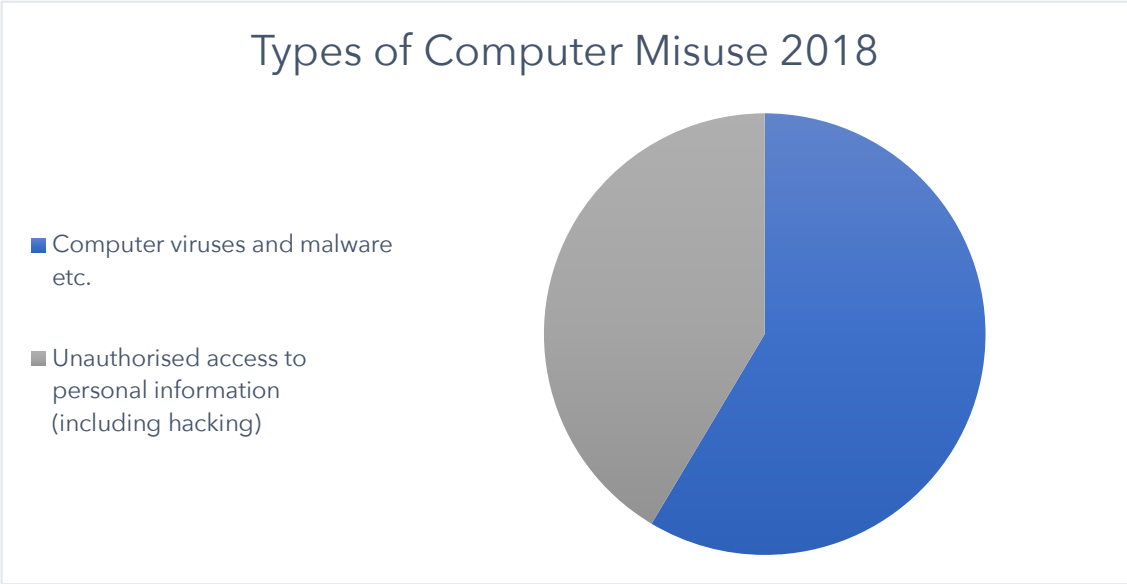
[156] See, eg, Oliver Poole and Justin Davenport, 'Scotland Yard starts new team to look into hacking', *London Evening Standard* (10 June 2011) < https://web.archive.org/web/20110614082416/http://www.thisislondon.co.uk/standard/article-23959562-scotland-yard-starts-new-team-to-look-into-hacking.do>.

[157] See, André Bywater, 'Cybercrime & Security Update: Prosecutors confirm 702 hacking cases charged', *Cordery Legal Compliance* (24 November 2014) <http://www.corderycompliance.com/cybercrime-security-update-prosecutors-confirm-702-hacking-cases-charged/?>.

In comparing the CPS' number of total prosecutions with that held by the Ministry of Justice, it is possible to deduce, although with a limited degree of confidence, that of the 218 offences pursued by the CPS, 55 of those involved *only* offences under the CMA, or where an offence under the CMA was listed first. The remaining 163 offences may have thus involved circumstances where the offences under the CMA were charged in addition to, or secondary to, a further substantive offence. Put another way; general criminal offences were 74.8% of offences pursued in 2013 for criminal conduct involving computers. This is a trend that has only continued. In 2016 the Office of National Statistics (the 'ONS') began publishing a breakdown of all reported instances of crime that were identified as involving a computer. The results for the years 2016 – 2018 can be observed in the table below:



What is immediately apparent here is the dramatic increase in reports of computer-facilitated harassment and stalking, the possession and distribution of obscene publications and child exploitation material. 'Computer misuse' is defined by the ONS as both the possession and use of viruses and malware and the 'unauthorised access to personal information (including hacking)'. Reports of instances of these crimes represent ~1% of all reported instances of computer-related crime. Indeed, the production or use of malware makes up the majority of reported instances of computer misuse.



Over the three years since the collection of these broader computer-related crime statistics began to be collated and released, there has been a dramatic increase across most of the general criminal offence categories, particularly harassment and stalking, obscene publications and child exploitation material offences. There have also been increases in reports of computer-enabled blackmail and fraud (although the volume of reports is perhaps lower than might otherwise be reasonably expected). Nevertheless, computer misuse, while itself subject to an increase of reported instances, appears minimal and isolated in its utility as a characterisation of computer-related/enabled crime.

It is immediately apparent, however, that there is scope for a significant degree of potential overlap between the CMA offences and more general criminal offences. As was observed throughout this chapter, the offences within the CMA were drafted broadly so as to apply to any form of unauthorised computer use, including those that merely involve steps taken to achieve unauthorised access. The use and misuse of computers thus appear in practice to exhibit a substantial degree of overlap with conduct capable of falling within the framing of general offences. Changes in the use and function of computing technologies have seemingly contributed to the drastic rise in the reported use of computers in non-computer related offences. The questions then become; what are the causes of this apparent overlap, is the overlap justified, or, put another way, is the broad

nature of the CMA section 1 and 2 offences serving a proper and justifiable function within the criminal law?

While overlap in the criminal law is not in itself necessarily an issue, the fact that nearly three-quarters of actual prosecutions appear to have some interaction with general criminal offences raises concern. This concern is deepened when it is further considered that only 1% of crimes reported as involving computers represent 'pure' computer misuse. These experiences raise several challenges to the justifications put forward to support the creation, maintenance, and expansion of the CMA. These will be considered across chapters 4, 5 and 6, with particular focus on the changes that have occurred to computing technologies, our broader understandings of criminal behaviour involving computers, and the cumulative impact of these developments with the broadening of the structure and operation of general criminal offences alongside the operation, in particular, of the CMA's section 1 offence.

V CONCLUSION

In this chapter, it was observed that the recommendations put forward by the Law Commissions in their Final Report represented a substantial shift for the conservative and cautious approach that initially informed the Working Paper. The Law Commission thus recommended the creation of three new computer offences: an offence of causing a computer to perform a function with intent to secure access, an ulterior intent offence where the access intended to be secured was attempted to further an intent to commit a more serious general offence, and an offence in respect to the modification of the contents of a computer.

These offences were justified on the grounds that a legitimate public interest lies in the protection of the integrity of computer, and that 'hacking' needed to be deterred in order to promote investment and confidence in computing technologies. Further reference was made to the criminogenic nature of hacking, and that 'hackers' as an identifiable group would be the most likely to engage in the potentially harmful conduct enabled by computing technologies. As such, it was recommended that the offences be drafted broadly, particularly the basic offence, to dissuade such conduct, balanced with the recommendation that penalties should be proportionate to the resulting

consequential harms: the basic offence was to be a summary offence with an imprisonment term limited to the three months and reserved for only the most serious cases. The other offences would have proportionally higher punishments to reflect both the seriousness of the conduct and the requirement that a specific or further criminal intent on the part of the accused was a contributing and motivating factor of their conduct.

The CMA, as initially introduced, was modelled closely on these recommendations, save the provision for a maximum imprisonment term of six months for the basic offence. However, as the Law Commission did not provide a draft bill, the final construction of the offences was left entirely to Parliament. Their final bill aligned with the views of the Law Commission in a broad conceptual sense, but departed in essential respects, particularly with to the interpretative guidance provided to the courts.

Initial prosecutions were met with success. This success was the result of the number of guilty pleas entered into, and the tendency to initiate prosecutions against employees or 'insiders', rather than the 'outsider' hacker. However, definitional issues began to emerge initially resulting in a limitation of the scope of the offences, before ultimately being interpreted to apply to circumstances far beyond that initially contemplated, including to circumstance of 'authorised access for unauthorised purposes' and the granular, data-specific approach to delimiting authorised use from unauthorised use. New forms of computer misuse were further enabled by the introduction and adoption of the internet, in particular DoS and DDoS attacks, which required substantial amendment to the unauthorised modification offence, later becoming an unauthorised impairment offence. This was coupled with the introduction of two new offences in the form of creating, obtaining, and distributing articles for use in the commission of any of the CMA offences, and an offence for unauthorised acts causing, or creating significant risk, of material damage.

At the same time, the proscribed penalty for conduct contrary to the basic offence was substantially increased. It became triable either way, enabling a potential offence of an attempt to cause a computer to perform a function, and a new maximum term of imprisonment of two years, far above the penalty the Law Commission had initially

believed justifiable. Their recommendation was made, of course, in the context of a proposed offence that, despite being broad, was conceived to be narrower than the resulting offence.

Throughout its operation, prosecutions under the CMA have been difficult to track accurately, with the Ministry of Justice only recording prosecutions where the CMA was the first offence listed in the initiating instrument. Despite a seemingly low number of prosecutions according to these statistics, the actual number of prosecutions is substantially higher. Importantly, a large proportion of these prosecutions appear to be pursued in conjunction with other general offences. The recent increase in prosecutions has been the result of an increase in the available resources for law enforcement to pursue computer misuse, along with new strategies focusing attention on such conduct.

All the while, computing technologies have continued to evolve, and so too has the structure and operation of general criminal offences which have been themselves subject to review and amendment.

This thesis now turns its attention to exploring the scope of the section 1 and 2 offences in respect to the current and evolving landscape of computing technologies in an attempt to broadly understand the degree of overlap with general criminal offences, and the potential for increased over-inclusiveness. Chapter 4 begins with a focus on the definitions of 'computer' and 'access' in the context of the CMA's approach to technology neutral-drafting.

Chapter 4

'Computers' and 'Access': The Effect of Technology Neutral Drafting

---

Programmers should never be satisfied with languages which permit them to program everything, but to program nothing of interest easily.

Alan J Perlis [1]

I Introduction

Alan Perlis made the above remark during his acceptance speech in becoming the first recipient of the A.M. Turing Award in 1966, an award that has evolved to become regarded as the equivalent of the Nobel Prize within the field of Computer Science. Perlis was instrumental in the creation of ALGOL, a computer programming language that would become a standard feature in texts produced by academics and members of the Association for Computer Machinery for over 30 years. It has had a substantial influence

[1] Alan J Perlis, 'The Synthesis of Algorithmic Systems' (1967) 14(1) *Journal of the Association for Computing Machinery* 1-9.

on the development of more modern programming languages.[2] We see in his comments that such languages should be designed to provide users with the means to express an algorithm (or instruction to the computer) in a manner that best matches the problem they want to solve.[3]

The criminal law shares a similar ideal. The construction of an offence should provide law enforcement and prosecutors the ability to identify and respond to an experienced wrong with a characterisation that best fits that totality of the circumstances that qualify for a response from the criminal law.[4] Returning to our normative model from Chapter 1, the criminal law ought to seek to suitably define and identity harmful and wrongful conduct in such a way that those subject to the prohibition can be adequately informed of its scope.[5] In achieving this when it comes to computer-related offences, attention must also be given to balancing the Collingridge dilemma and the pacing problem such that underlying shifts in the use and operation of technology do not result in unintentional over-inclusiveness.[6] With respect to the normative model proposed in Chapter 1, any properly constructed criminal offence ought not to presume wrongdoing from a course of conduct, and the approach to defining that conduct should not be constructed and applied such that those subject to its prohibition are unaware, or inadequately informed, of its scope.

This chapter will explore how the drafting of the *Computer Misuse Act 1990* ('CMA'), particularly the interpretation of 'computer' and 'access' in the *actus reus* of the section 1 offence, sits as against the development of computing technologies. While the discussion in Chapter 3, concerning the offences themselves and the notion of 'access', provided a

---

[2] Barbara Ryder et al, 'The impact of software engineering research on modern programming languages' (2005) 14(4) *ACM Transactions on Software Engineering and Methodology* 431.

[3] N Solntseff and A Yezerski, 'A Survey of Extensible Programming Languages' in Mark Halpern et al (eds) *Annual Review in Automatic Programming: International Tracts in Computer Science and Technology* (Elsevier, 2014) 267.

[4] See, eg, Tatjana Hörnle, 'Theories of Criminalization' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 679, 686-95.

[5] These considerations fall within the ambit of Ashworth's principle of *fair labelling*. See, James Chalmers and Fiona Leverick, 'Fair Labelling in Criminal law' (2008) 71(2) *Modern Law Review* 217.

[6] See discussion in Chapter 1, 12-15.

brief doctrinal introduction to the approach taken by the courts, this chapter is concerned with considering the definitional framing and application of the section 1 offence to new forms of computing technologies. In doing so, the chapter unpacks some of the implicit assumptions in the structure of the section 1 offence, particularly in light of the claim that the CMA's offences are drafted in a suitably 'technology neutral' form. While 'computer' was left undefined and an inchoate form of 'access' was adopted in response to the pacing problem and concerns of ensuring technological neutrality with respect to the Collingridge dilemma, the practical effect has been a dramatic consequential, and mostly unintentional, increase in the scope of conduct that falls within the ambit of the section 1 offence. This is well beyond that risk of over-inclusiveness initially considered possible by the Law Commission when they expressed concern, as explored in Chapters 2 and 3.

II COMPUTERS: DEFINING THE BOUNDARIES

The CMA leaves the term 'computer' undefined. This approach was adopted both in accordance with the Law Commission's recommendation and, particularly, as part of an effort to make the CMA 'technology neutral'. Here, technological-neutrality refers to the adoption of broad and general terms in an attempt to prevent an offence from becoming 'obsolete' as technologies evolve.[7] Indeed, it is the breadth and flexibility of the term 'computer' that had been pointed to as a critical strength of the drafting of the CMA's offences:

> It is also comforting to know that the lack of definition under the Act means that future developments in computer technologies can easily be covered under the Act as indeed could offences committed against an ancient mechanical computer.[8]

However, an uncritical acceptance of the benefit of apparent technological-neutrality can obscure the true scope of conduct encompassed by the offence. Further, in general, the adoption of broad, technology-neutral terms can have unintended effects. As Bently observed in the context of copyright provisions with respect to reproduction, 'the drive for 'technologically neutral' laws … comes equally with the danger of bringing

[7] Douglas Hancock, 'To What Extent Should Computer Related Crimes Be the Subject of Specific Legislative Attention' (2001) 12 *Albany Law Journal of Science and Technology* 97, 99.

[8] Malcolm Highfield, 'The Computer Misuse Act 1990: Understanding and Applying the Law' (2000) 5(2) *Information Security Technical Report* 51, 53.

perfectly acceptable social practices into the realm of law.'[9] This is particularly the case with the CMA's section 1 offence in its reliance on the term 'computer' without any statutory guidance. By leaving computer undefined, that is, left to its ordinary meaning, the courts appear to have defined it as 'a device for storing, processing and retrieving information'.[10]

A *A Definition Left to the Common Law*

The Law Commission Working Paper defined a computer, for the purpose only of the discussion in the paper itself, as a 'device for processing and storing data'.[11] The computer, in processing data, could 'sort that data and extract information from it which otherwise would not be apparent'.[12] Regardless of its size or purpose, a computer consisted of 'three main elements: hardware, system software and application software'.[13] This was true of the 'largest "mainframe", through the minicomputer and down to the basic microcomputer (or personal computer) and now the portable "lap-top" computer'.[14] The Commission was of the view that a computer was 'easy to recognise, but very difficult to define',[15] so when it came to consider how 'computer' should be defined for the purpose of the proposed offences, the Law Commission relied on their public consultation to canvas views on three possible approaches: to provide a comprehensive definition, to define by partial exclusion, or to leave the term undefined.[16]

---

[9] Lionel Bently, 'Copyright and the Victorian Internet: Telegraphic Property Laws in Colonial Australia' (2004) 38 *Loyola of Los Angeles Law Review* 71, 176.

[10] *DPP v McKeown*, *DPP v Jones* [1997] 2 Cr App R 155, at 163 per Lord Hoffman in the context of admissibility of evidence.

[11] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [1.13].

[12] Ibid.

[13] Ibid [1.14].

[14] Ibid [1.15].

[15] Ibid [6.23].

[16] Ibid.

1 *Deciding not to define*

In respect of possibly providing a comprehensive definition, reference was made to the *Computer Fraud and Abuse Act* ('CFAA') in the United States. The CFAA, at §1030(e)(1), defined a computer as:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand calculator, or other similar device.[17]

The Law Commission was of the view that an attempt at this style of approach would result in a complex and unruly definition likely to confuse those involved in prosecutions.[18] Public consultation echoed these concerns. Such an attempt at a definition would run the risk of being both over-inclusive in the sense of applying to a wide variety of existing technologies, and under-inclusive in that the definition may constrain coverage of future technological developments.

Beyond the views of the Law Commission, the definition in the CFAA has elsewhere since been criticised based on its perceived over-inclusiveness.[19] However, as Clough observes, the fact the definition includes categories of devices excluded from the definition indicates that '[t]he dangers of an over-broad definition were clearly recognised in the drafting'.[20] He goes on to note, however, that the drafting of the exclusions effectively 'dates' the provision in that the use of technology-specific categories of

---

[17] Computer Fraud and Abuse Act 18 USC §1030(e)(1).

[18] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.39].

[19] See, eg, Orin S Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act' (2009-10) 94 *Minnesota Law Review* 1561; Reid Skibell, 'Cybercrimes & Misdemeanours: A Re-evaluation of the Computer Fraud and Abuse Act' (2003) 18(3) *Berkeley Technology Law Journal* 909; and Sarah A Constant, 'The Computer Fraud and Abuse Act: A Prosecutor's Dream and a Hacker's Worst Nightmare – The Case Against Aaron Swartz and the Need to Reform the CFAA' (2013) 16 *Tulane Journal of Technology and Intellectual Property* 231.

[20] Jonathan Clough, *Principles of Cybercrime* (2nd ed, Cambridge University Press, 2015) 65.

exclusions (typewriters and calculators) may need to be revisited to ensure they remain current.[21]

The Law Commission did consider, however, that it might be advantageous to adopt this aspect of the CFAA approach; by excluding particular technologies. This alternative approach would not define computer *per se* but rather provide a list of devices or technologies that ought not to be considered computers for the purpose of the offences: that is the *tertium quid* of definition by partial exclusion. In their Final Report, it was noted that the submissions received during the public consultation did not express 'much enthusiasm' for that approach.[22] As such, the Law Commission recommended that 'computer' ought to have its ordinary meaning, concluding that 'we cannot think that there will ever be serious grounds for arguments based on the ordinary meaning of the term 'computer'.[23] Leaving 'computer' undefined had also been the approach adopted in the *Police and Criminal Evidence Act 1984* s 69 which made provision in relation to evidence derived from statements produced by a computer without defining what qualified as a computer. This approach was favourably referred to by the Law Commission.[24]

During the passage of the *Computer Misuse Bill 1990* ('the Bill') through the House of Commons, as briefly explored in Chapter 3, one of the few MPs to raise concerns with the proposed offences was Mr Cohen, then Member for Leyton. In particular, Mr Cohen actively disagreed with the lack of inclusion of a definition of 'computer' in the Bill, arguing during the Second Reading debate that:

> [b]y omitting the definition, the Bill will not only apply to mainframe and personal computers and other computer technology, but will extend to a range of consumer electronics that currently have, or will have, programmable or computer-type functions. I am sure that the sponsor did not think that that was the case, but it could happen. In years to come, the Bill could apply to a washing machine, controlled by a chip, electronic car locks or programmable compact disc players, light switches, pocket calculators and

[21] Ibid.

[22] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.39].

[23] Ibid.

[24] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [6.23].

> watches. That is nonsense. Let us suppose that an Hon. Member finds an electronic personal organiser in the street and presses a button to find out whose it is so that he or she can hand it back. He or she would fiddle with the on-off switch, and, under clause 1 of the Bill, could be imprisoned for six months.[25]

At the Standing Committee Stage, where Mr Cohen attempted to have a definition inserted into the Bill to restrict its scope, his example of electric car locks was embraced as evidence for why 'computer' should be undefined, with another MP arguing:

> This is a computer misuse Bill. It seeks to tackle unauthorised access to computers which may well include electronic locks … Someone breaking into a car using an electronic key to operate the lock may not be caught under the present legislation if a policeman puts his hand on his shoulder before he gets in and tries to drive away. We are attempting to make it an offence for people to gain unauthorised access to an electronic system. The clause is properly drafted.[26]

Despite being unsuccessful, Mr Cohen again attempted to move amendments during debate on 4 May 1990 when the Bill returned to the House of Commons that would serve to limit the potential over-inclusiveness he perceived as being possible if 'computer' remained undefined. The proposed amendments at this stage would not attempt to define computer, but rather exclude computers that operated in particular settings from the scope of the section 1 offence. Mr Cohen's amendment would thus have provided in the section 1 offence that:

> (4) No offence under this section is committed by any person if the computer that performs the function is the computer to which access is secured or intended to be secured, and
> (d) the computer controls equipment used only for personal, domestic or recreational purposes, or
> (e) the computer has been lost and the access in question is secured, or intended to be secured, in order to establish ownership of the computer, or
> (f) the place where the computer is located can be used by unauthorised persons, and the access in question is secured at a time when the place is authorised for use by unauthorised persons.

Sub-section (4)(a) was intended to remove the potential for the offence to apply with respect to conduct involving personal equipment that may be operated or controlled by

---

[25] HC Deb 9 February 1990, vol 166, col 1168.

[26] HC Official Report, SC C (Computer Misuse Bill), col 9, 14 March 1990, as cited in Ian Lloyd, *Information Technology Law* (7th ed, Oxford University Press, 2014) 204.

a microprocessor. In explaining this, Mr Cohen referenced an opinion piece by barrister Alistair Kelman published on 21 February 1990 in *Connexion* that observed:

> The Bill may throw up some unlikely hackers if it survives unamended. These could include those who fax other people's letters to third parties without the author's permission and neighbours who use washing machines and microprocessors without prior consent.[27]

Debate on this proposed amendment was swift, with Mr Colvin, then Member for Romsey and Waterside, arguing that the exclusions were drafted too broadly such that computers with 'dual-use' would thus fall outside the scope of the offence, as would 'the radar and navigation equipment of a small [private] aeroplane. Unauthorised access to that equipment could be extremely serious'.[28]

Sub-section (4)(b) sought to exclude circumstances where an individual accesses a lost device in order to ascertain ownership from the ambit of the offence. Mr Colvin argued that this would be unnecessary arguing that any such individual could reasonably assume that legitimate owner would want the device back and thus they could access it for those purposes without evidence of a clear instruction to the contrary.[29]

Sub-section (4)(c) received limited verbal argument in support of it by Mr Cohen, who focused more of his time on a second proposed amendment to introduce a public interest defence which, along with this amendment, was subsequently withdrawn. But the intent of the exclusion seems to echo arguments he had raised during the second reading of the Bill:

> The argument behind the Bill and the Law Commission's report is that we need special crimes concerning access to computers because computers are special and unauthorised access can cause damage. If computers are special, the owners of them should have special responsibilities. We have legislated to the effect that the owners of guns have to keep them

[27] HC Deb 4 May 1990, vol 171, col 1330.

[28] HC Deb 4 May 1990, vol 171, col 1332.

[29] HC Deb 4 May 1990, vol 171, col 1332.

> in lockable, custom-built storage cupboards, yet computer misuse can also cause death and there is no duty on computer owners to maintain security.[30]

This exclusion would thus appear to be creating an incentive for computer owners to have taken active steps to physically secure their computers before the section 1 offence could apply. In that sense, the effect of the amendment would have been to implicitly require a physical trespass be proved in order to establish the section 1 offence applied, but without that requirement being a part of the substantive offence. While well-intended, the clumsy drafting of this exclusion would have rendered the section 1 and section 2 offences inapplicable in almost all circumstances. Mr Colvin focused on the example of a dishonest employee or a cleaner who, having authority to be in the room containing a computer, would thus not be within scope.[31]

While a sensible objection, it appears not to have been further noted that the exclusion related to the circumstances of the positioning of the computer, not the person accessing it. So the applicability of the offence to an individual who gained access to a computer remotely would depend on whether or not the computer itself was physically secured from any potential access by unauthorised persons, irrespective of the characteristics of the accused themselves.

Mr Cohen withdrew his amendments. As such 'computer' was indeed ultimately left undefined, and no limitations on conduct potentially fulfilling the *actus reus* elements of the offence were incorporated.

(a) The approach of the Courts

As noted above, the Law Commission's view was it would be unlikely 'that there [would] ever be serious grounds for arguments based on the ordinary meaning of the term 'computer'.[32] In the context of prosecutions under the CMA, this appears, as yet, to be broadly correct in practice. The opportunity for argument as to whether or not a

---

[30] HC Deb 9 February 1990, vol 166, col 1170

[31] HC Deb 4 May 1990, vol 171, col 1332.

[32] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.39]

particular device is a computer had instead arisen in the context of the *Police and Criminal Evidence Act 1984* ('PCEA') and the admissibility of statements produced by a computer as evidence at a time when such admissibility was determined in accordance with section 69 which provided:

> (1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown -
> (a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
> (b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.

The effect of this provision was that, contrary to what would have been a general proposition that the defendant may challenge the accuracy and reliability of computer-produced evidence, the prosecution would first bear the onus to establish that the computer was operating properly. This is exceedingly difficult given the complexity of software and the potential impossibility of replicating the precise combination of hardware, software and user input that produced the statement relied upon.[33]

The PCEA provided no definition of 'computer'. While, at the time, this approach was relied upon favourably by the Law Commission in recommending that 'computer' ought also to be undefined for the purposes of the CMA, the House of Lords would later be presented with two cases that began the process of considering the scope of what might be considered a computer for the purposes of section 69. The two cases *DPP v McKeown and DPP v Jones*, ('*McKeown and Jones*')[34] decided together, concerned the proper operation of a Lion Intoximeter 3000 (a 'breathalyser') used by Cheshire Police to measure the presence of alcohol in the breath of vehicle drivers. The device in question had produced results in both cases that indicated the drivers had consumed alcohol above the legal limit. However, the device exhibited a fault in its internal clock, displaying an incorrect time: a

[33] See, Lloyd (n 26) 250; and, for challenges arises with respect to the accuracy of software beyond the criminal law, see *St Albans District Council v ICL* [1996] 4 All ER 481 and Elizabeth Macdonald, 'The Council, the Computer and the Unfair Contract Terms Act 1977' (1995) 58 *Modern Law Review* 585, 591.

[34] *DPP v McKeown*, *DPP v Jones* [1997] 1 WLR 295.

drift of 13 minutes. While both Ms McKeown and Mr Jones were convicted at first instance, their convictions were overturned on appeal to the Divisional Court.

In the case of Ms McKeown, she was initially prosecuted pursuant to section 5(1) of the *Road Traffic Act 1988* for driving a motor vehicle above the proscribed limit (twice producing a test result of 78 micrograms per 100 millilitres of breath: the legal limit is 35). She challenged the admissibility of the test results as evidence for her conviction on the basis of the time error, arguing that as a computer, the breathalyser was not operating properly pursuant to PCEA s 69(1)(b) and the results were thus inadmissible as evidence.

In the case of Mr Jones, he was prosecuted pursuant to section 7(6) of the *Road Traffic Act 1988* for failing to provide, without reasonable excuse, a specimen of breath when required to do so. A week after Ms McKeown's positive test, Mr Jones had driven his car into a roundabout and appeared visibly intoxicated. He was taken to Widnes Police Station to be tested on the same breathalyser. His first test registered 148 micrograms, four times the legal limit. He was then alleged to have refused to properly provide a second breath sample, with the test aborting. It was later argued on his behalf that he could not lawfully be required to provide a breath sample for a breathalyser with an inaccurate clock, and further that the only available evidence that his second breath sample was not sufficient was the computer reading from the faulty breathalyser and, per PCEA s 69(1)(b), that evidence ought to be inadmissible.

In both cases, the issue before the House of Lords was whether the breathalyser was a computer for the purpose of PCEA s 69, and thus whether the inaccuracy of the time recorded in the produced results of the various tests was such that they satisfied the requirements of s 69(1) to render the results inadmissible. In respect of whether the breathalyser was a 'computer', Lord Hoffman began by making the following observation:

> The Lion Intoximeter 3000 … consists of an analyser which measures the alcohol content of the breath by means of an electronic signal, a computer which converts the signal into

> digital form with a visual display on which the result of the test is shown and a printer on which it can be printed out[35]

Here, Lord Hoffman can be observed drawing distinctions between the different 'parts' of the breathalyser. These distinctions were possible because of the design of the device. The Lion Intoximeter 3000 is a large desktop breathalyser device. From outward appearances, its design appears to present as two separate components: on the right, a concealed area containing the equipment to analyse the breath sample with a hose attached, and on the left a typical 'terminal' with keyboard and a digital display screen. A separate printer could then be attached to the device to produce a paper output of the results of the test that had been displayed on the screen. Lord Hoffman thus approached the question of whether or not the device was a computer on the basis of the terminal component of the breathalyser:

> A computer is a device for storing, processing and retrieving information. It receives information from, for example, signals down a telephone line, strokes on a keyboard or (in this case) a device for chemical analysis of gas, and it stores and processes that information.[36]

As a device that received the 'electrical signal' from the analyser, processed and converted it to a test result viewable from the digital display, the terminal was indeed a computer for the purposes of section 69. But the testing component and printer were regarded as separate from 'the computer'. Having so determined, Lord Hoffman turned to the question of the proper functioning of the computer:

> section 69 is not in the least concerned with the accuracy of the information supplied to the computer. If the gas analyser of the Intoximeter is not functioning properly and gives an inaccurate signal which the computer faithfully reproduces, section 69 does not affect the admissibility of the statement … [a]ll that section 69 requires … is positive evidence

---

[35] Ibid 298.

[36] Ibid 302, per Lord Hoffman. While no reference was made to it, the Oxford English Diction defines a 'computer' as:

> An electronic device (or system of devices) which is used to store, manipulate, and communicate information, perform complex calculations, or control or regulate other devices or machines, and is capable of receiving information (data) and of processing it in accordance with variable procedural instructions (programs or software); esp. a small, self-contained one for individual use in the home or workplace, used esp. for handling text, images, music, and video, accessing and using the internet, communicating with other people (e.g. by means of email), and playing games.

> that the computer has properly processed, stored and reproduced whatever information it received.[37]

Evidence had been provided by Sergeant O'Dell, who had facilitated the tests, that while the time on the breathalyser was incorrect, the analyser had been properly calibrated. A further statement from Dr Paul Williams, a director of the company who manufactured the breathalyser, indicated that 'the alcohol analytical system and breath sampling system were separate from the circuitry which controlled the accuracy of the clock.'[38] One could not impact that other. In accepting this position, and on the assumption the clock was part of the computer, Lord Hoffman determined that the malfunction with respect to the time displayed on the test results was not a relevant consideration for the purposes of s 69(1)(b). They were admissible, and thus the original convictions were safe.

The effect of this decision and approach was to interpret s 69 such that only a malfunction which affected the manner in which the computer processed, stored or retrieved the information used to generate the statement tendered in evidence, and not the document as a whole, was a relevant malfunction. This eschewed a literal approach for one seemingly more pragmatic. It did, however, rely on a conception of a computer as being separate from its constituent parts. Indeed, Lord Hoffman would observe in *obiter*:

> if the error lay in the clock mechanism itself, I doubt whether it would constitute part of "the computer" for the purposes of section 69(1). The section, as I have said, is concerned with the processing and storage of information and not with the accuracy of the information supplied. The clock, although no doubt physically in the same box as the computer, is something which supplies information to the computer rather than being part of the processing mechanism.[39]

Despite providing the general definition for a 'computer' as being a 'device for storing, processing and retrieving information', Lord Hoffman appears to have had a more limited view in mind. Indeed, that limited view was adopted in the latter appeal in

---

[37] Ibid.

[38] Ibid 300.

[39] Ibid 303.

Reid v DPP ('*Reid*'),[40] where a similar issue arose with respect to section 69 but this time in relation to the quality of the printout of the results from a breathalyser. All three printouts that were produced exhibited 'abnormalities': the second half of the first character in each line was omitted, and one of the printouts had the top line printed out in a font size smaller than the rest of the document. The information in the printouts, however, accurately reflected the results displayed on the digital screen at the time of the tests. Adopting the approach in *McKeown and Jones*, the printer was treated as not being a part of the 'computer' and thus it was decided that the Crown Court at first instance was entitled to conclude that the printing issues were 'unconnected to the operation of the computer part of the intoximeter'.[41]

(i) 'processing' data as the key delimiter?

While Lord Hoffman's approach in *McKeown and Jones* has been described as a 'common-sense' interpretation of the operation of section 69,[42] the same might not necessarily be said for the definition of computer itself. This approach seemingly requires treating each component of a device separately and assessing as to whether it performs all three of the underlying functions: storing, processing, and retrieving. Omerod and Laird set out two alternative approaches to defining a computer, the first adopting the elements of Lord Hoffman's articulation (although seemingly without reliance on *McKeown and Jones*), and the second providing a broader interpretation, but without comment.[43]

The first approach centres on the abilities of the device. To be considered a computer, and adopting the framing of Lord Hoffman, the device must be able: '(i) to store information; (ii) to retrieve the information so stored; and perhaps most importantly

[40] [1999] RTR 357.

[41] Ibid [8A] and followed in *DPP v Barber* (1999) 163 JP 457.

[42] See, eg, Katie Quinn, 'Computer Evidence in Criminal Proceedings: Farewell to the ill-fated s 69 of the Police and Criminal Evidence Act 1984' (2001) 5(3) *International Journal of Evidence and Proof* 174.

[43] David Omerod and Karl Laird, *Smith and Hogan's Criminal Law* (14th ed, Oxford University Press, 2015) 1182-3.

(iii) to process that information'.[44] The decision in *Reid* with respect to the malfunctioning printer might then be understood on the basis that while the printer received and processed the instructions from the computer terminal of the breathalyser, thus performing the function of producing a printed copy of the results, it neither stored any data nor was it able to retrieve that data. This framing provides a clear separation between devices used to manually make calculations (an abacus or slide-rule) as against devices that store and process data independently.[45]

Without expressly making the link, Omerod and Laird offer a further restriction on what should qualify as 'processing'. They suggest that processing needs to go beyond merely commencing a pre-programmed function based upon a non-, or minimally-, variable signal input, like a washing machine.[46] Such a device would merely be obeying instructions rather than *processing* them. Traffic management systems are employed as an additional example to explore further their proposed distinction; '[a] machine which merely ensures that traffic lights will show red or green at stated intervals is not a computer; a machine which varies the intervals in response to information about traffic density is'.[47]

This becomes a difficult interpretation to accept in attempting to rationalise the decisions discussed above. Indeed, such a construction of processing ought to have meant that the Lion Intoximeter 3000 in both *McKeown and Jones* and in *Reid* was not a computer at all. There, the terminal receives a signal from the breath analyser indicating the composition of the gasses analysed, the terminal then merely matches that result as against pre-programmed reference levels to calculate a result. It merely 'obeyed the instruction' it was given by the breath analyser component. It did not automatically respond to variances in the people taking the test – indeed it required a set level of breath in order to process results irrespective of the lung capacity and general health of the individual (the basis, albeit not believable given the circumstances, of Mr Jones' defence

[44] Ibid 1182.

[45] Ibid.

[46] Ibid.

[47] Ibid.

in respect of his prosecution for failing to provide an adequate second breath sample). In that sense, the breathalyser seems to be more in line with Omerod and Laird's washing machine than their advanced traffic management system.

This is not to say that complexity in the tasks performed by a device might not be a relevant consideration in defining what is and is not a computer. But any such focus on complexity will inevitably rest on the specificity of the conceptual abstraction developed to explain the function of the device. Taken together, the underlying approach of Lord Hoffman along with a further consideration of the degree of processing would necessitate, in any given circumstance, breaking the device down to its component parts to identify the part that *might* qualify as a computer, and then further make an assessment as to the tasks that part is in fact performing. This is an approach that would carry substantial risk as computing technologies evolve; the line becomes increasingly difficult to draw as those technologies are incorporated into all manner of consumer and industrial products, and the *degree* to which those technologies are incorporated into the component parts of those products continues to become ever more integrated.

A potential difficulty in considering a computer as effectively not being the sum of its component parts, at least for the purposes of the CMA, comes in the form of the additional interpretative guidance in respect to the treatment of a 'removable storage medium'. Sub-section 17(6) of the CMA provides:

> (6) Reference to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer, and a computer is to be regarded as containing any program or data held in such medium.[48]

As the use of the term 'removable storage medium' is not defined, it would thus be interpreted with reference to its ordinary meaning which would be along the lines of a computer storage device designed to be inserted and removed from a system. This sub-section was intended to cover data stored on floppy disks, magnetic tape and hard drives, but also applies to optical discs (eg. CDs and Blu-ray discs), memory cards, or any other

[48] *Computer Misuse Act 1990* s 17(6).

external device that contains data storage capabilities (digital cameras, phones etc,). Many of these mediums store data in such a way that it cannot be accessed without the use of a computer (save digital cameras and phones). The effect of sub-section 17(6) is that each of these is deemed to constitute part of a computer when so attached or inserted. While it might suitably be argued here that the inclusion of a removable storage medium as capable of being deemed part of a computer operates as a specific exception to the general proposition, it does highlight a weakness in approaching the 'computer' as the component that *processes* the data to the exclusion of other components that provide the data that enables that processing.

The second, or alternative, proposed approach to interpreting 'processing' offered by Omerod and Laird is substantially broader; '[a] computer may be thought of as any machine which responds to signals (now usually electronic) to perform programmed functions'.[49] Here, processing is defined on the basis of the mere initiation of a response to a given input. That is, this approach removes the question of the complexity of the processing activity engaged in by the device, and instead focuses on the existence of a capacity for the device to detect and respond to an instruction that results in the initiation of a software-defined task.

The breadth of this approach cannot be overstated. Here, to use Omerod and Laird's example, a washing machine would qualify as a computer in and of itself, so too would any other digital device. Under this construction, the unauthorised use of another's washing machine would thus fall within the bounds of the CMA section 1 offence. If this were indeed the case, then the section 1 offence would have the potential to operate with a substantial degree of overlap with many other non-computer specific criminal offences. Omerod and Laird briefly imply that such overlap would be dealt with by prosecutorial discretion: in such circumstances, the appropriate offence to charge would be one which reflected a fairer label of the criminal conduct.[50] In the case of the washing machine, they propose a more suitable prosecution would be one based on the offence of the dishonest abstraction of electricity under section 13 of the *Theft Act 1968*. The same would apply,

[49] Omerod and Laird (n 43) 1182.

[50] Ibid 1183.

they suggest, to a dishwasher or microwave oven.[51] To support this, they argue that these examples of devices are not sold as computers, nor are they under a general understanding considered to be computers.

However, this purported limitation on the basis of prosecutorial discretion and common sense is inadequate. The question is not whether something is *generally* considered to be a computer, but whether a particular device is a computer *for the purpose of* the CMA. The term 'computer' necessarily needs to be defined such that the scope of the offence can be properly understood. The fact that another general offence could apply in a given fact scenario, regardless of the purported appropriateness of that other offence, provides limited if any guidance as to the proper construction of the CMA section 1 offence itself. While Omerod and Laird are correct that a charge for abstraction of electricity is the more appropriate charge, that this is the case is not sufficient. The definition of 'computer' ought not to be construed in a process that might be described as a *post hoc* construction centred on a need to 'fill a gap'. To be properly understood, the offence requires a clear definition in its own right, irrespective of the existence of other offences that may be better suited.

At this point, it appears neither approach in the abstract is particularly satisfying. The first approach, with a focus on the complexity of the 'processing' being undertaken, becomes overly technical and specific to the point of being potentially too subjective and speculative. This produces unnecessary complications in identifying whether a device is a computer and thus provides considerable scope for differing opinions based upon minimal technical differences in the devices themselves. The second approach eschews that complexity in favour of an approach that is overinclusive to the point of absurdity.

In terms of the admissibility of computer evidence with respect to the PCEA s 69, a sensible approach to defining 'computer' was ultimately achieved with the repeal of that section in 1999.[52] Computer evidence is no longer regarded as a special category for

---

[51] Ibid.

[52] *Youth Justice and Criminal Evidence Act 1999* s 60. Indeed, one argument relied upon by the Law Commission in recommending s 69 be repealed and not replaced was that changes in computer technologies were

the substantive law of evidence, instead being subject to the general common law presumption of regularity as stated in *Castle v Cross*: '[i]n the absence of evidence to the contrary, the courts will presume that [mechanical instruments] were in order at the material time.'[53] While not resolving all the complexities,[54] the move away from treating 'computers' as a special class meant the courts no longer had to grapple with constructing a suitable definition. The same is not the case for the purposes of the CMA.

2 *'Computers' and the CMA*

While it was the Law Commission's view that it would be unlikely 'that there [would] ever be serious grounds for arguments based on the ordinary meaning of the term 'computer',[55] it has been observed above that this was ultimately not the case with the use of 'computer' in PCEA s 69 which was relied upon as an example in support of leaving 'computer' undefined for the purposes of the CMA. However, a serious challenge is yet to reach the courts in respect of a prosecution under the CMA: thus far, whether a device at issue in fact constituted a computer has not been disputed.

Perhaps sensibly, most of the prosecutions under the section 1 (and section 2) offence have centred on the use of conventional computing devices: desktop PCs, laptops, and network servers. In those cases where a different form of device has been used, there has been no challenge raised as to whether the device was a computer or not. In the case of *R v Ashford,*[56] introduced in Chapter 3, the device in question was a stolen smartphone belonging to a PR agent. Whether or not the smartphone was a computer was not challenged, although it is, of course, difficult to see how it could have been; there are perhaps no conceivable arguments that a smartphone is not a computer for the purpose of the CMA. A smartphone can satisfy the *McKeown and Jones* test as a device that is

making its application too broad and the provision too burdensome on prosecutions: too many pieces of evidence were becoming capable of being regarded as computer-generated.

[53] [1984] 1 WLR 1372, 1377.

[54] See, Quinn (n 42).

[55] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.39]

[56] (Unreported, Westminster Magistrates Court, 13 August 2014).

capable of storing, processing and retrieving data on either interpretation as to the complexity of the processing involved.

A further opportunity could have presented itself in the case of *R v Kaye*[57] where the accused had made use of a modified version of the *Mirai* malware to build a network of thousands of home 'smart devices' which he used to launch a distributed denial of service ('DDoS') attack against a Liberian telecommunications company. The accused pleaded guilty to one count of an offence contrary to CMA section 3, one count of an offence contrary to CMA section 3A and one count of an offence for possessing criminal property. The section 3 charge was in respect of the DDoS itself, and the section 3A was in respect of creating and possessing the malware. What was not factored in was the act of causing the malware to be installed in the many thousands of household devices. Each instance could conceivably constitute either the section 1 offence, but also the section 2 offence where the intent for installing the malware was to enable the commission of the section 3 offence (the DDoS attack).

There is clearly a resourcing issue here: it would be practically impossible to identify the status of each device sufficient that a section 1 or 2 offence could be prosecuted. Instead, that conduct became a consideration for sentencing: with the accused receiving a 32-month custodial sentence for the section 3 offence, a 12-month custodial sentence for the section 3A offence, and a 12-month custodial sentence for possessing criminal property, to be served concurrently. But, the fundamental question of whether any or all of those 'smart devices' that were infected with malware were 'computers' for the purpose of the CMA was avoided by not pursuing charges at that level.[58] While this might have been appropriate given the practical limitations in the circumstances, such cases continue to lend support to the status quo position that the reliance on the term computer without definition within the CMA remains sustainable.

---

[57] (Unreported, Blackfriars Crown Court, 11 January 2019).

[58] Similar conduct has been prosecuted in the United States in respect to the use of *Mirai* style malware, but there it was for fraud offences and for conspiracy to contravene the Computer Fraud and Abuse Act. See, Brian Krebs, *Mirai IoT Botnet Co-Authors Plead Guilty* (17 December 17) Krebs on Security <https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/>.

Indeed, subsequent reviews of the CMA, including the 2004 report by the All-Party Internet Group (the 'APIG'),[59] have also emphasised the utility of leaving 'computer' undefined. But, careful attention needs to be placed on the framing of the questions that have led to that conclusion. The APIG, for instance, framed their consideration on the basis of whether the lack of definition had 'been a problem'.[60] The Home Office is described to have reported they had '"never come across a case" where the courts had failed to use a "broad definition"'.[61] Peter Sommer, who made a successful career as an expert witness in computer-related prosecutions, also advised that 'he was "not aware that [the lack of definition] has caused any difficulties"'.[62] The focus, then, has been on assessing the definition on the basis of whether any challenges have arisen for *prosecuting* conduct: that is, has the lack of definition caused any prosecutions to fail. Again, this is a different question to as to whether the undefined use of 'computer' sufficiently communicates to the public the scope of the offence.

However, this status quo position, of computer remaining undefined, may not continue to hold. To understand why requires a consideration of the development of computing technologies since the implementation of the CMA. Particular attention needs to be placed on the continuing incorporation of computing technologies into an ever-increasing array of devices, and the changing nature of how these devices operate and are interacted with. That is, the status of the devices that make the large-scale cyber-attacks like those in *R v Kaye* above possible.

As it currently stands, there is a serious possibility that the lack of a clear definition of what qualifies as a 'computer' for the purpose of the CMA results in an offence that might resemble what Edwards termed an empowering offence. That is, the section 1 offence provides an increased ability for arrest for conduct involving the use of a 'computer' well beyond the original framing of conduct impacting the integrity of a

---

[59] See, All-Party Internet Group, *Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group*, 2004, London, HMSO. <https://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf>.

[60] Ibid 4.

[61] Ibid.

[62] Ibid.

computer as a private store of data. The true scope of the section 1 offence's potential application remains unknown. The offence casts a wide net, with the confines of what is and is not criminal with respect to 'computers' seemingly being delegated to police and prosecutors. The exercise of discretion, the impact of resource allocation, and internal policies provide the limitation for what is and is not criminal.[63]

This claim, however, cannot be supported if there exist other mechanisms in the drafting of the offence that may serve to provide a limitation to the scope of the offence, or at least contribute to providing some form of clearer definition. With respect to the section 1 offence, such limitation may come in the form of leveraging the reliance on the concept of 'access'. The issue then, however, becomes not one of a lack of definition for the term 'access' as exists for the term 'computer', but instead of the provision of a wide definition that represents a mismatch between the conception of technology that informed the framing of the definition of 'access' with the evolving nature and use of computing technologies.

III 'ACCESS' AND THE EVOLVING NATURE OF COMPUTING TECHNOLOGIES

It could be argued that the definition of 'computer' for the purposes of the CMA ought to be constrained by being interpreted in light of the need for the accused to 'intend to secure access'. Putting aside the *mens rea* aspect of this potential limitation, the notion of securing access might otherwise serve to delimit the boundaries of the types of devices that fall within the scope of the section 1 (and section 2) offence. On this reading, computers must necessarily be devices for which 'access' can in fact be secured. Where there is no capacity for 'access' to occur, the device might thus not be a computer for the purposes of the offence, irrespective of whether the device stores, processes, or retrieves data.

[63] See, eg, William J Stuntz, 'The Pathological Politics of Criminal Law' (2001) 100(3) *Michigan Law Review* 505; Celesta A Albonetti, 'Prosecutorial Discretion: The Effects of Uncertainty' (1987) 21(2) *Law & Society Review* 291; Robert L Milsner, 'Recasting Prosecutorial Discretion' (1996) 86(3) *Journal of Criminal Law and Criminology* 717; William F Baxter, 'Separation of Powers, Prosecutorial Discretion, and the "Common Law" Nature of Antitrust Law' (1981-2) 60 *Texas Law Review* 661.

But for the term 'access' to provide any form of interpretative limitation, it must itself be clearly defined. However, as introduced in Chapter 3, the CMA exhibits a distinct lack of clarity as to how 'access' should be interpreted. [64] This lack of clarity has resulted in the broader commentary of the CMA's section 1 and 2 offences to often be beset by consistent conceptual conflation and, particularly in the case of early prosecutions, confusion.[65]

A *The Conceptual Framing of the 'Access' Offence*

As has been observed previously, the work of the Law Commission and later commentary surrounding the CMA has centred on the issue of 'hacking' and the risks that activity represented to the *integrity* of 'computers' and 'computer systems'. In its essence, therefore, the CMA was structured to criminalise behaviour that might otherwise be said to constitute *digital trespass*. This is evident from the structure of the section 1 offence, drawing heavily on analogy to the tort of trespass to goods: the section 1 offence requires direct and intentional conduct (involving the use of a computer) where that conduct is unauthorised and represents a form of 'access' to (or interference with) the computer or data held within it.

Trespass to goods involves the direct, intentional,[66] and unauthorised interference with another's personal property.[67] Interference can involve minor acts such as touching the property that causes no harm,[68] to acts that result in some form of damage to the property.[69] Where the interference with the property amounts to permanent or

---

[64] See, Chapter 3, pages 101-4.

[65] See, eg *DPP v Bignell* (1998) 1 Cr App R 1.

[66] Unintentional interference is potentially actionable in negligence, see, eg, *National Coal Board v J E Evans & Co (Cardiff) Ltd* [1951] 2 KB 861.

[67] Non-physical interference is not sufficient, see *Hartley v Moxham* (1842) 3 QB 701.

[68] See, eg, *Arthur v Anker* [1997] QB 564 and *Vine v Waltham Forrest London Borough Council* [2000] 4 All ER 169; *Kirk v Gregory* (1876) 1 Ex D 55 involving the movement of jewellery from one room to another; *Wilson v Lombank Ltd* [1963] 1 All ER 740 where a representative of the defendant mistakenly seized the claimant's car while it had been left with them for repairs.

[69] See, eg, *Ellis v Loftus Iron Co* (1874) LR 10 CP 10, where the defendant's horse bit and kicked the plaintiff's mare through their shared boundary fence.

temporary physical harm or destruction, or permanent or temporary impairment of the property's use or value,[70] the offence of criminal damage may apply.[71]

This conceptual similarity between the tort of trespass to goods and the section 1 offence is important. While not explicitly referred to when proposing the structure of the offence, the tort of trespass played an important role in the formulation of the Law Commission's recommendations. In the Working Paper, an analogy to the tort of trespass was suggested to form the basis of an argument as to why mere unauthorised access ought not to be considered criminal in the absence of some further aggravating factor.[72] The delimitation between conduct being treated as tortious versus warranting a criminal response, therefore, comes down to an assessment of the degree and result of a given *interference*. The criminal law in these circumstances ostensibly concerns itself with the more serious forms of damage, rather than interferences that might better be regarded as a nuisance or hassle.[73]

In the Law Commission's view, however, it was the very nature of the operation of computers themselves that constituted the necessary 'aggravating factor' that would justify all forms of 'hacking' being criminalised. Rather than adopt a model that would restrict or give shape to a particular conception of hacking or a particular form of harm, the risk to the 'integrity' of a computer or computer system became the focus:

> "The importance of the integrity and proper functioning of operational computer systems is, we think, obvious, and the need for total confidence in that integrity leads to great expense and inconvenience if such systems are penetrated, even if later investigations show that no actual impairment of the system has been achieved. Because even attempts to gain

[70] *Morphitis v Salmon* [1990] Crim LR 48; *R v Whiteley* (1991) 93 Cr App Rep 25. Damage, in the sense of impairment of use or value, seems to require some form of impact on the integrity of the property rather than mere deprivation of use; see, *Lloyd v DPP* [1992] 1 All ER 982; *Drake v DPP* [1994] Crim LR 855.

[71] *Criminal Damage Act 1971* s 1.

[72] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988), [6.15].

[73] Albeit in practice the courts have adopted a wide interpretation of what conduct can amount to criminal damage: the trampling of grass as in *Gayford v Chouler* [1898] 1 QB 316; graffiti smeared in mud despite being easily washed as in *Roe v Kingerlee* [1986] Crim LR 735; adding water to milk as in *Roper v Knott* [1898] 1 QB 868); and land may be damaged by placing substantial amounts of waste upon it as in *R v Henderson, R v Battley* (Unreported, Court of Appeal Criminal Division, 29 November 1984).

> unauthorised access to such systems have those possible consequences, there seem to us to be the strongest reasons for using the criminal law to express disapproval of such conduct.[74]

'Access', in its practical sense and with an emphasis on computer integrity, would be conceived with reference to the uses of computing technology as it existed at the time: that is, largely focused on the emergence of home computers and laptops that enabled outsiders to become capable of gaining access to large, commercial, valuable, and self-contained computing systems. The democratisation of computing and the emergence of networking technologies had resulted in 'access' to computers being obtainable without requiring *physical* access to the computer. These factors influenced the conclusion that 'access' to computers warranted the attention of the criminal law in a form that arguably departed from the traditional tort/crime delineation with respect to the trespass to goods model. The rise of computing and lack of physical interference in most instances of hacking contributed to the recommendation to criminalise.

But 'access' itself is a concept broader than *interference* or *damage*. This was considered by the Law Commission in their Final Report where they concluded that the potential breadth of the term 'access' could be sufficiently limited by not requiring it in the substance of the *actus reus* and instead requiring there be conduct that 'causes a computer to perform a function' which necessitates some form of direct interaction with the computer.[75] 'Access' would thus appropriately form the basis of the *mens rea* by being treated as the intended endpoint of a course of conduct: that is the chain of conduct leading to securing 'access'. However, the treatment of 'access' within the structure of the offence does little to define what it actually means.

At the time of the Law Commission's Final Report, the Oxford English Dictionary's definition of 'access' included an additional definition that read 'to gain access to data etc., held in a computer or computer-based system, or the system itself'.[76] This definition, ultimately relied upon to inform the Law Commission's arguments with

---

[74] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989), [2.15].

[75] Ibid [3.26].

[76] The current formulation of this definition reads 'to obtain or retrieve (data or a file); to gain access to (a system or network)'.

respect to 'access', represented the definition of access in its transitive verb form. That it is in its transitive verb form is particularly evident from the circular nature of the definition: access means *to gain access* to *data*. With the adoption of the phrase 'secure access' in the section 1 offence, and in relying on its use in its transitive verb form, the accused might then be said to be required to *intend to complete the process* of obtaining the information stored in the computer or data. Such an intention might then only be properly directed at a device where it is, in fact, possible to interact in such a way that information stored in it can become knowable to the accused: the definition of computer consequently being conceived as limited to only the kinds of devices where that form of access is possible.

However, the use of 'access' in the phrase 'with intent to secure access to any program or data' is not in its transitive verb form as discussed by the Law Commission. Instead, 'access' operates in its noun form as the direct object of the verb *secure*. Of the numerous definitions of the noun form of 'access' provided in the Oxford English Dictionary, the two most pertinent provide that access means 'the right or opportunity to benefit from or use a system or service', or specifically in relation to computing, 'the opportunity, means, or permission to gain entrance to or use a system, network, file, etc.' Thus, someone who causes a computer to perform a function with intent to secure access would be an individual who takes steps merely to place themselves in the position of being able to gain the opportunity or means to use or benefit from the use of that computer, rather than intended to have the computer complete some form of processing. To 'secure access', then, might refer merely to intending to undertake steps that result in the use or benefit of the computer or underlying data becoming *possible*.

The interpretation of access in its noun form is thus considerably wider than its use as a transitive verb. An adoption of 'access' as a noun would seriously limit any potential reading down of scope of devices capable of being considered a 'computer', even with appeals to common sense. 'Access' would be construed as including any means to use or benefit from the 'computer': to 'use and benefit from' cannot reasonably be said to provide any definitional or otherwise limiting guidance on what a computer might be. That is, it might be enough merely to establish that it is possible to use or otherwise benefit from the device, regardless of questioning what that device actually is.

These alternative interpretations are, of course, premised solely on a grammatical approach to understanding the use of the term 'access'. The CMA itself provides some interpretational guidance to the term 'access'. Unfortunately, however, that guidance is perhaps less than useful. The CMA appears to hedge its bets between the two approaches, as the definition of 'secure access' provided in section 17 operates across both conceptions: with approaches to interpreting access offered that fit both the noun and transitive verb forms of the word:

> (4) A person secures access to any program or data held in a computer if by causing a computer to perform a function he –
>
> (e) alters or erases the program or data;
>
> (f) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
>
> (g) uses it; or
>
> (h) has it output from the computer in which it is held (whether by having it displayed or in any other manner)
>
> and references to access to a program or data (and to an intent to secure such access) shall be read accordingly
>
> (5) For the purpose of subsection (2)(c) above a person uses a program if the function he causes the computer to perform –
>
> (c) causes the program to be executed; or
>
> (d) is itself a function of the program.

Therefore, 'access' can be interpreted so as to refer to *any* use or interaction that results in *any* form of response from the computer or system.

The analysis provided by the Law Commission, with their focus on the definition of access as a transitive verb, now sits somewhat uneasily with the ultimate adoption of 'access' in its broader noun form. Indeed, some of the concerns raised, and sought to be mitigated, by the Law Commission in adopting the focus on 'access' have ultimately eventuated through the departure from their recommendation in the final drafting of the section 1 offence.

The Law Commission was of the view that it should be clear that 'access' should not extend to mere 'physical access', to accessing a hard-copy of the information, or to circumstances of *computer eavesdropping*.

First, physical access. The Law Commission was concerned that the ultimate drafting of the offence should not include acts that involve coming into mere physical

contact with a computer. As an example, the Final Report suggested that 'an office cleaner entering without permission a room where there is a computer might be said to have obtained access to it.'[77] While suggesting that such conduct would never be proceeded against in practice,[78] it was thought desirable not to leave this issue to be determined by prosecutorial discretion.

The second concern was in respect to 'print-outs' of the information. The Law Commission did not want to see the criminalisation of unauthorised access to physical documents, at least arising through the operation of a 'hacking' offence.[79] The extent of their objection, however, was not clearly set out. While not explicitly provided, it perhaps can be assumed that the Law Commission was referring to instances where an authorised user prints material from a computer and an unauthorised person later obtains that physical print-out. The focus here, of course, being the content of the information, rather than the integrity of the computer.[80] The alternative reading would be that the Law Commission did not wish to see the mere printing of information stored on a computer to be criminalised, but such an interpretation sits uncomfortably with their ultimate recommendation that the *actus reus* be constructed around any act that caused a computer to perform a function: the computer must necessarily be caused to 'perform a function' if it is to produce a hard copy output via printing.

The final concern was that 'access' should not include conduct analogous to *eavesdropping:* that is, either looking at information already displayed on a computer screen by an authorised user, or the use of electronic devices to 'listen in' to electronic

---

[77] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989), [3.23].

[78] Compare this with the views expressed to support the implementation of the *Criminal Justice and Courts Act 2015* s 33 regarding the distribution of private sexual photographs and films. The offence does not take into account the age of offenders. Thus, children who send such photographs to one another are at risk of being prosecuted as sex offenders before the age of 18 (as well as potentially offences under the *Protection of Children Act 1978* s 1(1)). Despite Parliament clearly setting out that children would not be prosecuted, and the CPS guidelines requiring caution and stating that in most cases involving individuals under the age of 18 a prosecution would not be in the public interest, numerous examples of children being charged or cautioned have resulted. See, eg, Thomas Crofts and Eva Lievens, 'Sexting and the Law' in M Walrave et al (eds), *Sexting: Palgrave Studies in Cyberpsychology* (Palgrave Macmillan, 2018) 119. This is referred to again in chapter 5.

[79] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989), [3.24].

[80] Ibid.

communication.[81] This concern was not limited to forms of 'wiretapping' or methods of intercepting digital communications but was apparently premised on surveillance devices: the installation of cameras and other equipment in order to record what was displayed on the computer screen, or otherwise to observe the entering of access credentials. As English law does not have a common law right to privacy, the Commission was concerned not to provide what could be construed as a *de facto* privacy protection.

It was on the basis of these three possible interpretations of 'access' that the Commission ultimately recommended the adoption of the requirement that the accused 'cause a computer to perform a function' and that such conduct be carried out with the 'intent to secure access'. This framing, according to the Law Commission, would exclude mere physical access and mere scrutiny of data where there is not the necessary degree of interaction with the computer.[82] While acknowledging that this would include the mere act of turning a computer on, the requirement that there be an intention to 'secure access' was thought to be a sufficient limitation.

The changing nature of computing technologies, however, has given rise to the potential that the drafting of the section 1 offence is not sufficient to exclude at least the first concern for which the Law Commission recommended caution: the criminalisation of mere physical access. The lack of a clear definition of computer, and the broad approach to 'access' being capable of being established by mere use, is thus incapable of providing interpretative guidance as to what is and is not a computer. This has arisen due to the trends in the development of ubiquitous computing, sensor networks and Internet of Things (IoT) devices. A serious risk of over-inclusiveness in the coverage of the section 1 offence has inadvertently developed.

[81] Ibid [3.25].

[82] Ibid [3.26]

B The 'new' computers

The early development of computing technologies throughout the period leading up to the formulation of the CMA was canvassed briefly in Chapter 2. By the time of the events in the foundational cases of *R v Gold and Anor*[83] and *Cox v Riley*,[84] computing technologies had begun transitioning from the large, specialised and expensive devices in the realm of corporate, industrial, and academic application, to become smaller, generalised and designed with an increasing degree of end-consumer focus. The internet as we know it was yet to be widely adopted, so early networks were proprietary and required specialist equipment to operate.

It was on this basis that the criminal opportunities arising with respect to these newer implementations of computing technologies began to be conceived of as unique and new. In order to promote reliance upon its proper operation, the computer itself required protections that were apparently unavailable elsewhere in the criminal law; or in the least, not clearly or sufficiently available.

The Law Commission's frame of reference in respect to the notion of computing technologies was thus centred on the application of computing technology in commercial settings, and further was limited to a conception of computers as being relatively self-contained albeit with an emerging ability for external access via dedicated data lines. The examples used in the scoping of the Law Commission's report was the emerging role of computers in banking, business administration, air traffic control, hospital systems, and robotic controls in manufacturing.[85] The mischief they conceived was therefore limited to the types of activities that could be directed at those systems. Any external access was necessarily complex. A hacker would need access to the correct 'data line', a modem compatible with the network to be accessed, and knowledge of the communications

[83] [1988] 2 All ER 186.

[84] (1986) 83 Cr App R 54.

[85] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989), [1.15].

software used.[86] Hackers were therefore framed as "hav[ing] a background in software development or systems engineering, and thus hav[ing] inside knowledge."[87]

The proprietary nature of the computing systems and networks, the complexity involved in gaining access to those systems, and the lack of general consumer level access to that class of technology greatly affected the foundations of the CMA. 'Access' to a computer required clear and direct interaction, even when achieved externally: the correct data line needed to be identified. While concepts of information or data security were emerging and increasingly common in implementation, these mechanisms were relatively crude, often relying on basic forms of access protection in the form of simple passwords, or merely keeping the details of the data line secret. The computers, software and systems in question were also relatively task-oriented: while they could be put to different uses, there was limited scope for the simultaneous capability for, or operation of, multiple computing tasks.

While the technology at the time might have supported the conclusions drawn by the Law Commission, the introduction of the CMA did not halt the continuing technological development of computing technologies. Computers no longer exist to carry out a limited set of specific tasks. They can perform many operations and communicate with other computers and devices. Computing hardware has become ever-increasingly powerful, and software has become more sophisticated, now even algorithmically capable of forms self-adjustment and operation. We have moved away from people 'using' computers to perform particular functions, to having computers respond and interact with 'users' across a multitude of settings and capabilities.[88]

In a conceptually similar way to that with which the Google search algorithm tailors its results, in respect of a search query you physically enter into its 'search bar' by typing on a keyboard or tapping on a screen, to your personal web history (it *learns* your interests and responds accordingly), computers are becoming increasingly designed to *predict* what

[86] Ibid [1.23].

[87] Ibid [1.24].

[88] Susan Brenner, *Law in an Era of Smart Technologies* (Oxford University Press, 2007) 123-35.

you are going to need and provide it for you without the need for user input. While the Google search algorithm does this via software, this kind of predictive and responsive functionality is being coupled with hardware that is eroding the nature of physical interaction with computing devices.

While the predominant means of 'using' computing technology may still be thought of today as remaining centred on us 'using' them to complete defined tasks by providing a physical input via a keyboard, mouse, or screen to prompt a computation, the advancement of the IoT and the currently expressed aims of many software designers, is to remove the need for physical input, or physical input in that form. This is the crux of the challenge for the CMA's approach to defining 'access'.

Consider the development of IoT devices. The term IoT refers to the embedding of network and computing technologies into any number of everyday items which enables them to communicate via the internet and be monitored or controlled by either a user or automated software. The IoT includes the development of sensors that can detect position, acceleration and movement, temperature, light, humidity, sound, and more which can be used to monitor or control any number of factors in multiple settings: from industrial application, production lines and supply chain management, to the products now making up consumer level 'smart homes' technologies. In respect of the latter, we see internet-enabled and computerised washing machines (like those in Omerod and Laird's examples above), music and sound systems, lighting controls, and heating and cooling systems to name but a few.

This new category of device seeks to apply the 'benefits' of internet connectivity to all facets of life, creating a seamless integration of devices communicating together independently of the 'user'. These computers do not require an intentional access: they operate independently of the operator to create a seamless experience. These devices, aside from their initial activation, will access and communicate vast amounts of data autonomously of the user.

The development and implementation of the IoT is under increasing scrutiny from industry, academia and governments. However, much of that scrutiny has related to

privacy risks associated with the free flow of data about individuals, or the cybersecurity implications of poor practices by manufacturers of these devices vis-à-vis, for example, the application of encryption technologies. Little has been said with respect to how the operation of these automated and sensor-based devices challenge the notion of accessing a computer. It might well be the case that in its quest to be technology-neutral in respect to what may or may not qualify as a computer for the purpose of the CMA, the focus on 'use' has been rendered not 'technology-neutral' in that in centres on a particular conception of how someone interacts with that computer to 'cause it to perform a function'.

These kinds of sensors and technologies already raise questions with respect to devices that common-sense would dictate are indeed computers: smartphones. Consider the following:

> A is sitting at a table in a café with friends B, and C. B gets up and goes to the counter to order a coffee, leaving their smartphone on the table. A asks C if they know what time it is, which C, for whatever reason, is unable to answer. A, noticing B's phone, decides to, without B's consent, physically tilt the phone forward. The action of physically tilting the phone triggers the phone's internal accelerometer, designed to detect when the phone is being picked up. The smartphone automatically activates, having detected physical movement, turning on the display and showing the 'lock screen' which, aside from indicating that the contents of the phone are protected, displays the time. A sets the phone back down.

In this situation, the mere tilting of the smartphone caused it to activate and display the time. Despite not dealing with the device in any form which might be analogous to earlier forms of interacting with a computer (via a keyboard or mouse) or even interacting with the touch screen (the modern equivalent of using a keyboard or mouse), A has clearly 'accessed' the phone. The physical movement of the device triggered a response that enables the phone to be 'used'. While this example clearly involves a physical interaction with the device, the threshold for the degree of physical interaction with the device upon which 'access' can be said to have been achieved is minimal. By merely physically touching the device, an access has occurred by virtue of the inclusion of an accelerometer that activates the device.

Now consider the nature of the 'access' in the scenario below:

> A and B host a technology-focused radio show. In the context of discussing the uptake of a high profile 'digital assistant' smart speaker, the pair discuss the method by which the speaker can be interacted with. Such interaction requires the verbal use of a particular activation or 'access' phrase which, when spoken, triggers the device to listen to a command. B, as an example of the scheduling function, makes a statement to the effect "[activation phrase] add dinner with C at 7 pm on Wednesday to my calendar". A then laughingly observes that B has likely triggered many of these speakers, to which B agrees, laughing that that was her intention. In fact, hundreds of digital calendars belonging to people listening to the show who own that particular speaker see the appointment added to their calendar.

Here, the device in question is a smart speaker that functions by constantly recording its surrounding environment until it hears the relevant activation phrase. The device is likely a computer: many include the same computing and processing capabilities of the smartphone in the first example above and no reasonable argument has been made, or attempted,[89] that a smartphone does not qualify as a computer. But this type of device is interacted with solely on the basis of voice, not physical interaction. The statement by B, then, can be understood as access under two of the forms provided by the CMA. By making the statement she did, B has caused the smart speaker to perform a function that has 'alter[ed] … the program or data' per sub-section 17(2)(a) in that her statement has resulted in the addition of a new calendar entry with end-users digital calendars. Her statement can also be said to have 'used' the smart speaker per sub-section 17(2)(c) given that both her statement resulted in the software that enables the smart speaker to cause that alteration in the end-users digital calendar to be executed per sub-section 17(3)(a), and that such an alteration was itself a function of the smart speaker's software per sub-section 17(3)(b).

While the 'access' above centred on an interaction via voice, there are now many situations where mere physical proximity can be said to result in an 'access' by way of the expansive definition of 'use'. Any computer system that relies on biometric security protection, particularly facial recognition software, operates on the basis of initiating an automated scan of the face of an individual who positions themselves in front of the

[89] See, *R v Ashford* (Unreported, Westminster Magistrates Court, 13 August 2014).

device's camera. Consider the café example above, but this time instead of leaving their smartphone on the table, B instead leaves their laptop open but secured by a password. A physically manoeuvres herself to be able to view the screen so she can identify the time as displayed in the corner of the screen. Suppose B's laptop had an automated facial recognition security feature. A, by placing herself in the physical proximity of the screen intending to observe the time, but despite not touching or otherwise interacting with the device, triggers the facial recognition process. Without any direct intervention, other than being in physical proximity to the laptop's camera, A has now 'used' the laptop: her physical proximity resulted in the computer undertaking an analysis of her face. Even though the feature would recognise that A was not in fact B, and thus prevent her from gaining any meaningful use of the laptop, she has nevertheless 'used' the laptop. Her intention to view the time, thus triggering the facial recognition response, is likely sufficient for the purposes of the section 1 offence.

But it is not just these, arguably *de minimus,* examples that raise questions as to the scope of 'access'. A question of fair labelling and charge selection arises in circumstances where computer technology has been applied in 'non-traditional' contexts and exploited in the commission of an otherwise non-computer related offence. In Nov 2017, West Midlands Police publicly released video footage of a 'relay attack' on a vehicle parked in Solihull.[90] The vehicle in question featured a keyless entry system: instead of a physical key, the owner of the vehicle uses an electronic 'fob' that emits a radio frequency with a designated access code that, when received or detected by the car's internal computer, permits the car to be unlocked and started. The offenders made use of two 'relay devices', the first was carried and positioned by the window of the house in order to receive and amplify the signal from the relevant 'fob' stored inside the house. The second was held by a co-offender adjacent to the vehicle which, when the 'relayed' signal from the device near the house was received, allowed the car to be unlocked and driven away. This process, relied on to commit theft of the car, took less than 75 seconds.

The labelling question here is one of whether the conduct of the accused is best described as a pure theft of the vehicle, as offences under the CMA, or both? Were the

[90] West Midlands Police, 'Relay attack Solihull', *Youtube* (26 Nov 2017) <https://www.youtube.com/watch?v=8pffcngJJq0>.

offenders interrupted during this sequence of events, the CMA offences are clearly completed, and, depending at what time the interruption occurred, perhaps an attempted theft. The difficulty in practice of prosecuting and successfully proving a charge of attempt perhaps creates an incentive in a situation like this that the charges under the CMA would be relied upon to secure a conviction. But does a successful prosecution under the CMA accurately communicate to the offenders or the broader public the nature of the wrongdoing in this case? While this question will be returned to in Chapter 5, an additional important question in relation to 'computer' and 'access' arises here: at what point does a computer become the object it is embedded in and controls, or a what point does an object become a computer?

It seemingly took 27 years for the example of the electronic lock in a car, discussed at the Standing Committee Stage of the passage of the CMA, to appear in practice. But much has changed since MPs dismissed concerns of over-inclusiveness.[91] The continued trend to add elements of computing technology to all manner of devices raises the spectre that without a clear attempt to provide some form of limitation to the concept of 'computer' or 'access' under the CMA, the section 1 (and section 2) offence run the risk of applying in any number of absurd and unexpected scenarios. The ability for law enforcement and prosecutors to creatively push the boundaries in the future remains an open possibility.

IV CONCLUSION

In this chapter the recommendation of the Law Commission that 'computer' ought to be left undefined for the purpose of the CMA was considered in respect of the same, ultimately abandoned, approach in evidence law upon which support for that recommendation was heavily relied upon. As well, the potential for the term 'access' to operate as a means of limiting the scope of what may or may not be a computer given the changing and evolving nature of computing technologies was explored. Ultimately, the construction of both terms has substantial potential for over-inclusiveness.

[91] See, Lloyd (n 26).

'Computer' was left undefined in an attempt to ensure the offences within the CMA would remain 'technology-neutral'. However, the conceptual focus on 'access' and 'use' within the structure of the offence has likely resulted in the offence in fact not being technology-neutral in that imbued in its structure remains a particular conception of what a computer is and how it is used, despite not naming it so. This presents an issue as the scale of the IoT, and the increased reliance and integration of computing technologies, sensors and new modes of interaction (voice etc.) into all manner of products continues to occur. Crime committed using these integrated computing technologies also raise the issue of charge selection: should conduct involving acts that fall neatly within a general sphere of the criminal law, such as fraud or theft, be prosecuted and dealt with solely on that basis regardless of the use of computing technologies, or can and should the CMA offences operate in addition to, or instead of, these offences?

The push for technology-neutrality in the drafting of new laws seeks to ensure that the law keeps pace with technological change. But it also presumes that the new law was necessary in the first place, thus warranting the status of being enduring and 'technology-neutral'. On first reading, the observations in the latter half of this chapter might appear to support the contention that the issue is that the criminal law is struggling to keep up with technology. However, for this to be a convincing view, consideration must be then directed towards the suitability of general offences to respond to the same conduct.

Take the car theft and the enabling relay attack in Solihull. There, the implementation of computing technology merely increased the ways in which the car could be stolen. The crime remains that the car was, in fact, stolen. The means of facilitating the theft (digitally copying and re-broadcasting the access code) are not directly relevant to proving the theft occurred. The general offence applies, despite the presence of the inbuilt computer system controlling access to the car.

But if the computer that controlled access was physically separated from the car, our approach to describing the conduct changes. The physical separation of the computer from the car now, despite the 'control relationship' being the same as above (the computer still unlocks the car), gives rise to a characterisation of conduct that falls closer to the current presumptions of the CMA. An attempt to access that physically

separate computer becomes one of 'unauthorised access' or 'hacking', which then seems to correctly fall within the ambit of the section 1 (and 2) offence. Any eventual theft being enabled by that conduct is dealt with as and if the need arises, but the CMA offences apply quite plainly.

What we see perhaps, as computing technology has evolved to become ever more *integrated* and *integral* to everyday conduct, is not that the criminal law is struggling to keep pace with technology but rather that the technology is finally catching up with our pre-existing legal paradigms. The idea that computer-related crime needs to be labelled separately made sense when computing technologies only existed separately. As the boundaries of computing technologies blur and fade away, perhaps so too does the need, at least for the criminal law in these circumstances, to treat computer misuse as a separate and identifiable criminal wrong.

Returning to the normative model from chapter 1, it was observed that the appropriate construction of a computer-related offence should clearly define the bounds of conduct and culpability within the structure of the offence and that this should be commensurate with the harm or risk of harm. Further, the offence should not be able to be applied in a manner such that those who are subject to the offence are unaware or inadequately informed as to its scope. It is difficult to see how, with the current potential for both 'computer' and 'access' to be interpreted so widely, these constraints could be said to have been respected. An offence that potentially criminalises circumstances ranging from mere physical proximity to a device on a table, making a verbal joke, undertaking conduct criminalised elsewhere, in addition to responding to the actual harm relied on to justify the offence (breaches to the integrity of a computer), seems to rely almost entirely on police and prosecutors to effectively define and limit its application.

But this in itself is not reason enough to discount the section 1 (and section 2) offences. It may be the case that while the focus of the target of the *actus reus* of the offences (computers) is cast broadly, an analysis of the complete *actus* might serve to provide some limitation. So too may the *mens rea*. However, the construction of the complete *actus* of the section 1 and 2 offences are drafted in the inchoate mode. As such, for the potential over-inclusiveness of the offences to be appropriately contained, the *mens rea* must undertake a

large amount of work to suitably transform the normative character of an accused's conduct such that it can be considered criminally wrongful. Analysis of this issue will form the subject of chapter 5.

Chapter 5

Inchoate Drafting & Delimiting Wrongfulness: the Heavy Lifting of 'Unauthorised Access'

If debugging is the process of removing errors, then programming must be the process of inserting them.

Anonymous

I Introduction

Despite its subsequent review and amendment, the CMA remains functionally situated within the understanding of the use of computers and the likely perceived harms of computer misuse as conceived in the late 1980s: that the 'unauthorised access' to computers was uniquely harmful in that it breached the integrity of the data and operation of the computer, and this could cause disruption and financial loss to corporate computer networks. Further, in circumstances where the breach of integrity through obtaining 'unauthorised access' did not result in subsequent loss or damage, it was

believed the broader criminal law was not equipped to respond. Thus, such conduct ought to be criminalised due to the risk of that harm eventuating.[1] That is, the unauthorised access *itself* was evidence of a criminal intent. Further, such a law would work to discourage 'hackers' from seeking to gain 'unauthorised access' in any form.

While the CMA's framing of computer misuse, and the perception of the actions and role of hackers, seemingly has not changed over the intervening decades, our broader use of computing technologies has. There is an increasing array of circumstances where a person may be said to have obtained 'unauthorised access' where they, in fact, possess no ulterior criminal intent. This is a product both of the changing nature of computing technology, and the court's adoption of a broad approach to considering authorisation with reference to individual sets of data and pieces of software,[2] technological protection mechanisms, terms of service and other 'acceptable use' and employment policies,[3] and even physical positioning of devices within a building along with a verbal warning.[4]

This chapter, therefore, examines the section 1 offence's broad targeting of conduct that 'causes a computer to perform a function' and its reliance on the 'unauthorised access' standard to delimit wrongfulness in order to illustrate how these terms now capture conduct beyond that conceived when the CMA was drafted. This over-inclusiveness is in addition to that identified in Chapter 3, and troubling in that it has arisen due to the lack of a clear connection to the issue of culpability with respect to envisaged harms of computer misuse. That is, this chapter argues that the adoption of inchoate drafting in the substance of the section 1 offence, in particular, unjustifiably presupposes wrongdoing on the part of a computer user. There is a lack of a direct connection to an intended or consequential harm that ought to enliven criminal liability. Further, there is an absence of any *mens rea* requirement (beyond having knowledge that

---

[1] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [2.10]-[2.25].

[2] *R v Bow Street Magistrates Court and Allison, ex parte United States (No. 2)* [1999] 3 WLR 620.

[3] See, E. Susan Singleton, 'Computer Misuse Act 1990 – recent developments' (1993) 14(1) *Company Lawyer* 22; *R v Bennett* (Unreported, Bow Street Magistrates Court, 10 October 1991); *R v Spielmann* (Unreported, Bow Street Magistrates Court); and *R v Delamare* [2003] EWCA Crim 424.

[4] *Ellis v DPP (No. 1)* [2001] EWHC Admin 362.

an intended access is, in fact, unauthorised) that is capable of normatively changing the character of otherwise benign conduct such that it can be considered wrongful.

The focus here is not to dispute that there are circumstances in which computer intrusions, or *digital trespass*, may indeed warrant a response from the criminal law.[5] Rather, this chapter seeks to address the criminalisation of otherwise benign conduct in circumstances where there is an absence of an *ulterior criminal intent*: that is, the section 1 offence results in the criminalisation of *digital trespass per se.* It considers the normative question of whether 'authorisation' is a desirable standard by which to distinguish legitimate computer use from wrongful computer (mis)use in the context of an offence that does not in fact require unauthorised access to be established. All that is required is that the accused 'caused a computer to perform a function'.

As such, this chapter will argue that the 'unauthorised access' standard was conceived to target a conception of 'hacking' and a harm that is no longer accurate, useful, nor justifiable. The standard has been adopted from the civil law, specifically the tort of trespass to property, but without sufficient criteria to warrant the conduct becoming criminally wrongful.[6] The result has been that while the CMA was conceived to respond to circumstances where computers were the *target* of malicious or wrongful conduct, it instead is capable of applying to almost all conduct involving the use of a computer (directly and indirectly). The offence includes conduct not just related to the integrity of the computer, resulting economic harms, or other disruption, but instead to

---

[5] This issue will be returned to in Chapter 6, where the rationale for the operation of the CMA is considered in the context of other legal frameworks, particularly the operation of civil trespass claims and the impact of the *General Data Protection Regulation* ('GDPR').

[6] See, Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988), [6.15]; and Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [3.22]-[3.24] where the Commission expressed a desire for the drafting of the offence to restrict its conception of 'access' so as not to be conflated with physically entering the room where the computer was located, in effect criminalising physical trespass. See, additionally, Joseph Olivenbaum, '<CTRL> <ALT> <DEL>: Rethinking Federal Computer Crime Legislation' (1996-1997) 27 *Seton Hall Law Review* 574, where at 641 Olivenbaum considers the applicability of trespass as an appropriate framework to reconsider the *Computer Fraud and Abuse Act* in the United States, noting that the Act was introduced to Congress with the explanation that it responded to conduct:

> akin to trespass onto someone else's property. A person who rummages through the information contained in a computer … causes the same harm as an intruder who clandestinely enters a person's home to look through the contents of the owner's personal records and documents

any interaction with software, data, or other material accessible in a digital form that might otherwise more appropriately fall within other spheres of law.

II INCHOATE DRAFTING

The drafting of new offences, or reformulation of existing offences, in such a manner that they operate to criminalise conduct on the basis that a particular harm is a *likely* or possible result of that conduct is typical of a broader trend in the criminal law.[7] Otherwise lawful conduct might be considered criminally wrongful where the accused has an 'ulterior intent' that the underlying conduct in question contributes to the commission of a further substantive offence.[8] These offences are said to be drafted in an *inchoate mode*. That is, the conduct elements of the offence focus on the *typical* steps undertaken by an accused in preparation to commit what might otherwise be a more serious offence. The offence seeks to criminalise a course of conduct early in the process in an effort to prevent a more serious harm from resulting, rather than responding only when that harm is realised, as is the case with result-based drafting.

Inchoate drafting requires a deconstruction of the characteristic steps in a specific course of criminal conduct. These types of offences fall within a spectrum of criminalisation alongside the more traditional forms of inchoate, or preliminary, offences: attempts, conspiracy, and the various forms of accessorial liability. The function of offences that are drafted in an inchoate mode, however, is to bridge a 'gap' that arises where the traditional forms of inchoate offences, attempts in particular, are not available

---

[7] See, generally, Ashworth and Zedner *Prevention and the Limits of Criminal Law* (Oxford University Press, 2013); Doug Husak, *Overcriminalisation: The Limits of the Criminal Law* (Oxford University Press, 2007); Andrew Simester and Andrew von Hirsch, *Crimes, Harms and Wrongs: On the Principles of Criminalisation* (Hart, 2011).

[8] See, eg, Jeremy Horder, 'Crimes of Ulterior Intent', in Andrew Simester and Tony Smith (eds) *Harm and Culpability* (Oxford University Press, 1996); Peter Asp, 'Preventionism and Criminalization of Nonconsummate Offences' in Andrew Ashworth, Lucia Zedner and Patrick Tomlin (eds), *Prevention and the Limits of the Criminal Law* (Oxford University Press, 2013) 23; Douglas Husak, 'The Costs to Criminal Theory of Supposing that Intentions are Irrelevant to Permissibility' (2009) 3(1) *Criminal Law and Philosophy* 51; Peter Westen, 'The Ontological Problem of 'Risk' and 'Endangerment' in Criminal Law' in R.A. Duff and Stuart Green (eds) *Philosophical Foundations of Criminal Law* (Oxford University Press, 2011) 304, 308; RA Duff, 'Intentions Legal and Philosophical' (1989) 9(1) *Oxford Journal of Legal Studies* 76, 88 where Duff explores the nature of 'ulterior intent' as an intent extending beyond the *actus reus* and its consequences, relying on the interpretation set out in *Jaggard v Dickinson* [1981] QB 527, at 532.

because the conduct at issue is not sufficiently proximate to a completed result-based offence.[9]

This approach to drafting new inchoate mode offences has been supported by commentators in a number of contexts.[10] In some cases, the acts criminalised by such provisions might involve conduct that has a limited, if any, legitimate use or purpose. In these circumstances, the offences 'presume a further criminal intent from the very fact' of the conduct occurring.[11] The clearest example of this approach perhaps arises within the field of 'possession' based offences. For example, the possession of an offensive weapon in public without lawful excuse is an offence.[12] The onus is on the accused to establish their possession has a legitimate excuse, without which wrongfulness is otherwise presumed from the mere fact of possession of the weapon. The justification for this particular form of possession offence arguably rests on the risk of harm that could result from the use of such a weapon: serious injury and loss of life.

More frequently, inchoate mode offences operate to criminalise an otherwise lawful act in circumstances where the accused undertakes that act with an evidenced intent (an ulterior intent) that the conduct contributes to the commission of a further offence. The structure of those offences is thus likely to include the requirement that the accused has knowledge of a potentially harmful use or result of the conduct and intends to achieve or proceed to give rise to that harm. This model of inchoate offence arises in a number of circumstances. For example, the possession of a machine or implement capable of being used in the creation of forged instrument is criminalised where the accused knows the

[9] See, eg, *R v Geddes* [1996] Crim LR 894; Ashworth, *Principles of Criminal Law* (Oxford University Press, 4th ed, 2003) 468. Additionally, in circumstances where there is only one offender, the offences of conspiracy or encouraging and assisting (*Serious Crimes Act 2007* ss 44, 45 and 46) are unavailable to address any gaps in the coverage of conduct.

[10] See below nn 22.

[11] Andrew Ashworth, *Principles of Criminal Law* (Oxford University Press, 4th ed, 2003) 470. *Cf* Douglas Husak, 'Reasonable Risk Creation and Overinclusive Legislation' (1998) 1 *Buffalo Criminal Law Review* 599, at 618.

[12] *Prevention of Crime Act 1953* s 1; *R v Jura* [1954] 1 QB 503; and *Williamson* [1978] 67 Cr App R 35.

machine has been designed for that purpose and possesses an intention that the machine be used to make such an instrument, either for themselves or another.[13]

The offence of burglary[14] and the offences of fraud[15] also incorporate this approach. The offence of burglary is complete when an accused either enters a building as a trespasser with the intention to steal,[16] or while in a building as a trespasser later steals property or attempts to steal property.[17] In that sense, the offence of burglary criminalises the commission of an otherwise civil wrong, the tort of trespass, where that trespass is used to intentionally enable the commission of theft. The intention to steal normatively changes the character of the underlying conduct, transforming it from a civil to a criminal wrong.

The reformulation of the fraud offences, a product of the commencement of the *Fraud Act 2006* which shifted the focus of the offences away from requiring the result-based conception of deception,[18] now criminalises the conduct of an accused who, in various forms, commits a dishonest act[19] while intending to make either a gain for themselves or another,[20] or to cause a loss to another.[21] It is no longer required to establish that an accused's conduct resulted in a completed deception: the undertaking of a dishonest act with the intent to achieve that deception for gain or to cause loss is sufficient.

It is clear, even from this brief summation, that the adoption of the inchoate mode drafting of criminal offences occupies a spectrum of possible formulations. This spectrum

---

[13] *Forgery and Counterfeiting Act 1981* s 5(3).

[14] *Theft Act 1968* s 9.

[15] *Fraud Act 2006* ss 2, 3 and 4.

[16] *Theft Act 1968* s 9(1)(a), 9(2).

[17] *Theft Act 1968* s 9(1)(b), 9(2).

[18] See, further, Law Commission, *Fraud* (Report no 276 Cm 5560, 2002) [3.25]-[3.28].

[19] *Fraud Act 2006* s 2(1)(a).

[20] *Fraud Act 2006* s 2(1)(b)(i).

[21] *Fraud Act 2006* s 2(1)(b)(ii).

has been explored by numerous commentators,[22] but particularly relevant for the purpose of this discussion is the work of Jeremy Horder in his work to develop a typology of the various types of inchoate offences or, as he refers to them, 'crimes of ulterior intent'.[23] Horder's categories of crimes of ulterior intent provide a useful framework to understand the operation of, and differences in, the construction of the CMA's section 1 and section 2 offences.

A *Horder's Categories of Inchoate Crimes*

1 *'New' and traditional forms of inchoate crime: labelling and attempts*

Horder's approach to developing a typology or framework of the approaches to inchoate mode drafting is situated within the context of what would appear to be serious inconsistencies in the development of the increasing array of inchoate mode offences across the broader criminal law. These inconsistencies have been described as a symptom of the lack of overarching and agreed-upon principles of criminalisation which might otherwise provide guidance to the reasoned, ordered and coherent creation of such offences.[24] Horder further adds that the *ad hoc* and 'haphazard growth of the law'[25] has contributed to apparent inconsistency, highlighting that it is a specific crime to commit

[22] See, eg, Law Commission, *Conspiracy and* Attempts (Law Com No. 318, 2009); Peter Ramsay, 'Democratic Limits to Preventative Criminal Law' in Andrew Ashworth, Lucia Zedner and Patrick Tomlin (eds), *Prevention and the Limits of the Criminal Law* (Oxford University Press, 2013) 214 for discussion on 'pre-inchoate crimes', or those that would fall in Horder's categories 4 and 5 (discussed below); Douglas Husak, *Overcriminalization* (Oxford University Press, 2008) 160–1; JJ Child, 'The Structure, Coherence and Limits of inchoate liability: the new ulterior element' (2014) 34(4) *Legal Studies* 537; JJ Child and A Hunt, 'Mens rea and the general inchoate offences: another new culpability framework' (2012) *NI Legal Q* 245; Ian Leader-Elliot, 'Benthamite reflections on codification of the general principles of criminal liability: towards the panopticon' (2005) 9 *BC L Rev* 391; B McSherry, 'Expanding the boundaries of inchoate crimes: the growing reliance on preparatory offences' in B McSherry et al (eds) *Regulating Deviance – The redirection of Criminalisation and the Futures of Criminal Law* (Hart, 2009); GR Sullivan, 'Bad thoughts and bad acts' (1990) Criminal Law Review 559; PH Robinson, 'A functional analysis of criminal law' (1994) 88 *Northwestern University Law Review* 857; RA Duff *Criminal Attempts* (Oxford University Press, 1996); Michael T Cahill, 'Inchoate Crimes' in Markus Dubber and Tatjana Hörnle (eds) *The Oxford Handbook of Criminal Law* (Oxford University Press, 2014) 513. For a discussion on Action Theory as applied to defining criminal conduct, see, eg, Leo Zaibert, 'Philosophy' in Dubber, above, 132, 133-8; Gideon Yaffe, *Attempts in the Philosophy of Action and the Criminal Law* (Oxford University Press, 2010).

[23] Horder (n 8) 153.

[24] Ibid 155; and Andrew Ashworth, 'Is the criminal law a lost cause?' (2000) 116(2) *Law Quarterly Review* 225.

[25] Horder (n 8) 155.

an assault with intent to rape or to steal, but not to commit such an assault with intent to murder.[26] Further, it is a crime to possess a shotgun with an intent to endanger life, but no such crime exists for the possession of a poison held for the same purpose.[27]

Horder uses this observation not to criticise the adoption of inchoate mode drafting. Instead, his comments are part of a broader effort to respond to, and further develop, arguments first set out by Peter Glazebrook;[28] that Parliament ought to seek to 'painstakingly … prohibit all the specific kinds of conduct worthy of condemnation as criminal, when done with the intention to commit the crime.'[29] Glazebrook's view arose in the context of a broader critique of the lack of clarity with respect to conduct that in any given situation may or may not constitute an attempt. Whether or not an attempt of a given offence has occurred, as noted above, turns on whether the conduct of the accused is sufficiently proximate to the completed offence: their conduct must extend beyond acts that are 'merely preparatory'.[30] The problem here is situated within concern for the labelling function of the criminal law.[31] A successful prosecution for an attempt of a crime may not, as a label, necessarily fairly reflect the degree and nature of the conduct that was actually engaged in by the accused.

In an effort to respond to the labelling issues, both Glazebrook and Horder appear to suggest that carefully structured and graduated offences that are focused on the degree of conduct engaged in, coupled with a similarly graduated degree of intent, may result in a framework of offences that better balance the common law principle of parsimony in

[26] Ibid 162.

[27] Ibid 155.

[28] Peter Glazebrook, 'Should We Have a Law of Attempted Crime?' (1969) 85 *Law Quarterly Review* 28.

[29] Horder (n 8) 157.

[30] *Criminal Attempts Act 1981* s 1; and see *Gullefer* [1990] 1 WLR 1063, 1066.

[31] See, James Chalmers and Fiona Leverick, 'Fair Labelling in Criminal Law' (2008) 71(2) *Modern Law Review* 217.

offence definition[32] and of fair warning (or maximum certainty).[33] In respect of the principle of parsimony, Horder suggests that one way the principle might be respected 'is to cut back on over-inclusiveness';[34] that is, by clearly and specifically grading offences through articulating the relevant norms transgressed throughout the steps of the logic sequence of a course of criminal conduct. Under this approach, the conduct necessary to commit an offence can be directly and sufficiently set out.[35]

However, while Glazebrook's position considers the complete adoption of such a comprehensive approach to drafting the criminal law alongside the abolition of criminal attempts,[36] Horder, relying on the principle of fair labelling (or representative labelling),[37] argues that criminal attempts can and should operate alongside the separate criminalisation of specific classes of inchoate mode crimes.[38] To charge an accused with *attempted murder* for standing outside a purported victim's house with a weapon, would, to Horder, constitute a misrepresentation of the accused's degree of culpability.[39] If the accused in this example were, in fact, to be prosecuted for attempted murder, there is the possibility that they may escape criminal liability altogether where their presence at the victim's house in possession of the weapon is considered 'merely preparatory'. Thus, were it considered appropriate that the accused's conduct here ought not to escape criminal liability, an inchoate mode offence of possession of an offensive weapon with intent to murder could work to bridge the 'unacceptably large representative labelling gap between one of the most serious offences against the person ... and comparatively minor

[32] See, eg, Ashworth, (n 11), 66, 80-82; Peter Alldridge, 'Making Criminal Law Known' in Stephen Shute and Andrew Simester (eds) *Criminal Law Theory: Doctrines of the General Part* (Oxford University Press, 2002) 103.

[33] Ibid 75-78

[34] Horder (n 8) 167.

[35] Ibid 171.

[36] Glazebrook (n 28).

[37] See Ashworth (n 11); Chalmers, (n 31).

[38] Horder (n 8) 167.

[39] Ibid 161-2.

offences, like possessing offensive weapons'.[40] The charge of attempted murder would remain available where the accused's conduct had, in fact, got closer to realising that intent.

For Horder, this approach is suitable and justified on the basis of the nature of the proximity requirement to establish an attempt: that is, the difficulty in assessing the underlying elements to establish an attempt in any given fact situation as this necessarily relies on questions of judgment and degree.[41] For Horder, the offence of attempted murder would remain appropriate in those circumstances where the accused's conduct has reached the point where such a label (attempted murder) accurately reflects the *totality* of their conduct. The rise of the importance of considering the labelling issue with respect to attempts has evolved with the changing nature of the offence as being purely a product of the common law to one provided by statute.

Prior to the passage of the *Criminal Attempts Act 1981* (the 'CAA'), the test for assessing whether an accused's conduct constituted an attempt was determined on the basis of proximity: that is, was the accused's conduct sufficiently proximate to the completed offence? No precise test had been evolved, but the principle had been described as requiring conduct that was 'immediately and not merely remotely connected' to the completed offence.[42] The notion of 'proximity' had inevitably been informed by other approaches to varying degrees: for example, the unequivocal act test and the last act test.[43] The result was a lack of certainty, but with a dominant, although

[40] Ibid.

[41] Ibid 162.

[42] *Jones v Brooks* (1968) 52 Cr App R 614, approved in *Haughton v Smith* [1975] AC 476.

[43] The 'unequivocal act' approach, where the accused's conduct is assessed as to whether there existed conduct on the part of the accused with no other possible explanations other than to complete the offence, influenced the decisions in *Davey v Lee* [1968] 1 QB 336; *Jones v Brooks* (1968) 52 Cr App R 614; and *Comer v Bloomfield* (1970) 55 Cr App R 305. And the last act or final stage test, where the conduct of the accused is assessed as to whether they had done all that was necessary to complete the offence except, as the name implies, the last act, influenced decisions in *R v Eagleton* (1855) 6 Cox CC 559, 571; and the heavily criticised decision in *R v Robinson* [1915] 2 KB 342.

not decisive view, towards criminalising only where the accused's conduct was sufficiently close to completing the offence.[44]

On this basis, the conduct of the accused in the attempted murder example above would not be sufficient. To complete the offence, the accused, despite having positioned themselves in front of the victim's house with a weapon, would still need to, perhaps, gain access to the house, locate and confront the victim, and then make use of the weapon such that they could be said to have caused the death of the victim. The preference of the common law was to only permit criminalisation in the final stages of the course of conduct; the acts immediately prior to pulling the trigger.

In the context of their review of inchoate offences with a view to codification, the Law Commission recommended the adoption of a statutory form of attempts that would be centred on the notion of acts beyond mere preparation.[45] The Commission was of the view that the term 'proximate' in the drafting of the codified offence of an attempt should be avoided as it could result in a literal interpretation as meaning 'nearest, next before or after [and thus] it would clearly be capable of being interpreted to exclude all but the "final act".'[46] Given a contributing motivation for codification was to relax the standard required to establish the *actus reus* of an attempt, such a result would be undesirable.

Thus, since the introduction of the CAA, the accused's conduct must be beyond 'merely preparatory' to attract criminal liability as an attempt; that is, they must have 'embarked on the crime proper'.[47] This relaxing of the standard, from sufficiently proximate to beyond merely preparatory, has resulted in an expansion of the application

---

[44] See, eg, *R v Komaroni* (1953) 103 L Jo 97 where the defendants followed a lorry waiting for the opportunity to steal it, even offering mechanical assistance when it broke down. Their conduct was held to have constituted a continuous act of mere preparation.

[45] Law Commission, 'Attempt, and Impossibility in Relation to Attempt, Conspiracy and Incitement' (Law Com No 102, HMSO, 1980)

[46] Ibid [2.48].

[47] *R v Guellefer* (1990) 91 Crim App R 356. See, eg, *R v Geddes* [1996] Crim LR 894 where the accused, despite being in a school lavatory with rope, tape, and knife with the intent to capture and restrain a child, had not in fact 'actually tried' to do so before being caught.

of attempts to conduct not likely to have satisfied the pre-CAA approach.[48] So it is presumably on this basis that Horder makes his claim that a 'large representative labelling gap' can manifest. Under the 'beyond merely preparatory' approach, it is conceivable that an accused who obtains a weapon, places themselves outside the victim's house with the intention to enter and kill may have moved beyond 'mere preparation'.

The approach to attempts has thus shifted from one which begins from the completed offence and asks how close the accused progressed to producing the relevant harm, to one that begins with the accused and considers their actions from the commencement of their course of conduct.[49] It is on this basis that the utility of the creation of inchoate mode offences in circumstance likely to represent Horder's conception of labelling over-reach can be understood.[50]

2 *The typology of crimes of ulterior intent*

The creation of a suitable framework to understand the structure of inchoate mode crimes requires there to be a necessarily clear logic sequence in the commission of an offence.[51] Horder, therefore, differentiates between five categories or types of inchoate mode drafting approaches from which such the logic sequence of a course of criminal conduct can be understood and thus differentially criminalised. The factor upon which these categories are based is the degree of, and the means by which, an ulterior criminal

---

[48] See, eg, *R v Tosti and White* [1997] Crim LR 746; and *R v Toothill* [1996] Crim LR 876.

[49] Of course, the interpretation of beyond 'merely preparatory' has been subject to differing approaches itself. See *Guellefer* (n 47); *Tosti* (n 48); *Toothill* (n 48).

[50] *Cf* the position of Clarkson who contends that on review of the cases involving attempts there appears to be a requirement that accused's conduct has included a confrontation with the victim (in the case of offences against the person) or a confrontation with property (in respect of offences against property). Thus, in the example of the charge of attempted murder for standing outside the victim's house with an offensive weapon would likely not be successful in that there has been no confrontation with that person as a purported victim, thus somewhat weakening the value of that example of mislabelling. It does, however, support Clarkson's contention that the focus on evidence of a confrontation in respect of a charge of an attempt is resulting in too many individuals escaping criminal liability for conduct that might properly be deemed criminal. He identifies cases such as *Geddes* (n 9) and *Campbell* (1991) 93 Cr App R 350 as representative of individuals escaping liability where the accused were in fact on the verge of committing the crimes, but the judges in those cases determined that their conduct could not amount to an attempt 'at law': the jury thus not able to decide whether the accused 'in fact' made an attempt. See, Christopher M.V. Clarkson, 'Attempt: The Conduct Requirement' (2009) 29(1) *Oxford Journal of Legal Studies* 25.

[51] Horder (n 8) 163.

intent is to be established. The ulterior criminal intent operates on the basis that 'the normative significance of [an accused's] conduct changes dramatically when viewed in light of his or her intent'.[52]

Horder thus identified five types of inchoate mode offences:

1. Committing a lesser crime, intending to commit a greater one;
2. Committing a crime, intending to do some non-criminal wrong;
3. Committing a civil wrong, intending to commit a crime;
4. Doing something overtly innocent intending to commit a crime;
5. Crimes where the intent is by its nature ulterior.[53]

The bulk of Horder's arguments, as explored above, focus on his consideration of the first category: the commission of a minor crime with the ulterior intention of committing a more serious offence. He then pays some attention to additional controversies at the heart of his third and fourth categories. It is these two categorisations that can guide analysis of the CMA's section 1 and section 2 offence.

Horder labels crimes that fall within category three and four as 'preparatory' crimes in that the criminality of the conduct does not arise by the achieving of a particular result, but rather where the accused's criminal intention affects the normative significance of conduct that might be, absent that intent, innocent, or would otherwise constitute a civil wrong.[54]

In his third category, crimes involving the commission of a civil wrong, we can place the offence of burglary discussed above: an accused commits burglary where they are a trespasser (a civil wrong) while intending to commit a crime (intending to steal). In a footnote to his introduction of this category, Horder suggests that the CMA's section 1 offence would be a further example of this type of inchoate crime. He provides no

[52] Ibid 154.

[53] The fifth category encompasses traditional inchoate crimes (such as attempts), and crimes that require a fault element that extends beyond the immediate conduct, such as theft contrary to the Theft Act 1968 section 1 where the accused must intend to permanently deprive the person of their property: thus the fault element extends beyond the mere intention to appropriate the property in question.

[54] Horder (n 8) 157.

explanation for how he concluded that the section 1 offence falls within that category, merely noting that the offence related to hacking.

In category four, crimes involving otherwise innocent conduct undertaken with the intent to commit a crime, belong the inchoate mode drafted crimes such as possessing something with intent to destroy or damage property contrary to section 3 of the *Criminal Damage Act 1971*, or possessing gun powder with intent to commit a crime contrary to section 64 of the *Offences Against the Person Act 1861,* and the offence of possession of a machine for use in creating forged instruments introduced at the start of this chapter. Here, possession of the relevant item is not in itself inherently wrongful, but the development of an ulterior criminal intent in the use of that item changes the character of that possession, rendering it criminally wrongful. Possession of a machine that may be capable of producing a forged instrument is lawful until the accused intends to create the forged instrument.

This chapter will now turn its attention to how the CMA's section 1 and section 2 offences fit within Horder's categories of inchoate mode offences, and thus explore the extent of resulting criminalisation. As we shall see, contrary to Horder's note, the section 1 offence does not fit neatly within category three, nor can it seemingly be placed in category four. While the mere fact that an offence does not fit neatly within these categories does not indicate the offence cannot be justified, it does permit exploration of the broader framework of conduct for which the offence was drafted, and thus allows consideration of its appropriateness in the context of the logic sequence of hacking.

B A Logic Sequence of 'Hacking'

The construction of the CMA's five offences might be considered as a broad attempt to 'individuate the relevant norms' in conduct undertaken in the commission of criminal conduct involving the use or presence of a computer.[55] Such an approach might thus recognise the various forms and scale of harm possible in spheres of society reliant on the use of computers. Thus, through the identification of a clear, logical sequence of

[55] Horder (n 8) 171.

necessary conduct, criminalisation can occur at the point where a relevant ulterior intent is formed that changes the normative character of otherwise non-criminally wrongful conduct. In this sense, the offences might be seen to proportionally and appropriately respond to the degree of wrongdoing where an accused is interrupted, or otherwise unable to complete a more serious offence. The CMA's offences might then be seen as more clearly labelling the scope of the offender's conduct, where a prosecution for an attempt may not properly communicate the qualities of their wrongdoing either to the offender themself, or the public.[56]

In the case of the commission of a crime involving 'hacking', the logical sequence of the conduct elements in a characteristically typical form could be set out as follows:

1. The accused identifies a target computer, and *may* seek to obtain or develop digital tools that will assist them.[57]
2. The accused sets out to gain unauthorised access to that computer (that is, they carry out digital trespass) exploiting weaknesses in the computer's security.[58]
3. If successful, the accused may then undertake conduct that impairs the functioning of that computer, or obtains information or sufficient control in which to facilitate the commission of a further offence, or otherwise may retain 'access' in an undetected form for an extended period of time.[59]
4. The accused, relying on the access obtained, commits a further general offence.

---

[56] For a discussion on the principle of Fair Labelling, see Ashworth (n 11), 88-92; and Chalmers (n 31).

[57] Such tools might involve the creation or purchase of an 'exploit kit', software capable of infiltrating target computers, systems, networks or devices. The individual may also purchase information on a 'zero-day' vulnerability: a critical flaw in software that is unknown to the creator, owner or company responsible for the software and thus able to be exploited. A substantial market has been created online for the detection and sale of such vulnerabilities.

[58] Be it a weakness in the software (by finding mistakes in the computer's software that can be leveraged to gain access or control), or a weakness in the organisational policies or human behaviour (institutions or corporations poorly implementing digital security procedures, or the mere guessing of access credentials). Each of these may occur in any number of forms. It is important to note that even unsuccessful attempts to gain unauthorised access to computers result in a change to the system: it logs the attempt and undertakes processes to validate the access attempt.

[59] The latter option here refers to the phenomenon of an Advanced Persistent Threat (or APT). Sophisticated actors who exploit a vulnerability to gain access to a computer or network and work to remain undetected by the owner or computer or network security technologies. Such conduct represents a serious threat to business and government and is often alleged to be state-sponsored activities. This will be discussed in chapter 6.

While this construction is premised on the condition that the computer is the target of the accused's conduct,[60] this structure, unsurprisingly, lays out the underlying conduct targeted by each of the CMA's five offences.

In step one, the obtaining or developing of digital tools that can be used to commit an offence is proscribed by section 3A – *making or supplying articles*.

In step two, where the accused sets out to gain unauthorised access, the section 1 offence (*unauthorised access)* and, depending on the scope of the accused's intent, the section 2 (*unauthorised access with ulterior intent*) offence apply. In circumstances where the accused's intent is to cause an impairment to the operation of the computer or data, or to hinder access to that computer or data, the section 3 offence (*unauthorised acts with intent to impair*) may apply.

In step three, where such impairment in fact occurs, the offence in section 3 certainly applies, and where that access is used to facilitate steps to complete a further substantive offence the section 2 offence continues to apply. Additionally, an attempt of that further offence might be available.[61] In step four, that further substantive offence is complete, thus prosecutable in that form, in addition to the earlier available offences.

As is clear, the section 2 offence is prosecutable at step three, and, where an ulterior intent to commit or facilitate a further offence was present when the steps to commit digital trespass occurred in step two, is additionally available at that point. Similarly, the

[60] As such, the increasing role of the use of a computer as a necessary step in the commission of other substantive offence is not considered here. See the discussion of 'access' and 'use' in chapter 4 and discussion of the broader cyber security landscape in chapter 6.

[61] Again, the issue of proximity may arise, but this will depend on the nature of the computer system. An attempt to transfer funds from a bank account that required unauthorised access to individual accounts it more proximate to the offence of fraud and theft than acts to obtain, say, the schematics of a 3D printed offensive weapon where further steps must be taken to give effect to those schematics and thus be said to possess an offensive weapon.

section 3 offence applies but is limited to acts that in some way impair the operation of the computer or the accessibility or reliability of any data.[62]

The section 1 offence, however, is prosecutable at each and every stage provided the accused knew their conduct was in fact unauthorised. While the section 2 offence criminalises such trespass only where an intent to commit a further substantive office is present, section 1 makes no such distinction. Instead, the section 1 offence criminalises the steps taken to undertake digital trespass (causing a computer to perform a function) where the accused intended to commit any form of digital trespass, knowing that such conduct would indeed constitute such digital trespass.

Returning to Horder's categories of inchoate form crimes above, let us assume for the sake of argument that 'unauthorised access' is merely a civil wrong: *digital trespass*. The section 2 offence can then properly be categorised as a crime involving the commission of conduct that might otherwise be considered a civil wrong (the digital trespass) with an intent to commit a further, or ulterior, crime. That is, the section 2 offence falls within category 3. Under this framing, however, contrary to Horder's reference with respect to the section 1 offence, the basic 'hacking' offence does not. Indeed, the section 1 offence would operate to criminalise the commission of a civil wrong while intending to commit a civil wrong: trespass to computer material.[63] Thus section 1 criminalises otherwise benign, but potentially civilly wrongful, conduct despite there being no ulterior criminal intent.

When digital trespass is not viewed as a civil wrong, the section 2 offence could be said to fall into the first category: committing a lesser crime with intent to commit a greater one. The lesser crime being the section 1 offence. But what then of the section 1

---

[62] The section 3 offence is prosecutable where any unauthorised act is committed with intent to impair computer material, whether or not such impairment actually occurs, or arguably could occur. Section 3(3) contemplates acts that result in impairment to computer material where the offender is reckless: recklessness is constructed in the sense that the act the accused undertakes *will* result in the impairment of the computer or data or hinder otherwise authorised users from accessing that material. The scope of conduct for which an accused could be said to be reckless in this context is thus limited, albeit in a restricted context.

[63] The approach to addressing unauthorised access within the context of trespass will be explored in chapter 6.

offence itself? It is clearly an inchoate mode offence in that it criminalises the 'causing of a computer to perform a function'. The necessary intent is to secure unauthorised access, but securing unauthorised access is only a crime because section 1 itself makes it so. In that sense, the section 1 offence again cannot be treated as falling within the third category, or even the fourth. While the causing of a computer to perform a function might be considered an overtly innocent act, like those in Horder's fourth category, the section 1 offence only requires the accused possess an intention to secure unauthorised access knowing it to be unauthorised. Conduct, again, only criminalised by operation of the section 1 offence itself.

If we accept Horder's categories as being fundamentally correct, the only option then is to place the section 1 offence within category five: crimes where the intent is, by its nature, ulterior. On this framing, the section 1 offence operates on the same plane as possession offences, general inchoate offences like attempts, or those crimes where the intent requirement extends beyond the immediate conduct. That is, the intent to secure unauthorised access must be regarded as in and of itself the key determiner of wrongdoing. It must be the intention to secure unauthorised access that normatively transforms the character of the conduct: causing the computer to perform a function. But as was explored in chapter 4, the net of 'access' for the purpose of the section 1 offence has been cast exceptionally wide. Additionally, the changing nature of technology and the means by which it is 'accessed' further reduces the barrier to fulfilling the actus of the offence. Can the presence of an intent to secure unauthorised access satisfactorily be relied upon to make an individual's (mis)use of a computer criminally wrongful?

It is here that the interpretation and application of the question of whether an accused's conduct was 'authorised' must be returned to.

III THE LIMITS OF UNAUTHORISED ACCESS?

As was briefly set out in Chapter 3, the role of 'unauthorised access' in the operation of the section 1 offence, in particular, is one that commentators, practitioners, and members of the judiciary frequently confuse: they equate the operation of the offences

with the successful obtaining of access to the computer.[64] Even those that acknowledge the conduct element merely requires the 'caus[ing] of a computer to perform a function', still continue to choose to focus on the notion of a completed access as constituting the offence.[65] This mis-categorisation impacted the interpretation of 'authorisation' in the cases of *DPP v Bignell*[66] which, despite being later disapproved in *R v Bow Street Magistrates Court and Allison, ex parte United States (No. 2)* ('Allison'),[67] is illustrative of this broader conflation.

A *Revisiting the decision in Allison*

It can be recalled from the brief summation in Chapter 3 that *Allison* involved an employee of American Express who used to her access to customer account details to provide credit card numbers to Mr Allison who then participated in the manufacture of forged credit cards. The decision in *Allison* will be considered here in more detail.

> Mr Allison was arrested and charged with conspiring:
>
> (1) to secure unauthorised access to the American Express computer system with intent to commit theft,
> (2) to secure unauthorised access … with intent to commit forgery, and
> (3) to cause unauthorised modification to the contents of the American Express computer system[68]

---

[64] See, eg, Sally Ramage and Edward Wheeler, 'The criminal offence of computer hacking' (2011) 203 *Criminal Lawyer* 3; Martin Wasik, 'Computer Misuse' (1992) 8(1) *Computer Law & Security Review* 25; and Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press, 3rd ed, 2016) 360-369. Most discussion of case law, including by the court itself, resort to using the phrase 'obtaining unauthorised access' despite this not being what the CMA requires.

[65] That the offence merely requires an accused to 'cause a computer to perform a function' opens up a wide array of conduct that now falls within the scope of the section 1 and 2 offences. For example, many modern smartphones contain technology that allows them to sense when they are being picked up, activating the screen and prompting a password request if the user has one set. The fact the smartphone responds digitally to the physical touch is sufficient to establish the requirement that the accused had 'cause[d] the computer to perform a function'. The mere act of powering on a computer is sufficient where the accused ultimately intended to gain access where they know such access is unauthorised.

[66] [1998] 1 Cr App R 1.

[67] [1999] 3 WLR 620.

[68] [1999] 3 WLR 620, 622.

At first instance, the magistrate committed Mr Allison only in respect of the third charge: conspiracy to cause unauthorised modification. In applying the approach to authorisation as originally set out in *Bignell*, the magistrate found that the employee of American Express had the authority to access 'the kind of data' in question, thus could not be said to have secured 'unauthorised access'. The Government brought judicial review proceedings of the magistrate's decision that there was not at least a *prima facie* case with respect to the two counts of the section 2 offence. The Divisional Court, in a judgment delivered by Kennedy LJ, dismissed the judicial review proceedings, but certified a question of law to be considered by the House of Lords that sought opinion on:

> Whether … a person who has authority to access data of the kind in question none the less has unauthorised access if:
>
> a) the access to the particular data in question was intentional,
> b) the access in question was unauthorised by a person entitled to authorise access to that particular data,
> c) knowing [sic] that the access to that particular data was unauthorised[69]

The employee of American Express did not have authority to access the specific account details in question in the circumstances in which she accessed them. Like in *Bignell*, the employee had general authorisation to access the computer system but could only access customer account details when they were specifically assigned to her: any access outside of this process was a breach of company policy. The employee in fact accessed 189 accounts that did not fall within her duties.[70]

As was set out in Chapter 3, the court disapproved of the reasoning used to reach the earlier decision in *Bignell* with respect to the construction of authorisation for the purpose of the CMA. In doing so, the House of Lords developed a three-step approach to assessing the question of authorisation that can be set out as:

> 1. Identify the specific access involved (whether it be to a computer, a system, a particular piece of software, or a set/piece of data)

[69] Ibid 623.

[70] Ibid.

2. Assess the circumstances and degree of any authorisation the individual may have had, and
3. Ask whether that degree of authorisation includes the specific access in question.

Applying this three-step approach to the facts in *Allison*, the American Express employee accessed the account details of particular accounts. The authorisation she had to access the system by virtue of her employment was limited to the set of accounts for which she had responsibility in circumstances where there was a legitimate requirement to effect such access (by virtue of responding to a customer request, or for internal procedures related to account maintenance etc.). This degree of authorisation was the product of organisational policies that were in effect and applicable to the employee, who was aware of those restrictions. The access of the customer accounts for which the employee had no responsibility, in the absence of any circumstances that would legitimate such access, therefore did not fall within the scope of this authorisation. From this it can be observed that authorisation has been interpreted to apply not to the integrity of the computer as a whole (as conceived by the Law Commission),[71] but rather to each and every individual piece of data or software. Thus, the court extended protection to digital 'information' in a manner they were not prepared to do for physical information.[72]

The decision in *Allison* reoriented the approach to authorisation for the purpose of the CMA to be more aligned with the approach in other areas of the criminal law, like in the case of *R v Jones and Smith* ('Jones').[73] *Jones* involved a prosecution for the offence of burglary. The accused, who had general permission to enter his parent's home, went on to enter the house with a friend in the middle of the night in order to steal two televisions. In this instance, in order to establish the accused had committed burglary, it needed to be established that he was a trespasser. Given the accused had a general right of access to the home, as granted by his father, the court developed a notion of 'exceeding permission'. The court observed:

> A person is a trespasser … if he enters premises of another knowing that he is entering in excess of the permission that has been given to him to enter, providing

[71] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [1.29].

[72] See, eg, *Oxford v Moss* (1979) 68 Cr App Rep 183.

[73] (1976) 3 All ER 54.

> the facts are known to the accused which enable him to realise that he is acting in excess of the permission given or that he is acting recklessly as to whether he exceeds that permission.[74]

The decision in *Jones* turned on the scope of the authorisation granted to the accused. While the accused had authorisation to be in the house, it did not follow that he had authorisation to do whatever he pleased once inside the house with his friend, and, specifically in that case, the accused did not have either an express or an implied authorisation to remove the televisions from the house. This is a logical position to adopt. To the extent that conduct might be considered authorised, it must necessarily turn on the context and purpose for which the authorisation was given. This approach has been utilised in other circumstances involving conduct that exceeds the scope of authorisation provided, including the burglary of a store where there was an implied license to enter the store.[75]

If we set the approach in *Jones* alongside the decision of the court in *Allison*, we see a corollary in the result of the two positions: the employee in *Allison* may have been authorised to access computer material, but she was not authorised to access it *for that purpose*. Thus, that access, or any steps taken to secure it, was unauthorised.

However, the approach adopted for the application of the CMA in achieving that result, as set out in the three-step test, might also be interpreted as inverting the framing of the general approach in *Jones*. Instead of beginning with the position that access was granted to all the data, but only for specific purposes which did not include the access the defendant obtained, the default position of the test could be considered reversed: for any given piece of computer material there is assumed no authorisation except where so triggered in the event of there being a justification for accessing it. In the case of *Allison,* this could be understood as there being no default authorisation to access customer records, and instead, such access only became authorised (under the organisation's internal policies and procedures) when prompted by a customer service request

---

[74] Ibid 59.

[75] See, eg, *Barker v R* (1983) 7 ALJR 426, 429 per Mason J 'if a person enters for a purpose outside the scope of his authority then he stands in no better position than a person who enters with no authority at all', but *cf Byrne v Kinematography Renters Society Ltd* [1958] 2 All ER 579.

necessitating such access. Such an approach expands the scope of criminalisation. A company or organisation's internal policies can then be treated as forming the basis of determining whether or not conduct involving computers is criminal.

B Non-harmful unauthorised acts?

The scope of any authorisation to access a computer or data thus becomes a question of technical limitation and general policy or contractual obligations. This approach broadened the possible application of the section 1 offence. In *Ellis v DPP (No. 1)* ('Ellis'),[76] an appeal against three convictions under section 1, a former student of the University of Newcastle upon Tyne who was permitted as an alumnus to use the public-facing computers in the University's library was caught, on occasion, using the computers reserved only for staff and students when those computers had mistakenly been left 'logged in' by a previous legitimate user. The use to which he put these computers was mere browsing of the internet, and there existed no evidence of any intent to commit a further criminal act. However, he was warned by administrators that his use of these computers was against university policy, and this was clearly set out by signage within the library. He persisted. In a later interview, the accused described his actions as being analogous to picking up a discarded newspaper.[77]

In upholding the convictions, Lord Woolf, CJ, stated that the section 1 offence was 'sufficiently wide to cover the use which was made of the computers by the appellant … [and] the appellant was aware that he was unauthorised to use the computers' by virtue of the warnings he received directly from university administrative officers.[78]

This case in particular highlights the operation of the section 1 offence in the context of Horder's categories on inchoate crime. The substance of the section 1 offence does not require harm; it proceeds on the basis that the mere intention to secure unauthorised access is sufficiently wrongful. In *Ellis*, the accused caused a computer to

---

[76] [2001] EWHC Admin 362.

[77] David Ormerod and Karl Laird, *Smith and Hogan's Criminal Law* (Oxford University Press, 14th ed, 2015) 1183.

[78] *DPP v Ellis* [2001] EWHC Admin 362, [16].

perform a function where that function was to access publicly available data available via the internet. His crime was thus using an abandoned active session on a computer in the wrong physical section of the library. While there was clearly a digital trespass in the sense that Mr Ellis made use of a university computing account that did not belong to him, he did not act maliciously in seeking those credentials and made no effort to, nor exhibited anything indicating he manifested an intention to, commit a further offence by virtue of that access. His unauthorised access does not appear, on any account, to represent a sufficient enough transformation to warrant his conduct being regarded as criminally wrongful.

Ellis makes plain that a mere breach of an organisation's policy, regardless of any resulting harm, provides the foundation for assessing the scope of authorisation for the purpose of section 1, especially where technical protection policies fail: in this case with computers being left logged-in. The lack of an ulterior criminal intent, like that found in the section 2 offence, resulted in Mr Ellis' conduct falling neatly within the section 1 offence. He merely had to intend to do the conduct he in fact did; to use the library computer knowing he was not, by operation of university policy, permitted.

The lack of a requirement for a further criminal intent within the section 1 offence can result in an expansive range of non-malicious conduct falling within scope on the basis that it was undertaken without proper authorisation. Consider the following scenario:

> A and B work in a shared office space. It is corporate policy that employees are only permitted to use the computers assigned to their own desks. In the space shared by A and B there is only one printer that is connected to A's computer. B has no such printing access due to a fault but is able to use a printer on another floor. Out of convenience, A informs B that B can forward documents to A to be printed. This works well when both are in the office, but A often does not work Fridays. A tells B that, when she is not in the office, she is happy for B to log-in to her computer to print when necessary. A gives B her access credentials to facilitate this.

In this scenario, despite A granting B permission to access the computer to print, any action B takes will be in contravention of the section 1 offence. A was not in a position to grant access to the computer, as this right belonged to the company who in their policy

documents prohibits an employee from using a computer that is not assigned to them. Despite B acting in accordance with A's instructions, B was aware of this policy. Thus they are on notice that any use of computers beyond the one assigned to them is unauthorised. B's use of A's computer to print a document is a crime. Indeed, the moment B struck the first key of A's access credentials with intent to log-in to the computer to print the document, the offence was complete.

This scenario focused on device-level authorisations. We can take this further by exploring data level authorisations. Suppose a similar agreement exists between A and B, but there is no corporate policy limiting use.

> A advises B that B can use a USB storage drive to transfer files to be printed, but they are not to do anything else with the computer. On this particular day, B does not have a USB drive to hand so instead emails the relevant file to their own e-mail account. B logs in to A's computer and instead of inserting the USB in order to print, as per the scope of their authorisation, B opens the internet browser, access their own e-mail account, finds the file and prints the document.

Here, as above, B has acted in contravention of the CMA's section 1 offence. A had the authority to provide authorisation/consent to the use of the computer, but the scope of that consent was limited to particular physical actions and data processes. Even though the result of B's conduct was the same in either approach, that is the printing of a document they were entitled to print, their conduct in accessing the web-browser and logging into their own email account went beyond the acts contemplated by A. Indeed, as with the first scenario, the moment B began typing the access credentials, intending to open the web-browser rather than insert the USB drive, her actions became criminal. Such is the effect of the standard of 'authorisation' on general-purpose computing technologies; despite the fact the section 1 offence was justified on the basis that it would operate to protect against harm to the *integrity of a computer*.

The focus on both authorisation with respect to the computer system itself,[79] and authorisation with respect to each individual piece of data,[80] raises some further interesting questions. Once a completed 'unauthorised access' of a particular data item has occurred on the part of an accused, if through that access the accused made a copy of that data and stored it on their own computer, who then becomes the person entitled to give authorisation with respect to further access to that data? Does the original owner's interest follow through with each copy made, rendering each further access a potential infringement or breach (like in circumstances where there has been an infringement of a copyright interest[81] or a breach of confidence[82]): or in this case, a further unauthorised access? Or does the mere fact the copy of data is now located on a device owned by the accused entitle them to be considered the individual with 'capacity to give consent' under the CMA?[83]

---

[79] *Computer Misuse Act 1990* s 17(8).

[80] *Computer Misuse Act 1990* s 17(5).

[81] In respect of primary infringement, a causal link must be established to the claimant's work, be it to the original work, or a copy of that work per, eg, *Sawkins v Hyperion* [2005] 1 WLR 3281, 3288. The defendant's knowledge is not considered; see, *Francis Day v Bron* [1963] Ch 587, 619; *Baigent v Random House* [2007] EWCA *Civ* 247. In respect to secondary infringement, the defendant must know, or have reason to believe, their conduct constitutes an infringement of a copyright interest, but such infringements are confined to those engaging in commercial transactions involving the infringing copies; *Copyright, Design, and Patents Act 1988* ss 22-4, 27. In these cases, the knowledge requirement is objective: whether or not the defendant *knew* or *had reason to believe* the conduct was wrongful, but it is not enough to merely *suspect* the conduct is wrongful, see *Hutchinson Personal Communications v Hook Advertising* [1995] FSR 365.

[82] In respect to third parties who obtain confidential information, the question turns on knowledge of the existing obligation of confidence attached, thus making them liable. When aware of the confidential nature of the information at the time of receipt they are bound by the duty of confidence; *Attorney-General v Guardian Newspapers (No. 2)* ('*Spycatcher*') [1990] AC 109, 260 per Lord Keith, 268 per Lord Griffiths. If a person receives information innocently but later learns of its confidential nature, they will also be bound by the duty; *English & American Insurance Company v Herbert Smith* [1988] FSR 232. There remains debate over the substance of the knowledge required, be in subjective as in *Thomas v* Pearce [2000] FSR 718, or objective/constructive in *Campbell v Mirror Group Newspapers* [2004] AC 457. In respect to private information, strangers without any direct relationship to the source of the confidential information will also be liable where there are reasonable grounds to realise that the information was subject to a reasonable expectation of privacy; see, *Douglas v Hello!* [2008] 1 AC 1; *Tchenguiz v Imerman* [2010] EWCA *Civ* 908; and M Richardson, 'Breach of Confidence, Surreptitiously or Accidently Obtained Information and Privacy: Theory versus Law' (1994) 19 *Melbourne University Law Review* 673, 699.

[83] A similar question was recently considered by the Twelfth Court of Appeals District in Texas in respect to the constitutionality of the revenge porn laws in the Texas Penal Code § 21.16(b). The court held the offence was unconstitutional in that it unjustifiably restricted the free speech right of third parties who are not aware of the victim's expectation of privacy in the photograph and had no part in the creation of the photographs, they received them 'innocently'. While decided within a different

This question would only require consideration in circumstances where the third-party *knew* the history of the data, as the section 1 offence criminalises acts of the accused where they *know* any access to computer material they might obtain is unauthorised.[84] Where the third-party had no such knowledge, the offence in section 1 could not be made out. This may be an appropriate response, but the scope of knowledge required on the part of the accused, however, remains relatively untested in the courts even in the context of *direct* contraventions of section 1, let alone the *indirect* possibilities arising above.

Following the decision in *DPP v Lennon*[85], involving the unauthorised sending of millions of emails as introduced in Chapter 3, it would also appear possible that constructive knowledge is sufficient, with the court endorsing the adoption of an objective standard to assess whether the accused ought to have had knowledge that their access was unauthorised in circumstances where there is not a clear indication to the contrary. The court considered how the person in control of the computer material would respond if access of the same kind were requested by an individual in the normal cause of business.[86] This framing seems to imply that in any given context there is a reasonable standard of access that an accused ought to be deemed to have been aware of based on the nature of the computer material in question: that is, constructive knowledge may be sufficient to establish fault. Such a standard is plainly unacceptable within the criminal law. The accused should be required to have actual, subjective knowledge. This issue requires judicial clarification.

---

constitutional context, this case does illustrate that in situations like the one proposed above, the knowledge requirement of the section 1 offence might safeguard against such 'innocent' third parties falling within the scope of the offence when improper authorisation is granted, but, as will be explored below, that the court seems to favour a constructive approach to knowledge on the part of the accused, this may be functional limitation in certain circumstances. See, *Ex Parte: Jordan Bartlett Jones* (12th District Court of Appeals, Texas, No. 12-17-00346-CR, 2018) 7; and, regarding constructive knowledge, see, Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd ed, 2015) 105.

[84] And this point is analogous to the facts in *Collins* [1972] 2 All ER 1105 where the accused was deemed not to be a trespasser for the purpose of the criminal law as he believed himself to have been properly invited into the premise, but in fact, the authorisation came from a person not entitled to offer it.

[85] *DPP v Lennon* [2006] EWHC 1201.

[86] Ibid [9].

C 'Unauthorised access' and ulterior intent?

The normative model established in Chapter 1 suggests that any computer-related offence should include a clear definition of the conduct and culpability within the structure of the offence that is commensurate with the harm or risk of harm that was identified in justifying its creation. Further, without a direct connection with serious harms and risks of harm, an offence ought not to presuppose wrongdoing purely on the basis of a course of conduct: something more is required.

An offence constructed in an inchoate mode ought to incorporate a strict *mens rea* requirement of intent that is capable of being sufficiently criminally wrongful in and of itself, or constructed at the intervals along the logic sequence of a course of criminal conduct such that the presence of the intention to commit a crime can be said to have normatively changed the character of the accused's conduct. While the CMA's section 2 offence provides that the accused must have caused a computer to perform a function with intent to secure unauthorised access knowing that the intended access was in fact unauthorised, it additionally requires proof that the accused did so in order to facilitate the commission of a further offence.

The framing of the section 2 offence thus strikes a balance between Horder's labelling gap. It contains the inclusion of a further ulterior criminal intent requirement, and thus a clear definition of culpability with respect to an identified harm. An accused who causes a computer to perform a function with intent to commit fraud thus commits the section 2 offence, regardless of whether or not their intended fraud occurs. Here, the intention to commit the fraud normatively changes the character of the unauthorised access. It changes from a mere transgression of authorisation to criminally wrongful on the basis that it was carried out in order to commit a further, more serious harm: the fraud.

The section 1 offence does not include such a connection to an identifiable harm. Instead, the section 1 offence presumes that any instance of unauthorised access is in itself sufficiently criminally wrongful such that where an intention to secure access that is unauthorised is evidenced the normative character of conduct involved in causing a

computer to perform a function becomes criminal. Further, that intended access need not be limited to a particular device, nor any data in particular. Moreover, the scope of authorisation can be determined by technical means, policy documents, or verbal warnings.

The section 1 offence, in its inchoate mode, thus represents criminalisation of conduct in a form that is neither commensurate with the spectrum of harm or risk of harm that can result from digital trespass, nor is it limited to the harms identified in supporting its creation: harm to the integrity of a computer. Instead, it operates to presuppose criminal wrongdoing purely on the basis of a course of conduct entered into with an intention to enter into that course of conduct: causing a computer to perform a function to secure access to that computer. Such framing makes it possible that civilly unlawful conduct can be treated as criminal merely because a computer was used. That is, the CMA's section 1 can be understood as treating the use of a computer as the feature that normatively transforms the character of an accused's conduct from civilly to criminally wrongful. The remainder of this chapter explores this in the context of 'bug bounty programs' and the terms of service agreements for online media streaming services as but two examples.

IV BROADER CHALLENGES TO 'AUTHORISATION' – 'BUG BOUNTY PROGRAMS' AND TERMS OF SERVICE AGREEMENTS

The data-level approach to authorisation creates additional issues. For example, with vulnerability reward programs, or 'bug bounty programs'.[87] These programs serve as an incentive for members of the public to report flaws in the operation of online services to the companies responsible for them. Cash rewards are offered, with the value of that reward depending on the severity of the flaw reported.[88] These programs are

[87] 'Bounty programs' exist in a number of contexts, for this brief foray context is limited only to those engaged in by large corporations who pay those who discover security flaws. Other contexts include programs operating for the broader 'open source software' development community who offer bounties for other programmers to write or inspect code for a product or service they are developing, see, eg, Sandeep Krishnamurthy and Arvind K Tripathi, 'Bounty Programmes in Free/Libre/Open Source Software' in Jürgen Bitzer and Philipp J. H. Schröder (eds) *The Economics of Open Source Software Development* (Elsevier, 2006) 165, 170-4.

[88] Matthew Finifter et al, 'An Empirical Study of Vulnerability Rewards Programs' (Paper presented at the 22nd USENIX Security Symposium, Washington DC, United States of America, 14 August 2013).

recognised as good practice for corporations seeking to maximise their *cyber security*, at least by economic theorists who attribute software vulnerabilities and (in)security to market failure.[89]

While becoming more common, participants in these programs are subject to strict compliance conditions. If the enforcement of these conditions by the company can be inherently discretionary when it comes to civil remedy (practicality and economic considerations will dictate recourse to such remedies), the same ought not to be said where participant conduct contravenes the CMA's section 1 offence. Consider the short-lived media hype surrounding recent 'bug hunter' Jani.

On 3 May 2016, Finnish news service *Iltalehti* reported that Facebook had made a USD$10,000 payment to a 10-year-old in Helsinki.[90] The child, Jani, had identified a vulnerability in Instagram's source code.[91] Through exploiting the vulnerability, Jani was able to delete comments posted by any users of the service. Jani's conduct would clearly fall within the scope of section 1 of the CMA. He caused a 'computer to perform a function',[92] he had a clear intent to 'secure access to … data'[93] that he had no authorisation to access at the time he did as the user accounts belong to both Facebook and the individual user for whom that account relates. He would have known that was the case if not from the terms of service, then at least from the design and operation of the service. The 'computer' was Instagram's server, and the 'data' were the user-generated content produced and posted on accounts belonging to other individuals. Here, the question of authorisation leaves some issues open.

---

[89] Taiwo A. Oriol, 'Bugs for Sale: Legal and Ethical Properties of the Market in Software Vulnerabilities' (2011) 28 *Journal of Computer & Information Law* 451.

[90] Alex Heath, *A 10-year-old hacked Instagram and Facebook paid him $10,000* (3 May 2016) Tech Insider <http://www.techinsider.io/10-year-old-hacks-instagram-facebook-pays-him-10k-2016-5>.

[91] Instagram is the social media service owned by Facebook that centres on the sharing of photos and images.

[92] *Computer Misuse Act 1991* s 1(1)(a).

[93] *Computer Misuse Act 1991* s 1(1)(b). Note: the data in question, and any intention to access that specific data, is irrelevant per s 1(2).

A The test for 'authorisation' and the operation of bug bounty programs

As we saw above, the test for 'authorisation' under the CMA following the decision in *Allison* was set out as follows:

> 1. Identify the specific access involved,
> 2. Access the circumstances and degree of any authorisation the individual may have had, and
> 3. Ask whether that degree of authorisation included the *specific access* in question.

Applying this to the case of Jani, Jani gained access to the personal accounts of various users subscribed to the Instagram service. At the time Jani was 'hacking' Instagram, he had no direct authorisation from them to access the service in any capacity other than as a user of the service.[94] However, it might be argued that the existence and offering of the 'bug bounty program' might be interpreted as providing authorisation to attempt to circumvent digital security mechanisms in circumstances where a successful attempt is later disclosed. Indeed, Facebook's 'Responsible Disclose Policy' begins by stating that 'if you comply with the policies below when reporting a security issue to Facebook, we will not initiate a lawsuit or law enforcement investigation against you in response to your report.'[95]

Facebook's terms of service are structured to comply with the United States *Computer Fraud and Abuse Act 1986 (*'CFAA'*),*[96] providing that any intentional violation of laws prohibiting unauthorised access to data does not fall within the ambit of the bug bounty program.[97] The CFAA prohibits the intentional access of a computer 'without authorization' or 'exceeding authorized access' to obtain information from a 'protected computer'.[98] Unlike the CMA, Congress provided no guidance for the interpretation of 'without authorisation' for the purposes of the CFAA, and a number of divergent

---

[94] However, even that is doubtful has any attempt Jani made to access the service would be in breach of the minimum age requirement of 13 years of age as set in Instagram's terms of service.

[95] Facebook, *Responsible Disclosure Policy* (2018) <https://www.facebook.com/whitehat>.

[96] 18 U.S.C. § 1030.

[97] Facebook, *Responsible Disclosure Policy* (2018) <https://www.facebook.com/whitehat>.

[98] Ibid.

approaches have arisen. These approaches include; a 'reasonable expectations' standard based upon the views of the website owner and its user,[99] a subjective 'intended function' test,[100] or, closer to the CMA approach, a permissions test where 'the person has not received permission to use the computer for any purpose … or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway'.[101] The approach to 'exceeding authorized access' has evolved similarly to the UK approach in *Allison*, but was aided by Congress defining the term as 'access[ing] a computer with authorization and … us[ing] such access to obtain or alter information in the computer that the accessor is not entitled … to obtain or alter'.[102]

While a specific and detailed analysis of these tests and their application is beyond the scope of this thesis, importantly for Jani (and Facebook) the question of authorisation only becomes necessary and relevant in relation to a potential prosecution under the CFAA when the accused successfully *gains access,* that is, they must successfully circumvent the security measures in the software, or act in contravention to the terms of service to achieve a level of access beyond that permitted. Where an individual is seeking to participate in the Facebook bug bounty program, any attempt they make to gain access to the service does not risk criminalisation under the CFAA unless they are ultimately successful in gaining that access. The gaining of actual access, in the sense of exercising the ability to control or modify the data, is not necessarily required to qualify for an award under the bounty program: the discovery of a vulnerability that *could* enable such access to be secured is sufficient. It is only when that complete access is obtained that the question of Facebook permitting the activity becomes an issue: with the decision to retrospectively determine whether or not the act in question meets their guidelines, and thus the very criminality of the acts themselves, left to Facebook. This is not the same situation under the CMA.

---

[99] *EF Cultural Travel BV v. Explorica,* 274 F.3d 577, 582 n.10 (1st Cir. 2001).

[100] *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991).

[101] *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127, 1135 (9th Cir. 2009).

[102] *Computer Fraud and Abuse Act* 18 U.S.C. § 1030(e)(6).

As this thesis has highlighted numerous times, the section 1 offence in the CMA does not, in fact, criminalise obtaining unauthorised access to computer material. Instead, it criminalises 'causing a computer to perform a function with intent to secure access'.[103] That is, in contrast to the CFAA, actual access to the computer material (be it the device itself, any software or data contained within it, or the use of a service or platform over a network connection) is not required to enliven criminal liability. Any act that provokes a response from the computer, even the mere typing of an incorrect password, satisfies the conduct elements. Therefore, the question of authorisation in relation to Facebook under the CMA must necessarily cover any initial attempts to find a security vulnerability.

Facebook's bug bounty program only protects those that submit a valid security vulnerability report.[104] Their authorisation of any attempts to find a vulnerability, or circumvent their digital security mechanisms, requires that the report be submitted as a pre-condition to their warranty that they would not initiate a legal response. Thus, a successful submission to a 'bug bounty program' could only be construed as the service providing retrospective authorisation for the conduct. In Jani's situation, had he not successfully found and demonstrated the flaw, his attempts would not have been reported to Facebook and thus not endorsed. Further, in circumstances where an accused is arrested at the time they are attempting to gain access, they have already completed the offence.

The actions of an individual wanting to participate in a bug-bounty program in advance of receipt of any authorisation raises the prospect of criminality for security researchers in the United Kingdom in a way that does not manifest in the United States. By permitting the construction of authorisation to be 'privatised', and effectively contract-based, whether or not the performance of a particular set of actions in one circumstance will be treated as criminal falls to the whim of a private entity.

While the tests as set out in *Allison* use the language of identifying the 'access involved', it must necessarily be the case that the same tests apply in situations where

---

[103] *Computer Misuse Act 1990* s 1(a).

[104] Facebook, *Responsible Disclosure Policy* (2018) <https://www.facebook.com/whitehat>.

complete access was not in fact obtained, especially given the fact that actually securing access is not required to complete the offence. That no such prosecution appears to have been brought yet is of little comfort. In such a case, the test from *Allison* would likely need to be framed with the focus on the 'access intended to be obtained' in limbs one and three:

1. Identify the specific access *intended*
2. Access the circumstances and degree of any authorisation the individual may have had, and
3. Ask whether that degree of authorisation included the *intended access* in question.

Given that the purpose of any access is not relevant to the commission of the offence, applying this framing to Jani had he been identified prior to successfully finding the vulnerability, the specific access he intended to obtain was to the personal accounts and information held by other users. His degree of authorisation was as a user of the service as set out by Instagram's terms of service agreement.[105] The broader Facebook bug bounty program terms, also applicable to Instagram, prohibit the intentional violation of unauthorised access to data laws, proscribes the use of test accounts, and explicitly prohibits the interaction with other accounts without the consent of those users.[106] As written and advertised on their website, therefore, the program does not authorise attempts to obtain access to the personal accounts of others. Jani, having clear access to these terms prior to his actions, and they are again presented during the reporting process, has thus likely committed the section 1 offence.

Perhaps it could be argued that the existence and offering of the 'bug bounty program' ought to be interpreted as an *implied* authorisation to take the steps that he did: the authorisation cannot be *express* as he has not fulfilled the requirements to enliven

[105] Instagram, *Terms of Use* (2018) <https://help.instagram.com/581066165581870?helpref=page_content>.

[106] Facebook does not have the capacity to authorise access to the user account data. That right belongs to the account owner/user. But there is a distinction between the personal data held in respect of the account, and the user-generated content individuals post in their account (which they may colloquially refer to as their private information). This user-generated content and associated intellectual property, again, remains the 'property' of the owner, but the Facebook terms of service claim a 'non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license' in respect of that content (videos and photos), but this requires duplication of the content from the user's account, not the provision of external party access to that account without the owner's express consent. See Facebook, *Terms of Service* (2018) <https://www.facebook.com/terms.php>.

Facebook's retrospective consent. But, such a broad scope of authorisation implied from the mere existence of the 'bug bounty program' would therefore necessarily constitute authorisation of all attempts by 'outsiders' to circumvent the digital security mechanisms, as the offence does not permit taking into account of the motivation of the accused. Any service that operated a bug bounty program (an increasingly common security approach)[107] would, therefore, be outside the scope of the section 1 and, consequently, the section 2 offence. This would run counter to the approach adopted by the court in *Allison,* where authorisation can be limited for each individual piece of data.

The structure of the offence similarly does not permit the consideration of the use to which any data gained through unauthorised access is put. An additional option available to Jani would be for him to attempt to exploit his discovery by selling it on an online market and avoiding reporting his find to Facebook at all.[108] That subsequent act would clearly bring him into the bounds of what was originally envisaged by the CMA. However, as has been illustrated, the section 1 offence makes any achieved 'access' criminal in and of itself, or, more accurately, any attempt to secure access where an individual's actions merely cause the computer to perform a function.[109] Under section 1, the latter circumstances are irrelevant to establishing the necessary conduct elements. Regardless of what Jani did with the data he accessed, he falls within the scope of conduct targeted by the section 1 offence.

However, this stance is inconsistent with the premise above that we can interpret 'authorisation' to allow private entities to retrospectively permit conduct that is otherwise

---

[107] See, eg, Andrew Kuehn and Milton Mueller, 'Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities' (August 1, 2014). 2014 TPRC Conference Paper; Ross Anderson and Tyler Moore, 'The Economics of Information Security' (2006) 314(5799) *Science* 610; Alexander Gamero-Garrido et al, 'Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research' (2017) *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* 1501; but in respect of long term effectiveness of these programs see Thomas Maillart et all, 'Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs' (2017) 3(2) *Journal of Cybersecurity* 81.

[108] Online markets exist, and arguably thrive, on the basis of selling identified software vulnerabilities, alongside markets for selling credit card details and other data of personal or financial significance. The legalities and implications of these markets lie outside the scope of this thesis, but see generally, Lillian Ablon et al, *Markets for cybercrime tools and stolen data: Hackers' bazaar* (Rand Corporation, 2014).

[109] The expansion to cover attempts to access was inserted with passage of the *Police and Justice Act 2006* (UK) s 35(2)(a).

criminal when the information obtained is used in a particular way. To do so is implicitly to acknowledge that not all instances of hacking are uniquely harmful, nor even harmful at all: a foundational justifying tenet of the section 1 offence. Indeed, the offence appears to be premised on the notion that the presence of the intent to secure authorised access is sufficiently criminal wrongful in and of itself. While the notions of 'authorisation' and 'consent' are found elsewhere in the criminal law, none seem to contemplate the retrospective acceptance of the accused's conduct as absolving criminal liability on the part of the victim after the offence has been completed.[110] Indeed, where such conduct is discovered during its commission, or immediately afterwards, such retrospective endorsement would be of little consequence.

It must be acknowledged, of course, that in practice there are many instances of criminal conduct that go undetected or unreported. Nevertheless, from the position of the criminal law, a lack of detection or reporting does not alter the criminal nature of the conduct: this becomes a question of enforcement. The issue for the section 1 offence, therefore, is that it is incapable of effectively differentiating harmful and non-harmful forms of hacking *a priori*. It treats all unauthorised access to computer material as equally harmful.[111] By merely requiring an intent to secure access, no consideration can be given to the accused's motivation.

---

[110] See, eg, in respect of burglary *R v Jones and Smith* (1976) 3 All ER 54; *Taylor v Jackson* (1898) 78 LT 555; but *cf* circumstances where entrance into property was for a dual-purpose or under inducement from a person not entitled to give the authorisation to enter, eg, *Collins* [1972] 2 All ER 1105; and *Byrne v Kinematograph Renters Society Ltd* [1958] 2 All ER 579.

[111] It is arguable that the distinction is taken into account during sentencing. But the experience thus far has been inconsistent at best. Courts have seemingly given emphasis to the broader deterrence arguments in respect of sentencing, and on conviction, sentences have been handed down irrespectively of the scale of conduct engaged in. This is not an issue unique to the United Kingdom, prosecutions in the United States for crimes of theft and fraud involving multiple offenders often see the accused who played the role of the 'hacker' given a disproportionately higher sentence compared to other members. See, eg, *United States of America v Albert Gonzales* (United States District Court, District of Massachusetts, Crim No. 1:09-CR-10382-DPW, 2010) where a co-conspirator (who made an earlier guilty plea despite refusing to cooperate with the investigation into Gonzales) provided the software that enabled the accused to carry out an elaborate credit card scam was ordered joint and severally liable for the entirety of loss incurred along with a two-year prison sentence and three years supervision post release, despite having no knowledge of the accused's intention beyond a general indication it would be criminal and receiving no financial or other benefit from the later fraud. This is not to say a response from the criminal law was not warranted, but rather the sentence appears disproportionate to the level of actual involvement in carrying out the fraud.

Irrespective of the construction of authorisation under the CMA applicable to Jani's scenario, none are reflective nor appropriate for the increasingly standard practice of offering 'bug bounty programs'. Indeed, Facebook and other technology companies routinely reward those who discover flaws in their products that could enable unauthorised actions. In 2015 alone, Facebook paid out USD$936,000 to 210 individuals and researchers: or hackers.[112] It is here that we can see problems with the CMA being constructed to identify mere unauthorised access as harmful conduct warranting criminalisation. Hackers have evolved. So too has the technology they work with. Both are vital to cyber security.

That the section 1 offence does not have the capacity to differentiate modes of computer use that are ultimately beneficial from those that are harmful might have an arguably unintended benefit. In circumstances where an accused is acting maliciously, they might seek to claim that their conduct was undertaken with the aim of participating in the bug bounty program. In this are echoes of the so-called 'trojan horse' defence: where an accused claims a third-party has installed malware on their computer and operated it without their consent, an exceptionally difficult proposition for the prosecution to disprove.[113] That the section 1 offence does not differentiate the purpose of access removes the possibility of this defence, or those like it, gaining improper traction.

It might be further suggested that these issues highlighted above might be overcome by the adoption of a form of pre-registration for participants in the program.[114] While this might seem like a suitable technique to avoid potential criminal liability under section 1, it would make no difference. While the issue of authorisation in respect of Facebook's

---

[112] Reginaldo Silva, *2015 Highlights: Less Low-Hanging Fruit* (9 February 2016) Facebook <https://www.facebook.com/notes/facebook-bug-bounty/2015-highlights-less-low-hanging-fruit/1225168744164016>.

[113] See, eg, *R v Caffrey* (Unreported, Southwark Crown Court, 17 October 2003); *R v Tsolomitis* [2012] SADC 12. See, further, Susan W Brenner, Brian Carrier and Jef Henninger, 'The Trojan Horse Defence in Cybercrime Cases' (2004) 21(1) *Santa Clara High Technology Law Journal* 1; Stephen Bowles and Julio Hernandez-Castro, 'The first 10 years of the Trojan Horse defence' (2015) (Jan) *Computer Fraud & Security* 5.

[114] Microsoft's bug bounty program, for example, requires organisations to pre-register, although this does not extend to individuals. Microsoft, 'Frequently Asked Questions about Microsoft Bug Bounty Programs' (2017) *Microsoft Security Tech Centre* <https://technet.microsoft.com/en-us/security/dn425055.aspx>.

system would be resolved, as introduced above, Facebook does not own the data contained within individual user accounts, they merely have a license to store, process, and pass on that data to parties authorised by the account owner: facts made plain in their terms of service. Any steps taken to access an individual's data by a participant in a bug-bounty program, even where they have registered and gained Facebook's authorisations, would constitute a breach of section 1 where that user has not explicitly consented to that action in respect of the data associated with their account.[115]

The use of bug bounty programs is just one example of routine conduct that runs contrary to the section 1 offence of the CMA, but in placing it alongside the office scenarios explored above, some core observations can be made. At best, the section 1 offence is consistently and completely undermined in a manner not experienced in other areas of the criminal law. The apparent lack of prosecutions of conduct at the level explored here implies this is a theoretical problem, with prosecutorial discretion and public interest considerations preventing criminal sanction in such circumstances. But the risk of prosecution remains. Indeed, other areas where the reach of the criminal law have been expanded, such as inter-child sex offences, and powers of police to compel access to encrypted computer material, have seen the powers used well beyond the intended scope set out by Parliament and law enforcement.[116]

---

[115] Additionally, Facebook's apparent authorisation for access to data they have in law no capacity to authorise might raise the prospect of prosecutions against Facebook for offences in respect of encouraging and facilitating the criminal conduct of participants in the program; *Serious Crimes Act 2007* ss 44 and 46.

[116] See, eg, *Criminal Justice and Courts Act 2015* s 33 regarding the distribution of private sexual photographs and films. The offence does not take into account the age of offenders, thus children engaged in the sending photographs to one another are at risk of being prosecuted as sex offenders before the age of 18 (as well as potential offences under the *Protection of Children Act 1978* s 1(1)). Despite Parliament clearly setting out that children would not be prosecuted, and the CPS guidelines requiring caution and stating that in most cases involving individuals under the age of 18 a prosecution would not be in the public interest, numerous examples of children being charged, cautioned, or otherwise have resulted. See, eg, Thomas Crofts and Eva Lievens, 'Sexting and the Law' in M Walrave et al (eds), *Sexting: Palgrave Studies in Cyberpsychology* (Palgrave Macmillan, 2018) 119; BBC News, 'Sexting boy's naked selfie recorded as crime by police' (3 September 2015) <http://www.bbc.com/news/uk-34136388>; Raymond Arthur, 'Sending a naked selfie can be a criminal offence – but not many teenagers know this' (27 September 2017) *The Conversation* <https://theconversation.com/sending-a-naked-selfie-can-be-a-criminal-offence-but-not-many-teenagers-know-this-84149>; and Kevin Rawlinson, 'Police report sharp rise in sexting cases involving children in England and Wales' (6 November 2017) *The Guardian* <https://www.theguardian.com/media/2017/nov/06/police-report-sharp-rise-in-sexting-cases-involving-children-in-england-and-wales>.

cases under the CMA already exhibit evidence of such reach. *Ellis*, discussed above, essentially involved the accused using computers in the wrong section of the library. *R v Cuthbert*,[117] introduced in Chapter 2, involved the accused merely checking that the website for which he had just donated money as part of a charity appeal was legitimate: he took steps to find out whether or not he himself had been the victim of fraud by seeking to ensure the website he had provided his credit card details was secure. Additionally, the case of *R v Gold and Anor,*[118] explored in Chapter 2 and one of the foundational cases motivating the formulation of the CMA, involved prosecution for conduct which is now characteristic of the behaviour expected of participants in bug bounty programs: the accused pair identified a security flaw that gave them access to parts of the system they ought not have had access, and they reported this to the system operator.

B Terms of Service – streaming copyright protected media

The use of terms of service agreements to regulate and delimit legitimate data access is not found only with respect to bug bounty programmes. Websites and online services are increasingly provided on the condition that a user accepts that their authorisation to make use of the service is to be governed by a terms of service agreement. Contravention of these terms of service makes the use of that service necessarily unauthorised. If indeed such access than falls within the ambit of the CMA's section 1 offence, as seems evidently the case, this can lead to some interesting and questionable policy inconsistencies. Take the provisions of the terms of service associated with the online media streaming services Netflix and the BBC's iPlayer service and the potential criminalisation for terms of service breaches under the CMA as against the policy approach adopted within intellectual property law.

Within their 'Terms of Use' which operates to define and limit the conditions of access to the platform, Netflix provide, at 4.3:

> You may view a movie or TV show through the Netflix service *primarily within the country in which you have established your account* and only in *geographic locations where we offer our service and licensed such movie or TV show*. The content that may be available to

[117] (Unreported, Horseferry Magistrates Court, 29 September 2005).

[118] [1988] 2 All ER 186.

> watch will vary by geographic location and will change from time to time[119] [emphasis added]

Further, at 4.5, Netflix provide that 'You also agree not to: circumvent, remove, alter, deactivate, degrade or thwart any of the content protections in the Netflix service'. Similarly, the 'Terms of Use' in respect of the BBC iPlayer service, provide:

> 3.2.1 If you are outside the UK
> *You may not access, view and/or listen to certain parts of BBC Content (such as video or live television services) using BBC Online Services if you are outside the UK*, although you may, in accordance with the Terms, access and view bbc.co.uk or other websites and listen to some (but not all) BBC radio content. The types if BBC Content that may be available outside the UK will usually depend on the BBC's agreement with the persons who own rights in such content.[120]

These provisions in their respective terms of service are supported and enforced by the use of geolocation techniques: methods of detecting the physical location of a computer or device accessing their service. There are a number of methods by which this can occur, including via self-reporting, account (credit card) data and/or delivery information, identifying a user's Internet Protocol (IP) address, and more advanced techniques including the integration of GPS data and ping response times.[121] Geolocation, in this context, is used as a technical means to protect the intellectual property rights of content creators and facilitate cross-jurisdictional licensing of that content. Were Netflix or the BBC to attempt to license the rights to a particular television show or film to a foreign broadcaster or service, the amount they could charge for such a licensing agreement would be severely limited if citizens of that foreign country were able to access the same content via their respective websites.

These geolocation techniques can, however, be quite simply circumvented by the use of a *virtual private network*, or VPN. VPN's work by encrypting all network activity originating from the computer used by an individual and directing or channelling that activity through a third-party server located in the relevant territory. In this sense, this

---

[119] Netflix, 'Terms of Use' <http://www.netflix.com/TermsofUse>.

[120] BBC iPlayer, 'Terms of Use – Personal' <http://www.bbc.co.uk/terms/personal.html>.

[121] James Muir and Pail Van Oorschot, 'Internet Geolocation: Evasion and counterevasion' (2009) 42(1) *ACM Computing Surveys* 4.

third-party server acts as an 'agent' of the user's computer, acting on their behalf within the network. To the web service being accessed, the requests appear to originate from within the allowed geographic region thus permitting access to the content, which is then forwarded by the 'agent' server on to the user's computer.

For example, a user in Australia can connect to a server based in the United Kingdom (UK) in order to obtain unrestricted access to the BBC's iPlayer service. All communication from the user's computer is directed, or routed, through the server in the UK. The instruction to connect to the BBC's service is sent from the Australian computer to the third-party server in the UK, which then makes the request to the BBC's service. The response from the BBC's service is directed back to the UK server, which then forwards the information on to the Australian computer.

Enacting this form of communication channel is surprisingly easy for everyday consumers, especially given the wide availability of services, including free and paid services (paid services are available for less than £5 per month). A user simply has to download VPN client software from a company offering VPN services and click 'connect'. To enact these capabilities unilaterally is more complex, but detailed instructions and support can be accessed.

VPNs, of course, are a 'dual use' technology. That is, they are not used just to evade geolocation techniques, and indeed are widely used by businesses to improve the security of their own networks by virtue of the encryption technologies employed, create extended networks across geographical locations to facilitate ease of use and increase work productivity, and allow for scalability – as a business grows, so too can its network without prohibitive cost. VPNs are also particularly useful for improving the protection of personal information and data when accessing untrusted public networks (at café's and in public spaces), but also to prevent corporations tracking and amassing data of user behaviour and targeting them with not only advertising but also pricing.[122]

[122] Some airlines, for instance, are known to track user searches and increase the fare prices on subsequent searches for the same travel option, knowing that users tend to search multiple sites simultaneously to make price comparisons.

The actions of a user in Australia making use of VPN to circumvent the geolocation protections on the BBC iPlayer website (or Netflix for that matter) constitutes a clear breach of terms of use agreement. The access, therefore, is unauthorised. Given the user had agreed to the terms of use agreement and they are aware of the geolocation protections thus prompting their use of the VPN, that user has committed conduct likely to fall within the scope of the CMA's section 1 offence. They have committed a criminal offence, potentially punishable with up to two years imprisonment. Criminalisation results from the breach of the terms of use agreement, which itself was constructed to protect intellectual property interests in the material in question. It is necessary, then, to consider what recourse the holders of those same intellectual property rights would have under intellectual property law itself given that there is now a criminal law response protecting those same interests by virtue only of the fact that a computer is involved in the breach of those rights.

Aside from the apparent operation of the CMA's section 1 offence, an individual user who infringes copyright through the obtaining of unauthorised digital copies of a work does not commit a criminal offence. Despite obtaining access to a work for which they may have made no payment or contribution, and without the permission of the copyright owner, they have not committed theft for the purposes of the *Theft Act 1968*,[123] nor is fraud likely to be established.[124] Further, the *Copyright, Designs and Patents Act 1988* incorporates criminal sanctions that apply only to those who infringe in the 'course of trade',[125] thus it is the providers of services that facilitate the infringement of copyright that a potentially liable for criminal sanction under that act, but not individuals who commit what is otherwise characterised as the civil infringement of copyright.

To the layperson who pays for a subscription to Netflix and accesses content available in another geographic territory by way of a VPN, or the person who accesses

---

[123] The current law, as noted earlier in the thesis, excludes information and, by extension, data from the definition of property; see, *Oxford v Moss* (1979) 69 Cr App R 183.

[124] See, Jeff Vinall, 'The Criminal Law's Treatment of Twenty-First Century Copyright Pirates: A Treacherous New Frontier for Property Offences' (2013) 2 *Oxford University Undergraduate Law Journal* 57, 63.

[125] *Copyright, Designs and Patents Act 1988* ss 107(1)(c) and 107(2).

otherwise freely available content on the BBC iPlayer service, the original content creators and owners are being monetarily compensated through the purchase of the service subscription, regardless of the location from which that content is accessed. Such a position, although common, does not take into account the interests of various territorial stakeholders who purchase licence and distribution rights for their market, and upon which their survival within the content industry rests. There is a normative distinction, then, between content streamed inappropriately but in the context of monetary consideration being provided to copyright orders (albeit not through the correct channels), and more traditional forms of 'file-sharing' where complete copies of copyright work are shared and distributed without any monetary consideration. When attention turns to criminalisation, this distinction produces untenable outcomes. File-sharing is not criminal.

The robust protection of intellectual property is considered highly economically important, although a convincing case has yet to be made that this should extend to the criminalisation of infringement by individuals. Arguments of the impact of the scale of file sharing are yet to justify the imposition of criminal sanctions on the individual. It is therefore questionable that the operation of the CMA's section 1 offence seemingly makes it a crime to stream content obtained through the purchase of a subscription to that material when done in contravention of a terms of use agreement. In this instance, a user who believes that they are appropriately compensating copyright owners for access to their material becomes liable for criminal prosecution for temporally restricted access, but a user who offers no monetary payment and obtains a copy of the file through file-sharing services for use at any time faces no such liability. The user who downloads an infringing copy of the content from an otherwise unrestricted website has not obtained unauthorised access.

The Australian who uses a VPN to stream content from BBC iPlayer commits the CMA's section 1 offence in respect of the access itself, and is additionally civilly liable for breach of copyright under Australian law, as well as the computer misuse offences of the State in which they reside (most of which were themselves modelled on the CMA's section 1 offence). The same is true in reverse: where a UK citizen accesses content from the

Australian Broadcasting Corporations iView service.[126] However, if they had instead accessed a 'piracy' facilitating service, such as the PirateBay, and downloaded a copy of the very same television show or movie, each has committed merely a breach of copyright in their respective territories. Here, it is the person or persons operating the PirateBay that have committed the criminal offence in facilitating copyright infringement in the course of trade.

The scope of the section 1 offence, and its reliance on the concept of 'unauthorised access' as the key determiner of whether conduct becomes criminal or not, has overridden the careful balancing and justifications vis-à-vis the line between civil penalty and criminalisation within intellectual property law. While focussed and targeted policy consideration within the realm of intellectual property law have resulted in the line being drawn high before resort to the criminal law is deemed appropriate, the isolated focus of the CMA in seeking to protect merely the 'integrity' of computers and data, however and in whatever context they are used, has seen those policy considerations effectively overridden.

V Conclusion

When the CMA was first introduced, Peter Alldridge raised the core substance of some of the issues discussed throughout this chapter with the drafting of the section 1 offence by exploring its application in the context of a physical burglary of a property with an outdoor sensor light.[127] As a burglar approaches the house, her movements

[126] In respect of the criminalisation of VPN use, the knowledge requirement of the section 1 offence gains particular significance. In the examples above, the user clearly knows that their use of the VPN is circumventing geolocation protection mechanisms. But what of the VPN user who accesses the above media services while the VPN is unintentionally active? Suppose an employee is travelling abroad and using their employer's VPN to undertake their work duties. When complete, the employee forgets to disconnect from the VPN and later proceeds to access Netflix. Here, they have clearly intended to access the service; the question is, did they know their access was unauthorised by virtue of the operation of the VPN? This ought not to be assessed on the basis of whether or not they knew access to Netflix by way of a VPN was in contravention of the terms of service generally, as that would necessarily be answered in the affirmative: they agreed to be bound by the terms of service. It would need to be assessed as to whether they knew that specific access was unauthorised, that is without realising the VPN was active: that is, did they have a reasonable belief their access was authorised. This, however, gives further weight for the need to clarify the reasoning of the court in *Lennon* vis-à-vis the subjectivity of the knowledge requirement.

[127] Peter Alldridge, 'Computer Misuse Act 1990' [1990] 9(6) *International Banking Law* 339, 400.

activate the light, which makes it more likely she will be observed: the risks associated with undertaking the burglary increase. Thus, she may be dissuaded from continuing her intended activities at that particular house. But, in so triggering the light to activate just with her mere presence, despite not ultimately gaining access to the house, the burglar has 'caused the lights to perform a function.'[128] Alldridge set out this example in 1990 to make the point that in other circumstances we would not regard the mere activation of a function sufficient to establish criminality.

However, since the time of his observation there are now 'computerised' lights that have developed into a form that may actually qualify as 'computers' themselves for the purposes of the CMA in that they are electronic devices capable of sending, storing and processing data.[129] Therefore, the activation of a WiFi-enabled sensor light might now qualify as 'causing a computer to perform a function'. The very abstraction made by Alldridge to illustrate the absurdity of the construction of an offence in this manner has arguably come to fruition.

In its broadest sense, the CMA's section 1 offence, in treating all computing technology and 'unauthorised access' in the same context, effectively criminalises the mere presence and use of computers, irrespective of any resulting or potential harm and without requiring a wrongful intention beyond the securing of the unauthorised access. While section 1 does require an intent to secure access while knowing that such access was, in fact, unauthorised, that intent does not have to be directed at any particular program or data,[130] or even any particular computer:[131] in effect, the intention to secure access is satisfied by the mere existence of the conduct that established that the accused caused the computer to perform a function. This situation is the result of the inchoate mode drafting adopted in the structure of the offence.

---

[128] Ibid.

[129] *DPP v McKeown*, *DPP v Jones* [1997] 2 Cr App R 155, at 163 per Lord Hoffman.

[130] *Computer Misuse Act 1990* s 1(2)(a).

[131] *Computer Misuse Act 1990* s 1(2)(b).

Swinging a baseball bat is not in itself a crime. But, add to the mix a person who is the target of the swing,[132] or an item of property,[133] and criminality arises. To restate the position of Horder set out at the start of this chapter, it is the presence of the criminal intent that changes the normative significance of the accused's conduct: the existence of criminality turns on any combination of the context in which the bat was swung, the intention of the person swinging the bat, or any resulting harm or damage. The section 1 offence operates with respect to computers in the same manner as if it were to be a criminal offence merely pick up the baseball bat intending to swing it, irrespective of the context of the swing.

This over-inclusiveness, if properly constrained by prosecutorial discretion, might nevertheless be *politically* acceptable if the section 1 offence is applying to conduct no otherwise dealt with in the context of the broader 'cyber' regulatory framework. Assessing whether or not this is the case is the subject of chapter 6.

[132] At a minimum this is a clear battery contrary to *Criminal Justice Act 1988* s 39, and, depending on the nature of injury, possibly an assault occasioning actual bodily harm contrary to *Offences Against the Person Act 1861* s 47, with actual bodily harm defined as 'any hurt or injury calculated to interfere with the health or comfort of the victim' where not 'transient or trifling' *Donavan* [1934] 2 KB 498.

[133] *Criminal Damage Act 1971* s 1. However, where the accused had an intention to use the bat to destroy the property, mere possession of the bat for that purpose might satisfy the offence proscribed in section 3 – possession with intent to destroy or damage. The intent to use the item to cause damage (in this case the bat) need only be established in respect of an intent to use it *at any time* or *when necessary*: *R v Buckingham* (1976) 63 Cr App Rep 159.

Chapter 6

COMPUTER MISUSE WITHIN THE BROADER 'CYBER' REGULATORY FRAMEWORK

There's no silver bullet solution with cyber security, a layered defence is the only viable defence

JAMES SCOTT[1]

I INTRODUCTION

While Chapter 4 and 5 set out the potential for the CMA's section 1 offence to be over-inclusive in respect of the scope of conduct for which it applies, particularly in respect of the degree of potential overlap across the logic sequence of hacking, such over-inclusiveness may nevertheless be appropriate where the offence operates across a spectrum of conduct not otherwise addressed but for the operation of the offences contained within the CMA. However, while the CMA's section 1 offence, with its purportedly technology-neutral drafting and conception of the integrity of computers and

[1] Senior Fellow at the Institute for Critical Infrastructure Technology.

data as a suitable harm to guard against and respond to by way of the criminal law, has remained substantially unchanged, the same cannot be said of computing technologies and the development of our understanding of the evolving computer crime landscape. Other general criminal offences, like fraud, have been substantially amended to include conduct enabled by computing technologies, and new (or substantially revised) civil regulatory schemes, like the *General Data Protection Regulation* ('GDPR'),[2] have also developed over the decades since the CMA came into force.

This chapter, therefore, seeks to place the potential over-inclusiveness of the CMA's section 1 offence, set out in chapters 4 and 5, alongside these developments. It begins by exploring the developments in the field of cybersecurity, within which computer misuse instinctively falls. New cross-disciplinary approaches are emerging to respond and manage the risks to the security and integrity of computer systems and networks, including the tracking and mapping of the cybersecurity threat landscape. This mapping involves collating reports of experiences and detection of malicious conduct, as well as providing advice on the scale of that behaviour as well as identifying trends in its prevalence throughout Europe and the world. As part of this analysis, the structure and operation of the CMA's section 1 offence in the context of the broader data protection regime, the GDPR in particular, is explored.

While not a comprehensive review of 'data protection', the chapter sets out to establish that the rise of civil data protection regimes work to create an incentive for those operating computer, platform and network services, to create ever more explicit terms of service agreements, exacerbating the section 1 offence's potential for over-inclusiveness by expanding the conduct capable of being considered 'unauthorised'. The chapter brings this to light in the context of the recent decision by the United Kingdom's Information Commissioner's Office decision to prosecute an individual by way of the CMA's section 1 offence for a data protection breach, with its provision for

[2] *European Parliament Regulation 2016/679/EU of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing of Directive 95/46/EC* ('General Data Protection Regulation) [2016] OJ L 119/1.

imprisonment, in place of pursuing a data protection offence punishable by way only of a fine.[3]

The chapter then maps the operation of the CMA offences and other general criminal offences along the 'cyber kill chain', the military-inspired model established by Lockheed-Martin to understand the stages of a 'cyber-attack', a similar approach to the logic sequence of hacking established in Chapter 5. Focus then shifts to consider these developments in the context of the taxonomies of computer crime that began emerging in the field of criminology in the mid-90s. Initially, computer crime was sought to be understood and categorised based on how the use of the 'computer' facilitated the crime in question; was the computer a tool to enable criminal behaviour, itself the target of criminal behaviour, or was its use merely incidental to criminal behaviour. These models have since evolved to include concepts of offender motivation and resulting potential harms.

The purpose of this chapter is not to comprehensively explore the full spectrum of either the criminal law or the evolving landscape of cybersecurity threats. Instead, this chapter serves the role of providing an initial survey and summary of the possible general application of criminal offences alongside those offences within the CMA to identify the scope of overlap. Further, and more comprehensive analysis is required, but falls beyond the scope of this thesis.

II THE CYBERSECURITY THREAT LANDSCAPE

As argued throughout this thesis, the CMA's section 1 offence, in providing no means to assess the motivations of an accused, presupposes harm from the conduct. Nevertheless, this may still be defensible if the threat of mere unauthorised access is sufficiently serious and there remains no, or limited, other recourse or response for victims in the civil or criminal law. To understand whether or not this is the case, it is necessary to articulate what those threats are. It is also necessary to have a framework to measure and assess the potential harms. Given the global scale of computer-related crime, enabled by the nature of the internet, this is an exceedingly difficult task, and one yet to be fully

[3] *Information Commissioner v Kasim* (Unreported, Wood Green Crown Court, 12 November 2018).

undertaken. There are, however, useful examples and approaches that can prove illustrative for the purpose of domestic criminal law, such as the annual reports produced by the European Union Agency for Network and Information Security ('ENISA').

A *ENISA*

Originally established by *Regulation (EC) No. 460/2004*,[4] and headquartered in Heraklion, Crete, the ENISA is tasked with assessing the security of electronic communication infrastructure and services of European Union Member States, to provide advice to Member States on the implementation of, and compliance with, various Network and Information Security Directives,[5] to facilitate cooperation between Member States, and to provide 'systematic forecast of future developments, challenges and threats'.[6]

The agency's efforts, in respect of these latter objectives, centre on the collection and analysis of data in relation to security incidents across Europe and the world, promoting risk assessment and risk management methods to governments and industry, working and communicating with Computer Emergency Response Teams ('CERTS'), and building public-private partnerships. Since 2012, one aspect of ENISA's efforts to fulfil these, admittedly ambitions, obligations has been the production of an annual 'Threat Landscape Report'. While the Agency itself has more broadly been the subject of uncertainty and criticism, largely under-resourced and at times used as a political plaything,[7] the annual report remains a useful tool as an effective summary of publicly available cyber threat intelligence.

---

[4] Following review, ENISA has since been renewed and re-established under Regulation (EU) No. 526/2013.

[5] Regulation (EU) No. 526/2013 Article 18. This includes Directive EC/2002/21, Directive 2002/58/EC and Directive EC/94/46.

[6] Regulation (EU) No. 526/2013, Articles 2-3.

[7] For example, prior to the recent implementation of the *Parliament and Council Directive EU/2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* [2016] OJ L 194/1, referred to at the NIS Directive, a dispute arose with respect to the creation of a cybersecurity certification scheme that that directive contemplated falling within the ambit of ENISA, but this was opposed by France and Germany whose domestic agencies dwarf ENISA in both size and capability.

1 The ENISA Threat Landscape Report

Aimed predominantly at risk managers, security professionals and policymakers in both the public and private sphere, the ENISA Threat Landscape Report ('the Report') seeks to consolidate and contextualise publicly available cyber threat information from a multitude of sources. While the initial 2012 report drew information from ~150 government and industry sources,[8] the 2018 report is the culmination of reviewing hundreds of sources of information relating to the experience of cyber threats, and actual cyber-attacks.[9] These sources being those produced within the 'reporting period' upon which the conclusions in the report are based. That is, sources for the 2018 report included only those produced between December 2017 and December 2018.[10] The report is written within the context of the growing importance of identifying trends in cyber-threats and understanding the evolution of cybercrime,[11] a key strategic objective of the European Union and United Kingdom's respective Cyber Security Strategies.[12]

While not directly a report based substantively on the mapping of computer-related crime, indeed its focus is on broader security considerations, the Report provides a useful framework for understanding the use of various techniques and technical exploits that pose substantial risks to each Member State's network and information security. Techniques and technical exploits that, unsurprisingly, underpin a multitude of activities constituting criminal conduct in and of themselves, or used in the commission of criminal

[8] European Union Agency for Network and Information Security, 'ENISA Threat Landscape Report 2012' (2013) available at <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/ENISAThreatLandscape>.

[9] European Union Agency for Network and Information Security, 'ENISA Threat Landscape Report 2018' (2019) available at <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>.

[10] Ibid 10.

[11] Ibid.

[12] See, eg, HM Government, 'National Cyber Security Strategy 2016 to 2021' (2016) <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>.

acts, are identified on the basis of prevalence within the broader context of cybersecurity.[13]

The Report cannot, however, be relied upon without first addressing some issues with its methodological approach and presentation. Given the wealth of sources dealt with, the Report indeed draws from a comprehensive information set, but it becomes difficult to draw comparisons between the threats focused on given the disparities and lack of consistency between data sources. This is not a factor exclusive to this Report and is indeed endemic of reports in this area given the difficulty in obtaining accurate data, and more so given the lack of the adoption of consistent and uniform metrics in which to assess such data. Additionally, these disparities in data source and quality result in the Report containing within it many contradictory assertions in relation to the prevalence, and ultimately the 'ranking', of the threats identified.

For the purpose of this analysis, however, the methodological shortcomings of the Report have limited impact. The point here is not to construct analysis around empirical observations of the law's capacity to respond to the 'number one' or 'top five' cyber threats, but instead seeks to undertake a thematic assessment of the law's ability to address the broadly identified trends within the Report. The Report also presents a comprehensive and independent review of available data from both within the EU and around the world. The analysis within the Report is seemingly not impacted by outside considerations, unlike other security industry vendor and vendor-independent surveys/reports. These industry surveys tend to rely on various direct reporting mechanisms between business customers and the organisation producing the survey. While useful to obtain a general sense of the cyber threat landscape, these surveys are generally designed and presented to further commercial interests, limiting the potential usefulness of each as a basis for research when considered in isolation.[14]

---

[13] There are a multitude of actions where computers intersect with the criminal law in the UK – the Audit Commission report of 2005 identified Fraud, Hacking, Invasion of Privacy, Sabotage, Theft, Use of unlicensed software, private work, Virus/Denial of Service, accessing pornographic/inappropriate material, but did not consider APTs, Botnets, Phishing, or State-sponsored attacks.

[14] See, eg, Symantec, '2019 Internet Security Report', *Symantec* (2019) <www.symantec.com/en/uk/security-center/threat-report/>; Thales, '2019 Thales Data Threat Report – Global Edition', *Thales* (2019) <www.thalesesecurity.com/2019/data-threat-report/>.

Another consideration in relation to the detection of 'trends' in relation to cyber-threats and computer-related crime more generally, echoing the question posed by Wall above, remains the open question of whether the incidence and prevalence of computer-related crime and associated threats are in fact actually increasing, or if our detection and reporting mechanisms are just improving.

(a) Identified threats and the criminal law

The 15 particular threats named in the Report are identified as; malware, web-based attacks, web application attacks, phishing, denial of service, spam, botnets, data breaches, insider threats, physical manipulation/damage/theft/loss, information leakage, identity theft, crypto-jacking, ransomware, and cyber espionage. This does not, however, represent 15 threat *types*, as, for example, crypto-jacking and ransomware rely on specialised forms of malware, and identity theft is a special category of data breach, representing a particular use of the data so obtained.[15] Therefore, for the purpose of this discussion, the threats identified by ENISA will be grouped thematically into six categories; malware; denial of service attacks; phishing and identity theft; data breaches, insider threats and information leakage; physical manipulation/damage; and cyber espionage. The purpose here is to consider what criminal offences are available to prosecute conduct under each cyber threat 'theme', or, where appropriate, avenues for remedy elsewhere in the law.

(i) Malware

Malicious code, or malware, has been described as 'code [that] can act like an inside agent, carrying out the dastardly plan of an attacker inside your computer'.[16] While a relatively simplistic definition, it does indeed encapsulate the purpose of malware: to do

[15] ENISA (n 9) 25.

[16] Ed Skoudis and Lenny Zeltser, *Malware: Fighting Malicious Code* (Prentice Hall Professional, 2004) 3.

harm[17] through causing varying degrees of interruption and/or damage.[18] The term malware can include viruses, worms and Trojans, amongst others.[19] In general discourse, these terms are often used interchangeably, but while there are differences in their operation and intention, these differences are becoming less significant even from a technical perspective.[20]

The Report describes malware as the most frequently encountered cyber-threat, being involved in 30% of identified data breaches.[21] Advancements made in encryption techniques are making the detection of malware ever more difficult, and malware is increasingly being developed to be directed at mobile and Internet of Things devices.[22] Further, while ransomware continues to be prevalent, there has also been a rise in 'crypto-jacking'.

Ransomware is a form of malware that operates to gain control of a user's computer, device or network in order, in doing so, to prevent legitimate users from accessing or using their data (either by encryption or some other means) unless a fee is paid to obtain a code that will 'unlock' their device. As the name implies, devices are held to digital ransom[23]

---

[17] Kurt Fanning, 'Minimizing the Cost of Malware' (2015) 26(3) *Journal of Corporate Accounting & Finance* 7, 9.

[18] Such software can serve a variety of purposes from simply displaying messages on the screen, to the exfiltration or destruction of data.

[19] There is a multitude of differing types of viruses and worms that engage a variety of techniques that target many different aspects of computing hardware and software: for a brief introduction see <http://www.webopedia.com/DidYouKnow/Internet/virus.asp> accessed on 21 June 2015.

[20] See Joseph Audal, Quincy Lu and Peter Roman, 'Computer Crime' (2008) 48 *American Criminal Law Review* 233; M Klang, 'A critical look at the regulation of computer viruses' (2003) 11 *International Journal of Law and Information Technology* 162.

[21] ENISA (n 9) 26.

[22] Ibid 26-7.

[23] See Greg Bangs, 'New Ransomware and Cyber Extortion Schemes Hold Businesses Hostage' (2014) 61(8) *Risk Management* 30.

Malware and ransomware clearly fall within the ambit of the CMA's section 3A offences – the making, supplying or obtaining articles for use in offences under section 1, 3 or 3ZA. However, the section 3A offence applies only where the article (the malware) is made, adapted, or supplied,[24] or obtained[25] with the intention to commit one of the above-listed offences under the CMA itself, or believing such use to be likely.[26] It would not seem to extend to circumstances where the accused's intention is instead to commit another general criminal offence. However, this is not a problem in respect to establishing an intention to commit, or being reckless as to the commission of, the section 1 offence, given its broad scope of application and weak intention requirement. Similarly, the section 3 offence is clearly enlivened with its application to conduct undertaken recklessly as to whether an act might impair a computer[27] or the operation of any program or data,[28] or to prevent and hinder legitimate access (use).[29]

Nevertheless, ransomware is also prosecutable as the offence of blackmail, and in some circumstances as fraud by false representation. Indeed, these charges have been successfully brought against offenders making use of ransomware. In *R v Qaiser,*[30] the accused undertook a substantial number of ransomware attacks on unsuspecting users of pornography websites. After clicking on an 'infected' pop-up advertisement that the accused caused to appear on their computers, the victim's computer would become 'locked' and they would be presented with a message purporting to be from the United States Federal Bureau of Investigation demanding immediate payment of a 'fine', without receipt of such payment their computers would remain non-functional. Using this method, the accused had profited in excess of £500,000 between 2012 and 2014. Following investigation by the National Crime Agency, the accused was charged with,

[24] *Computer Misuse Act 1990* s 3A(1).

[25] *Computer Misuse Act 1990* s 3A(3).

[26] *Computer Misuse Act 1990* s 3A(2).

[27] *Computer Misuse Act 1990* ss 3(3), 3(2)(a).

[28] *Computer Misuse Act 1990* s 3(3), 3(2)(c).

[29] *Computer Misuse Act 1990* s 3(3), 3(2)(b).

[30] *R v Qaiser* (Unreported, Kingston Crown Court, 8 April 2019).

and admitted, three counts of blackmail,[31] three counts of fraud by false representation,[32] four counts of conduct contrary to the CMA section 3 offence, and one count of possessing criminal property (for later acts of money laundering).[33] He received a sentence of imprisonment for six years and five months.

While *R v Qaiser* has been reported as being described by the National Crime Agency as 'the most serious case of cybercrime it has investigated',[34] it is not the first, or likely last, case to involve prosecution for blackmail and fraud alongside prosecution for conduct contrary to the CMA. The first case under the CMA for conduct also involving blackmail, albeit in respect of an application for habeas corpus in the face of an extradition request from the United States, occurred in *Zezev and Yarimaka v Governor of HM Prison Brixton.*[35] Zezev had been employed by a company that had subscribed to news and financial services provided by Bloomberg LP, operating out of New York. The applicants had gained access to the Bloomberg internal network and undertook to blackmail Mr Bloomberg by sending emails purporting to be from the company's head of security demanding payment in return for not going public and disclosing that the network had been compromised. While argued only in respect to the CMA's section 3 offence, given the nature of the extradition request, the conduct here falls equally comfortably with the offence of blackmail and fraud by false representation. Given the pair were operating in concert, charges of conspiracy to commit blackmail or fraud were also available.

The same pattern of conduct can be observed in *R v Rees*[36] which involved an accused who, operating as a self-styled 'paedophile hunter', pretended to be underage

---

[31] Contrary to *Theft Act 1968* s 21.

[32] Contrary to *Fraud Act 2006* s 2.

[33] Contrary to *Proceeds of Crime Act 2002* s 329(1)(c).

[34] Press Association, 'UK hacker jailed for six years for blackmailing pornography site users', *the Guardian*, (9 April 2019) <https://www.theguardian.com/uk-news/2019/apr/09/uk-hacker-jailed-six-years-blackmailing-pornography-website-users>.

[35] [2002] EWHC 589 (Admin).

[36] (Unreported, Cardiff Crown Court, 26 June 2015).

girls in chatrooms in order to elicit the exchange of indecent images from men (who believed the accused to be a teenage girl). The photos he provided to the men in return were infected with a type of concealed malware that would enable him to access their computer in order to obtain their personal details which he then used in order to blackmail the men involved on pain if being reported to the authorities for their conduct in soliciting someone they believed to be underage. And again, in *R v Kelley*[37] where the accused was one of 6 people (under the age of 21) who had gained access to the customer details of the telecommunications company TalkTalk and then demanded payment from the company in the form of 465 bitcoin (at the time worth approximately £90,000) in return for not releasing their customers details publicly. The accused also obtained data from TAFE Queensland and RC Hobbies in Australia, in respect of the latter demanding payment of 15 bitcoin. He pleaded guilty to 11 counts of conduct contrary to the CMA, blackmail, fraud and money laundering. However, a further eight charges, including additional counts of blackmail, were left on the file with the CPS stating it was not in the 'public interest' to proceed to trial on those counts.

The essence of the conduct engaged in by the accused in each of these cases falls well within the operation of the offence of blackmail, and indeed such charges were pursued. That they used computers and malware to give effect to their 'unwarranted demand with menaces' meant each had additionally acted contrary to the offences within the CMA. Moreover, at least more clearly in the case of *Kelley*, guilty pleas to those offences contrary to the CMA, given their breadth, can result in additional more serious charges being abandoned. Nevertheless, malware, when used as a tool in this fashion, clearly falls within the scope of the general criminal law offences of blackmail and fraud.

Crypto-jacking, however, does not fit quite so neatly. Crypto-jacking involves the 'high jacking' of a computer's processing power such that it can be used to 'mine' cryptocurrencies. The user of a website or service, or the victim of a malware infection, may experience their computer operating at a slower speed while the processing power is utilised by a third-party to undertake a series of computational tasks required by cryptocurrency platforms, such as Bitcoin, to continue operating. The completion of

[37] (Unreported, Central Criminal Court, 13 December 2016).

these tasks requires substantial computational resources and are therefore rewarded by a payment to those who contribute in the form of that same cryptocurrency, which can be exceptionally valuable. The issue at the core of crypto-jacking, then, is the unauthorised exploitation of the computational resources of the legitimate owner of the device, where the third-party is the person set to benefit financially from the exploitation of the victim's computational resources.

While no prosecution for crypto-jacking appears to have occurred at the time of writing, a number of criminal offences could be pursued. This type of conduct is clearly in contravention of the CMA's section 1 offence, as well as the section 3 offence: regardless of whether the crypto-jacking is executed by way of malware or via a website, the resulting 'slow-down' in the computer's performance would likely be deemed an 'impairment' for the purpose of the section 3 offence. Where malware is caused to be installed on the victim's computer, then the section 3 and 3A offences are clearly applicable.

However, where the crypto-jacking is carried out entirely by virtue of the victim accessing a website or service, while the section 1 offence would *prima facie* apply, it could easily be circumvented or negated through the inclusion of the underlying 'use' of the user's computer as a condition in the terms of service agreement governing the 'victim's' access to the website or service. Indeed, this approach has already been adopted by some media companies, on a trial basis, in lieu of charging users a subscription fee.[38]

Beyond the offences in the CMA, a charge for the dishonest abstraction of electricity is likely possible.[39] The third-party is clearly acting dishonestly and without the

---

[38] See, eg, John E Dunn, 'Watch our ads or we'll use your CPU for cryptomining', *naked security by SOPHOS* (14 February 2018) <www.nakedsecurity.sophos.com/2018/02/14/watch-our-ads-or-well-use-your-cpu-for-cryptoming/>.

[39] *Theft Act 1968* s 13. There is, of course, much criticism of the utility of this charge, particularly in respect to the quantification of the amount of electricity alleged to have been abstracted: non-processing intensive computing operations use what courts have traditionally regarded as trivial amounts of electricity. See *R v Siu Tak Chee* (Unreported, Hong Kong, August 1984) as cited in Tasmanian Law Reform Commission, *Report on Computer Misuse* (Govt Printer, Hobart, 1986) 23. In that case, the defendant's actions constituted the abstraction of electricity worth less than one-eighth of a Hong Kong cent. The Magistrate unconditionally discharged the defendant, observing that the prosecution should not have been brought.

authority of the computer owner making use of the electricity powering the device. Indeed, such a charge might in fact better label and reflect the harm experienced by the victim: they are paying the bill for the electricity used to generate the crypto-currency which profits only the perpetrator. Alternatively, or additionally, in circumstances where the victim has been induced to believe the site they are accessing is genuine, a charge for fraud by false representation may be possible.[40] Here, the third-party clearly intends to make financial gain by dishonest use of the victim's computer, liability will turn on the nature of the 'representation' identified. It should be noted, however, that it is sufficient for any such representation to be implied.[41]

While the CMA's section 1's application to crypto-jacking has the opportunity to be contractually negated, its application, in general, appears not to be 'plugging a gap'. Crypto-jacking is seemingly likely to be adequately covered by the more serious CMA offences, and potentially, in many instances, by fraud.

Whatever form a particular piece of malicious code takes, it appears that all aspects of its creation, use and implementation fall within the scope of the CMA's section 3A offences. The creation and implementation of malicious code is a typical precursor to malicious computer activity: for example, gaining control over other computers to create a 'botnet' (a network of devices infected with malicious code that can be utilised without the owner's consent)[42] from which to launch a 'DDoS attack':[43] in circumstances where such an attack occurs, the attack itself tends to be the focus of prosecution rather than the

[40] *Fraud Act 2006* ss 1, 2(1).

[41] *Fraud Act 2006* s 2(4).

[42] ENISA (n 9) 57. Botnets were identified as a significant threat in the report, but recently experiencing a downward trend, due to recent successful law enforcement action in disrupting such networks: in particular ZeroAccess. However, the total takedown of botnets is not feasible. Additionally, as explored in Chapter 4, botnets have been evolving to also make use of smaller devices, such as routers, sensors and 'Internet of Things' devices.

[43] Ibid 47.

preparatory acts. These preparatory acts, however, necessarily involved the creation, use and distribution of malicious code.[44]

Possession of malware, or the making or supply of malware is also potentially criminalised by the *Fraud Act 2006*. Section 6 makes it an offence to possess or have under one's control an article for use in the course of or in connection with any fraud, and section 7 makes it an offence to 'make, adapt, supply or offer to supply any article' where the accused has knowledge that it will be used in the course of or in connection to fraud,[45] or where it is intended to be used as such.[46] Section 8 provides that 'article' is to be interpreted to include any 'program or data held in electronic form'. The structure of these two offences bears a striking similarity to the CMA's section 3A offence. Both were introduced around the same time, with the section 3A formulation intended to 'fill the gap' where it might not be established that the malware was specifically intended for use in the commission of fraud.[47] There remains, however, a substantial degree of overlap.

Turning to the issue of malware distribution, such distribution commonly occurs via 'spam'. Spam, traditionally defined as irrelevant and unsolicited emails, was identified in the Report as a significant threat in and of itself. Despite the volume of spam substantially decreasing over time from a high in 2009 of 87.2% of all email traffic, it was noted that 39.2% of all emails and messages sent are unwanted.[48] Spam-type techniques have evolved to operate beyond just email and now operate across social media services,

---

[44] There are indeed cases where offenders have been charged with the building and maintenance of 'botnets', and such cases appear to be becoming more common, but these cases have generally arisen in the context of groups working together, where one person took responsibility for creating and administering the botnet, while collaborating in attacking targets. The prosecutions against the so-called 'LulzSec hackers' are a key example of this: Ryan Cleary was sentenced in concert with three other offenders for his role in administering a botnet. Cleary was sentenced to 32-months imprisonment – see *R v Cleary, Davis, Akroyd & Al-Bassam* (Unreported, Southwark Crown Court 16 May 2013).

[45] *Fraud Act 2006* s 7(1)(a).

[46] *Fraud Act 2006* s 7(1)(b).

[47] But, as was noted in chapter 3, it is not entirely clear why the development of possession of malware could not be prosecuted under the 'reckless enabling' formulation of the CMA's section 3 offence available pursuant to *Computer Misuse Act 1990* ss 3(2)(d), 3(3).

[48] ENISA (n 9) 54.

mobile apps, and other messaging platforms.[49] While sending spam messages is not in and of itself a crime under the CMA, commercial entities are bound by the *Directive on Privacy and Electronic Communications.*[50] However, spam messages are useful vehicles for distributing malicious code – a well-crafted email can prompt a user to open the message and execute an attached file. Where this is the case, the offence of fraud by false representation applies alongside the section 1, 3 and 3A offences.

It is clear that there is suitable scope for general criminal law offences to apply to conduct involving the creation and use of many types of malware, as well as clearly falling within the bounds of the CMA's section 3 and 3A offence. The role of the CMA's section 1 offence becomes less clear, save that it provides an avenue for non-contentious guilty pleas, thus allowing more serious charges to be left to lie on the file in the 'public interest'.

The discussion so far has focused on malware being directed at a 'computer' in the conventional sense. Where the 'computer' is a smartphone, however, a range of additional offences under the *Communications Act 2003* likely become available. These offences include the dishonest obtaining of electronic communications services[51] and the improper use of public electronic communications networks.[52] Further, the *Mobile Telephones (Re-Programming) Act 2002* makes it an offence to alter device identifiers or re-programme the device.[53] Unlawful interception, disclosure and interference offences can also apply, depending on the nature and use of the malware in the given circumstances.[54] But these offences relate, in a general sense, to gaining access and control of mobile devices to fraudulently make phone calls or utilise data allowances, remove manufacturer

[49] Ibid 55.

[50] EC/2002/58, [2002] 201 OJ L 37.

[51] Sections 125-126.

[52] Section 127. This section deals with the sending of messages that are grossly offensive, or have an obscene, indecent or menacing character. See *DPP v Collins* [2007] 1 Cr App R 5.

[53] Section 1.

[54] See *Wireless Telegraphy Act 2006* s 48; and *Regulation of Investigatory Powers Act 2000* s 1.

and network identification, or to intercept the content of communications – not to the multitude of other functions modern mobile phones are capable of performing.

(ii) Denial of Service attacks

Denial of Service ('DoS') attacks were introduced in Chapter 3. The Report identifies DoS attacks as an increasing threat given the growth in available network bandwidth and increasing sophistication and unpredictability of available and developing techniques.[55] In its post *DPP v Lennon*[56] form, DoS attacks fall squarely within the CMA's section 3 offence in that they operate to impair, or hinder the legitimate use of, a computer, network or service. Indeed, numerous prosecutions for DoS attacks under section 3 have been successful. *R v Weatherhead, Rhodes, Gibson & Burchall*[57] involved a series of DoS attacks against PayPal, Visa and Mastercard in apparent retaliation for the politically charged withdrawal of those companies' services to WikiLeaks. Weatherhead and Rhodes were sentenced to 18 months and six months imprisonment respectively. *R v Martin*[58] was in response to attacks against the websites of the University of Oxford, the University of Cambridge and the Kent Police. Martin pleaded guilty and was sentenced to two years imprisonment. These cases have been followed by many others, with the CMA's section 3 offence being pursued frequently by prosecutors in response to DoS attacks.[59]

The consistent reliance on the section 3 offence by prosecutors is likely helped by the lack of clear and apparent analogy for the conduct at issue: the disruption of access to a network service due to the server being overloaded with illegitimate access requests.

---

[55] ENISA (n 9), 47.

[56] [2006] EWHC 1201.

[57] (Unreported, Southwark Crown Court 24 January 2013).

[58] [2013] EWCA Crim 1420.

[59] Further examples include *R v Kaye* (Unreported, Blackfriars Crown Court, 11 January 2019) involving a DoS attack against Liberian mobile phone company Lonestar; *R v Mudd* (Unreported, Central Criminal Court, 27 March 2018) involving 595 DoS attacks against 181 IP addresses; *R v Bessell* (Unreported, Birmingham Crown Court, 18 January 2018) who had remote control of 9,083 'bots'; and *R v Jack Chappell* (Unreported, Manchester Minshull Street Crown Court, 20 December 2017) where the accused ran an online service that facilitated the launching of over 2,000 DoS attacks including against Amazon and Netflix.

Conceptually, however, analogy may be drawn to offences such as the willful obstruction of a highway.[60] In the same way an improperly parked car may temporarily disrupt the free passage of traffic along the highway, so too does the intentional overloading of a network server temporarily obstruct the free flow of legitimate users. While this fits conceptually, given the specificity of the offence as related to highways, it is clearly not applicable. The section 3 offence would thus appear, at least in respect to DoS attacks, to respond to a gap in the criminal law. Despite some possible civil liberties criticisms,[61] the section 3 offence appears reasonably well adjusted to respond to situations involving DoS attacks, at least where an offender is identified.

(iii) Phishing, Identity Theft, and Fraud

Phishing involves the development of emails or tools that, generally, link to fraudulent websites in an effort to 'trick' users into installing malware, or into voluntarily providing their account names and passwords for various services: social media and banking being the most valuable. Phishing is becoming increasingly specific and targeted towards individuals, developed by drawing together publicly available personally identifiable information in order to cultivate a higher level of trust in the authenticity of the email on the part of the recipient; sometimes referred to as 'spear-phishing'.[62] As with spam, phishing does not fall within the scope of the CMA *per se*, unless it is indeed accompanied by malware, or if account details are used to access computers or data (with such access necessarily being unauthorised).[63] But, as was the case in the discussion above with respect to spam, it should be noted that phishing clearly falls within the scope of the offence of fraud by false representation. This is even more so in cases of spear-phishing

---

[60] *Highways Act 1980* s 137.

[61] There is criticism of potential overreach in the drafting of section 3, particularly in relation to avenues of civil disobedience – with DoS attacks being argued as a form of 'digital sit-in' that are now clearly illegal. Consider, for example, the motivations of Weatherhead and Rhodes in their attacks against PayPal, Visa and MasterCard which were motivated by a political aim. For an exploration of the general argument see, eg, M. Klang, 'Virtual Sit Ins, Civil Disobedience and Cyber Terrorism', in M Klang and A Murray (eds) *Human Rights in the Digital Age* (2005).

[62] See Jason Hong, 'The State of Phishing Attacks' (2012) 55(1) *Communication of the ACM* 74.

[63] While the court in *Re Yarimaka* [2002] Crim LR 648, [18] contemplated that a 'spoofing' email that masquerades as originating from a particular source would 'manifestly affect its reliability', it later conceded that this would not always be the case, see *DPP v Lennon* [2006] EWHC 1201 Admin, [12].

given the necessary targeting of the relevant individual involved such they believe the email to have originated from a legitimate source.

The information gathered via phishing attacks can also be constructed and used to commit identity theft and undertake various other forms of fraud. Such conduct may constitute offences under the *Fraud Act 2006*, the *Identity Documents Act 2010*, and/or the *Forgery and Counterfeiting Act 1981*. Like other areas already discussed, the CMA covers many of the steps that may be utilised by offenders in the commissioning of fraud or identity theft, but not the actual fraud or the identity theft itself.

(iv) Insider threats, information leakage and data breaches

'Information leakage' is the unintentional disclosure of personal information, log-in credentials and other data. Such leakage can occur through flaws or weaknesses in technical processes (for example the Heartbleed vulnerability in OpenSSL),[64] through accidental disclosure, or through incidental disclosure (information that can be *inferred* from separate and seemingly unconnected disclosures).[65] While many would assume that hacking and the use of malware would account for the bulk of data loss, according to the Report approximately 50% of information leakage occurs as a result of a 'lost device'.[66] The information can be used to develop targeted phishing attacks, assist in identity theft or form the basis of the commission of fraud.

Depending on the context, it is entirely possible that information leakage of this kind does not clearly fall within the scope of the offences within the CMA. It is possible that access to such data will still be considered contrary to the section 1 offence, particularly if the leakage occurs due to vulnerabilities in technical processes believed by the user to be secure, but this is perhaps less likely to be the case in relation to information willingly posted on websites or social media. Use of that data to subsequently gain

[64] See, eg, Zakir Durumeric et al, 'The Matter of Heartbleed' in *Proceedings of the 2014 Conference on Internet Measurement*, November 5-7, 2014, Vancouver, Canada.

[65] ENISA (n 9), 79.

[66] Ibid 80.

unauthorised access to computers, networks or further data, however, will certainly be within scope.

The failure to take adequate precautions to guard against the breach of personal data, however, is subject to the comprehensive framework established by the *General Data Protection Regulation* ('GDPR') and the *Data Protection Act 2018* ('DPA'). Personal data is defined as 'information relating to an identified or identifiable living individual'.[67] The framework of the GDPR and the DPA are informed by an attempt to balance concern for individual rights and privacy, to promote the security of data processing practices by companies, while also recognising the economic value of data. The scope of what constitutes such 'personal data', though, remains to be fully tested, but it appears a broad definition, particularly with reference to the notion of an individual being 'identifiable' by the data in questions. The GDPR provides that:

> [a]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural persons.[68]

The concept of 'personal data' is thus context-specific – data will qualify as personal data where the context of its collection, storage or processing permits the identification of an individual. While this is a wide definition, it naturally covers fewer types of data than the CMA's section 1 offence, which applies irrespective of the nature, or any inherent quality, of the data in question. Beyond this, the broader framework of the GDPR and DPA works to incentivise data controllers and processors to produce ever more specific terms of service and operational procedures such that they can establish compliance. It is upon breach of these terms of service that criminality under the CMA's section 1 offence can arise.

The DPA, itself, establishes a number of criminal offences, with each punishable by a fine. A number of offences apply to conduct taken to obstruct investigations

[67] *Data Protection Act 2018* s 3(2).

[68] *General Data Protection Regulation* [2016] OJ L 119/1, Art 4.

undertaken by the Information Commissioner's Office,[69] as well as the making of false statements[70] or the destruction or falsifying of information and documents in response to the receipt of an 'information notice'[71] made by the Information Commissioner in the course of investigating a suspected regulatory breach. The DPA also makes it an offence to knowingly or recklessly obtain or disclose personal data without the consent of the data controller,[72] to procure such disclosure to another person,[73] or to retain personal data without the consent of the data controller.[74] A defence is available in respect of these three offences where the relevant data was obtained, disclosed or procured in an otherwise lawful manner,[75] or was done in the public interest,[76] or where the person acted under the reasonable belief they had a legal right to do so,[77] or a belief they had the appropriate consent.[78] It is also an offence to knowingly or recklessly re-identify de-identified data,[79] or, when a request has been made by an individual to exercise a right in respect of their personal data, to alter, erase, destroy or conceal that information in an attempt to prevent that disclosure.[80]

While many of these offences build on those contained in the earlier *Data Protection Act 1998*, the full extent of their application and interpretation is yet to be tested in the context of the broader regulatory framework established by the GDPR. Even so, a

---

[69] *Data Protection Act 2018* s 119.

[70] *Data Protection Act 2018* s 144.

[71] *Data Protection Act 2018* s 148.

[72] *Data Protection Act 2018* s 170(1)(a).

[73] *Data Protection Act 2018* s 170(1)(b).

[74] *Data Protection Act 2018* s 170(1)(c).

[75] *Data Protection Act 2018* ss 170(2)(a)-(b).

[76] *Data Protection Act 2018* s 170(2)(c).

[77] *Data Protection Act 2018* s 170(3)(a).

[78] *Data Protection Act 2018* s 170(3)(b).

[79] *Data Protection Act 2018* s 171(1). Similar defences are available as to the knowing or reckless obtaining of personal data contrary to s 170.

[80] *Data Protection Act 2018* s 173(3).

number of initial observations can be made. First, it is notable that the offence of knowingly or recklessly obtaining, procuring or disclosing personal data has a number of available defences, whereas the CMA section 1 offence does not. Second, both the offence of obtaining personal data and the CMA's section 1 offence cover the same conduct, but the specific data protection offence carries penalty by way of a maximum fine, while the general unauthorised access offence carries a penalty by way of maximum fine and/or up to two years imprisonment. Third, given the absence of available defences and that it does not need to be established that data was in fact 'obtained, procured of disclosed' for the purpose of the CMA section 1 offence, there are clear procedural, evidential, and cost advantages in pursuing charges with respect to the CMA section 1 offence rather than for offences contrary to the DPA, even where personal data is involved. Indeed, the decision to prosecute under the CMA section 1 offence in lieu of the DPA offence has recently been taken in practice.

In *Information Commissioner v Kasim*,[81] the accused was a former worker at an automotive repair firm who made use of software known as Audatex to manage customer details, as well as vehicle and accident information. The accused made use of a colleague's login details to access Audatex without permission and continued to do so even after he left the company and began working for a competitor. The accused sold the customer data he obtained from the system to various accident claim management services who then 'cold-called' the owners of the vehicles involved in accidents in order to offer their services. These customers complained about the nuisance calls to the Information Commissioner's Office who launched an investigation, ultimately uncovering the accused's conduct. A prosecution was then launched not for the obtaining and disclosure of personal data,[82] but instead as conduct contrary to the CMA's section 1 offence. A spokesperson, speaking on behalf of the Information Commissioner's Office, described this decision as being based on the fact that the authority 'wanted the sentencing court to have a wider range of penalties available to them to reflect the nature and extent of the

[81] (Unreported, Wood Green Crown Court, September 2018).

[82] Given the offending in this case occurred in 2016, the relevant charge would have been one of conduct contrary to the *Data Protection Act 1998* s 55 which largely mirrors the offence in *Data Protection Act 2018* s 170.

offending'.[83] The accused pleaded guilty and was sentenced to a six-month term of imprisonment.

It is perhaps unfortunate that the careful policy considerations in respect of the protection of personal data, with its focus on balancing the privacy rights of individuals with appropriate regulation of organisations who collect, store and process personal data for profit, can be effectively ignored on the basis of the broad scope of the CMA's section 1 offence. Consideration of data protection offences has consistently found against a response from the criminal law in the form of imprisonment. However, the CMA's section 1 offence was formulated before the rise of the economic and social importance of personal data processing arose. That it applies so broadly, and in a manner that the increasingly resourced Information Commissioner's Office can pursue, indicates that a substantial spike in prosecutions under section 1 may soon arise. The offence justified on the basis of protecting the integrity of computers may soon be used to criminalise breaches of privacy.

(v) Physical manipulation/damage

While 'physical attacks' are referred to in the Report as 'not a real cyber-threat', physical access to data, devices and resources within organisations represent a number of criminal opportunities.[84] This includes the theft of the computers and devices themselves, although recent surveys suggest that a majority of victims now perceive the harm in such circumstances to arise from the loss of access to their data, rather than loss of the device itself.[85]

The Report suggests that 'digital theft has overtaken physical theft with respect to corporate fraud'.[86] The evidence used to make out that claim came from observations

[83] See, eg, Jon Leyden, 'Car repair worker jailed over data privacy breach', *The Daily Swig* (13 November 2018) <https://portswigger.net/daily-swig/car-repair-worker-jailed-over-data-privacy-breach>.

[84] ENISA (n 9) 74.

[85] Ibid 75.

[86] Ibid 74.

made in the 2017/18 Global Fraud & Risk Report produced by Kroll, a division of consulting company Duff & Phelps. It is unsurprising, then, that the document relies on the terms 'theft' and 'fraud' for their generic, rather than legal, meaning. Under the terms 'digital theft' and 'corporate fraud', the report refers to embezzlement, theft of product and inventory, the production of fraudulent vendor invoices, mismanagement and theft of intellectual property, and employee misconduct. The 'digital' moniker is then a misnomer: the identified conduct is really simple theft, forgery and fraud, along with the relevant intellectual property responses. But each form of conduct here falls within the scope of the CMA's section 1 offence, and when untaken with the intention to commit theft, forgery or fraud, the section 2 offence applies also.

Physical damage to a computer or device falls within the scope of the *Criminal Damage Act 1971* ('CDA') provided that the damage alleged is only physical in nature and not instead arising on the basis of data manipulation. Unlike the originally enacted form of the CMA's section 3 offence, the current provision no longer itself operates to preclude the operation of the CDA. This has been argued by some commentators to mean that, in theory, the approach adopted in *Cox v Riley*, and *R v Whiteley*[87] to establish criminal damage on the basis of data manipulation could be resurrected.[88] This, however, is a clearly incorrect view. The exclusion as it existed in the original section 3 offence was instead inserted directly into the CDA itself.[89] The modification of the contents of a computer remains excluded from the operation of the offence of criminal damage.

[87] (1993) 93 Cr App R 25.

[88] See, eg, Diane Rowland et al, *Information Technology Law* (Routledge, 4th ed, 2012) 127.

[89] *Criminal Damage Act 1971* section 10(5);

> For the purposes of this Act a modification to the contents of a computer shall not be regarded as damaging any computer, or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(vi) Cyber espionage

Actions constituting cyber espionage,[90] and related threats of cyber terrorism, would fall within the scope of the CMA, particularly with the introduction of section 3ZA. Espionage, in particular, refers to particular tools and techniques used to threaten or inhibit the operation of governments or organisations, and is generally activity engaged in by State governments, or competing organisations. Within this might fall the 'advanced persistent threat' – a threat actor who, due to the advanced skills and capabilities generally associated with State-backed entities, gains unauthorised access to a network and remains undetected for an extended period of time in order to eventually steal, spy or disrupt. This form of conduct is distinguished from the more common forms of criminal activity facilitated by malware and other techniques given both the level of sophistication required, and the temporal disconnect between the initial infiltration of the network and the ultimate result. Cybersecurity industry reports have claimed that the average 'dwell-time' for which an advanced persistent threat goes undetected ranges from 71 days in the Americas to 204 days in the Asia-Pacific region.[91]

The challenge presented by this type of threat, however, is one of detection and mitigation. The initial access to the network falls within the CMA's section 1 offence, and likely the section 2 offence as the context of the intended outcome of such conduct is the commission of a further offence, irrespective of any temporal disconnect. Where steps are taken to ultimately disrupt the network, the section 3 offence applies, and that forms of malicious code were developed and deployed renders the initial development of that code as conduct contrary to section 3A. Where the ultimate outcome achieved is one of theft or economic gain by fraud, those offences are of course prosecutable; where the offenders are, or can be brought, within the court's jurisdiction.

[90] See Warwick Ashford, 'UK Hit by 70 Cyber Espionage Campaigns a Month, says GCHQ' *Computer Weekly* (1 July 2013) <http://www.computerweekly.com/news/2240187230/UK-hit-by-70-cyber-espionage-campaigns-a-month-says-GCHQ>.

[91] See, FireEye, 'M-Trends 2019', *FireEye,* (2019) <https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html>, 7-8.

This broad spectrum of threats clearly operates in the context of substantial overlap between the CMA's various offences and other general criminal law offences. This overlap can be visualised through mapping these cyber threats, along with the potential application of both CMA and general criminal offences, across the 'cyber kill chain'.

B *The Cyber Kill Chain*

The cyber kill chain was developed in 2011 by computer scientists working at Lockheed-Martin. The model was established in order to understand the steps carried out in a successful 'cyber-attack', thus providing a framework to guide the development and implementation of computer and network defences designed to disrupt and guard against the threat at each stage. The phases of the cyber kill chain were described as follows:

1. **Reconnaissance** – the selection of a target, the undertaking of research about that target, and initial attempts to identify security vulnerabilities in the target computer or network.

2. **Weaponisation** – building on the information gained through reconnaissance, tailored/specific malware is developed to target the identified vulnerability.

3. **Delivery** – the malware is transmitted to the target computer or network (email, websites, or via USB etc)

4. **Exploitation** – when the transmitted malware is triggered, it takes action on the target computer or network to exploit the vulnerability.

5. **Installation** – the malware installs an 'access point' (or 'back door') that now permits the unauthorised intruder access to the computer or network.

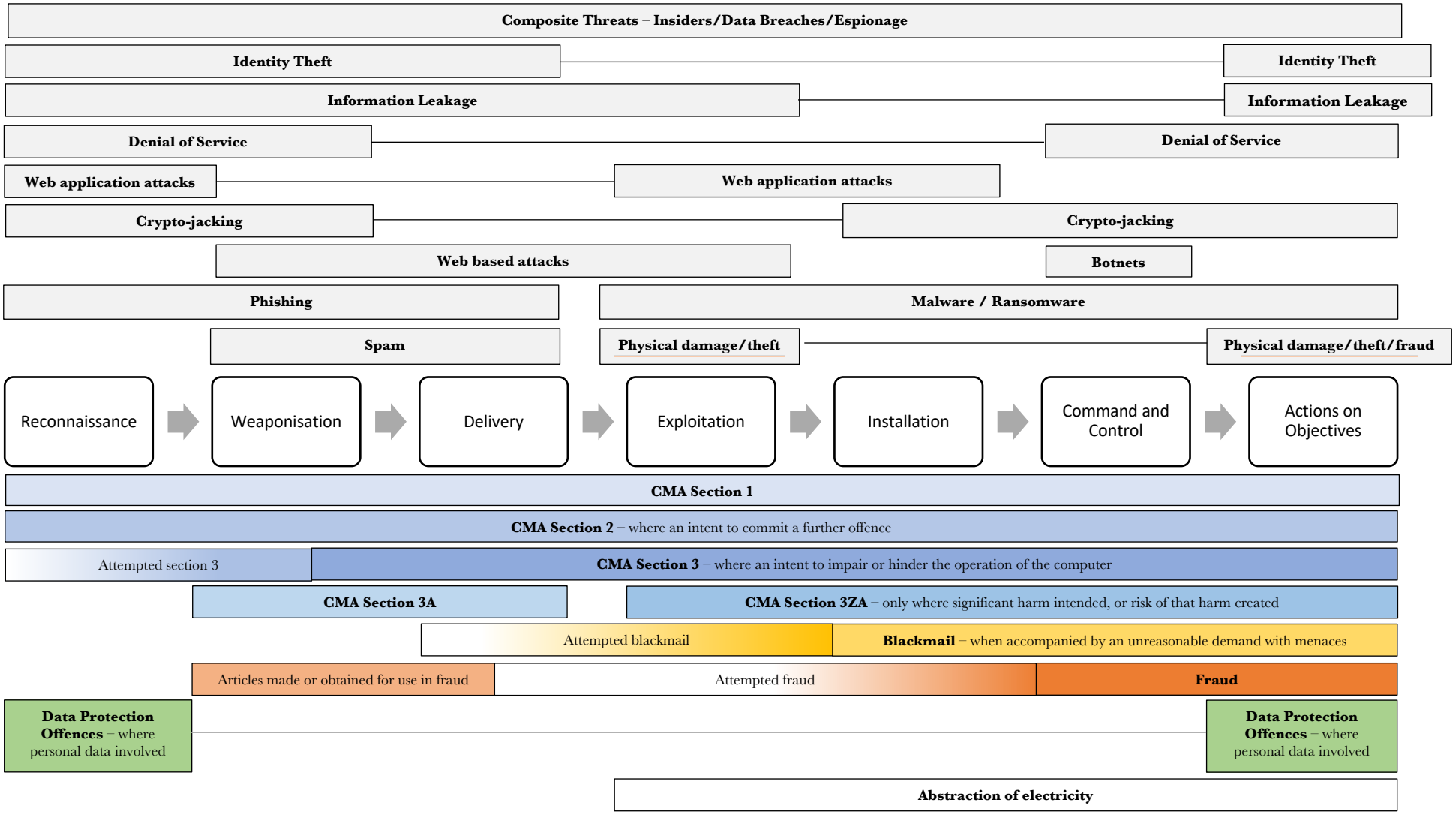
6. **Command and Control** – that access enables the unauthorised intruder to have persistent access to the target computer or network.

7. **Actions on Objective** – using that persistent access, the unauthorised intruder then sets about to achieve their goal; data exfiltration, destruction or encryption for ransom etc.

Using this kill chain as a model, we can visualise the operation of the offences within the CMA and other general criminal offences across each stage alongside the threats identified by ENISA.

In the following chart, the seven phases of the cyber kill chain are set out across the middle of the page. The cyber threats thus far considered are mapped *above* the relevant phase of the cyber kill chain upon which they can operate. *Below*, the reach of available criminal offences that may operate to criminalise that conduct is similarly mapped. This is not intended to be a complete mapping of the criminal law; rather, it represents the various broadly defined criminal offence categories discussed throughout this chapter.

ENISA Cyber Threats mapped to the 'Cyber Kill Chain'



Possible avenues for criminal prosecution

The CMA's section 1 offence applies at each stage of the cyber kill chain where the accused causes a computer to perform a function with intent to secure unauthorised access, knowing that access to be unauthorised. But, as can be observed, there is substantial overlap with the applicability of both offences under the CMA (section 2 and 3 in particular), and, as the conduct progresses, overlap with the general offences of fraud and blackmail. Each of these offences, however, require the establishment of some kind of criminal intent associated with clearly identified harms. The CMA's section 1 offence, again, responds to the harm of a breach of the integrity of computer. The section 1 offence, then, does not work to 'fill a gap' in the operation of other criminal laws by ensuring malicious conduct is captured, rather it presumes maliciousness without requiring any proof to that effect. It similarly applies to all types of data, eschewing the balancing of policy considerations inherent in other overlapping criminal offences, like those under the DPA relating to personal data.

As can be observed in the chart above, the moment the conduct moves beyond a mere digital trespass, liability arises under a number of available offences. Regardless, the section 1 offence applies and is likely completed. The section 1 offence, in its drafting, scope of application, lack of available defences, and thus relative ease of prosecution, runs the risk of continuing to evolve to become a prosecutorial plaything; from the most minor infractions, to applying to serious breaches of data protection, thus supplanting the available specific offences, and to operating as a substitute offence for more appropriate substantive offences in the charge bargaining process in an effort to pursue the 'public interest' at the lowest cost.

Much of this overlap appears to stem from continued confusion and conflation as to identifying what is, and is not, computer crime. Beyond this, when computer crime is targeted by specific legislative intervention, there is little appreciation and understanding of the broader interaction such intervention has with both the civil and broader criminal law. A contributing factor to this confusion and conflation continues to be both how to identify and understand the role of computers in the commission of crime, but also the distinction between data and information, and data and property. On the latter point, it becomes difficult to accept a doctrinally satisfactory position with respect to the application of a general offence to conduct involving data when a

foundational distinction with respect to how to classify data has been pre-emptively drawn. Since the formulation of the CMA, however, taxonomies of computer-related crime have been developed, although their utility with respect to understanding the application of and interaction between general and computer-specific offences has received limited attention.

III TAXONOMIES OF COMPUTER CRIME

Any claim of over-inclusiveness warranting reform with respect of the CMA's section 1 offence depends, in part, on the necessity of having computer-specific criminal legislation. The section begins by briefly setting out the computer crime typology developed by the United States of America's Department of Justice ('DOJ'). This model for understanding computer-related crime did not exist in a formalised manner during the formulation of the CMA. Further, it does not appear to have since been 244itself used to evaluate either the CMA or its foundational assumptions. Neither have the 'analogy oriented' models, or Wall's 'cybercrime matrix'.

A *The Computer-Crime Typology*

In 1996 the DOJ formulated a computer crime typology[92] that set out to assess 'the extent to which harmful acts are mediated by networked technologies'.[93] Criminal activity involving computers was proposed to be understood and approached through a tripartite classification system:

1. Crimes in which a computer or network is the intended *target* of the activity.
2. Crimes where technology operates as a *tool* in the commission of a broader offence that exists both with, and without, the aid of such technology.
3. Crimes where technology has a passive or *incidental* role.

[92] Computer Crime and Intellectual Property Section, US Department of Justice, The National Information Infrastructure Protection Act of 1996, *Legislative Analysis* (1996) <http://www.irational.org/APD/CCIPS/1030_anal.html>.

[93] David Wall, 'Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime' (2008) 11(6) *Information, Communication and Society* 861, 866.

The classification, therefore, rests primarily on whether the computer is the object, instrument, or merely a source for evidence of a crime.[94]

The first category, where computers are the target of wrongful conduct, includes conduct for which the identification of a fair analogy to pre-existing offences may not be possible. Within this category could sit conduct such as using and deploying malware, or orchestrating a Distributed Denial of Service ('DDoS') attack.[95] It captures conduct that 'fall[s] outside the jurisdiction and experience of the criminal justice process'.[96] It was this kind of conduct, where a computer was the focus of malicious acts, which the CMA was initially designed to address, particularly with its focus on the 'integrity' of the contents of a computer: any resulting harm to the proper operation of software or data is not necessarily something that has clear analogy to the general criminal law. The physical integrity of the computer remained as it was: this was the issue in the strained decisions concerning criminal damage in *Cox v Riley* ('Cox')[97] and *R v Whiteley*[98] before the enactment of the CMA.

The second category, where a computer is used as a tool, applies to the commission of existing general offences where the use of computers has made that conduct easier, altered the potential scope of that general offence, or magnified the risks associated with it. It is on this category of conduct that some early considerations of computer-related crime tended to focus: that this was 'old wine in new bottles'.[99] Conduct falling within this category, therefore, is the use of a computer to commit 'a crime falling within the

---

[94] Rowland et al (n 88) 103. *Cf* Richard Downing, 'Shoring Up the Weakest Link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime' (2005) 43 *Columbia Journal of Transnational Law* 705.

[95] See discussion in Chapter 3, 109, 111-3.

[96] David Wall, *Cybercrime: The Transformation of Crime in the Digital Age* (Polity, 2007) 10.

[97] [1986] 83 Cr App R 54.

[98] (1991) 93 Cr App R 25.

[99] Peter Grabosky, 'Virtual Criminality: Old Wine in New Bottles' (2001) 10 *Social & Legal Studies* 243; and Susan Brenner, 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9(4) *Virginia Journal of Law and Technology* 13.

parameters of the [existing] criminal law and, as such, there is [already] some legal basis for their definition.'[100]

In exploring this category, Fafinski uses the example of a 'phishing' attack.[101] A victim receives an email purporting to be from a trusted source that contains a link to a website. That website similarly purports to be from that same source. The construction of that email and website induce the victim to provide their personal and/or financial information, thinking they are providing that information to the trusted source. Instead, the malicious crafters of the email and website receive that information. This conduct clearly falls within the scope of section 2 of the *Fraud Act 2006*: we have an email and a website dishonestly and falsely being represented as legitimate for the purpose of financial gain. Here, the use of computers was merely peripheral to the offence of fraud itself: similar conduct is possible without the use of computers. Guinchard would concur: "the fact remains that the basis of fraud is a lie and the lying is as frequent online as it is offline."[102]

The third category, where the use of a computer is merely incidental, concerns circumstances where the computer or its data becomes a source of evidence in the investigation of some unrelated conduct. For example, a series of emails between parties to a conspiracy, where the content of the email and the corresponding data concerning the author, recipient, time of sending and perhaps the location of the senders of the emails can be used to establish evidence of the formulation of the relevant agreement to undertake a criminal course of conduct.

The three categories making up this typology would *prima facie* present a neat and comprehensive summary of the modes of conduct we could expect to see in computer-related crime. However, the model, as above in its most basic form, does not adequately account for some factors: offending patterns, the degree of harm, and level of

---

[100] Stefan Fafinski, *Computer Misuse: Response, Regulation and the Law* (Willan Publishing, 2013) 7.

[101] Ibid.

[102] Audrey Guinchard, 'Crime in virtual worlds: The limits of criminal law' (2010) 24(2) *International Review of Law, Computers & Technology* 175, 176.

victimisation.[103] It also fails to incorporate notions of motivation and intent. There is also scope for considerable overlap between categories.

B Wall's categories of 'cybercrime' – a renewed focus on harm

In 2008, Wall observed that in the 15 years following the enactment of the CMA, only around 200 prosecutions had been pursued. At the same time, the Ministry of Justice reported that they only had a 'handful of cases pending'.[104] This lack of prosecutions, he argued, presented a conundrum. Borrowing from former US Secretary of Defence, Donald Rumsfeld, he posed the question '[d]oes the low prosecution rate represent an 'absence of evidence' or is it evidence of the absence of cybercrimes?'[105] For Wall, an increased understanding of the nature of computer-related crime would go a long way to addressing this question and, thus, the gap between the experience of 'cybercrime' and the rate of prosecution.

While Wall's focus, as a criminologist, was on developing a more comprehensive understanding of the nature of 'cybercrimes' and those who commit them, the answer to his question appears to lie in neither of the options he proposes. The lack of prosecutions under the CMA is perhaps the result of it rarely being seen by prosecutors as the appropriate descriptor of the entirety of the conduct before them, and that the statistics he relied upon did not include circumstances where an offence under the CMA was listed as an additional charge to a more serious general offence on the charging instrument. Nor, then, its utility in charge bargaining. However, Wall's work in seeking to address the question in the form he posed it (the absence of enough evidence to prosecute or evidence of an absence of 'cybercrime') aids us in understanding why this is so. The more the nature and detail of potential use of computers in crime is understood, the clearer it

[103] See, eg, Matthew Williams and David Wall, 'Cybercrime' in Chris Hale et al. (eds) *Criminology* (Oxford University Press, 2013) 250. The model also focuses on one element of wrongdoing: the inclusion of a computer, ignoring other means of characterising the conduct.

[104] David Wall, 'Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime' (2008) 22 *International Review of Law, Computers & Technology* 45, 46.

[105] Ibid.

becomes that the inadequacy is not an absence of evidence, nor an absence of conduct, but rather the consequence of broad legislative drafting.

1 *Analogy-oriented conceptions*

In his collection of influential work, Wall has set out two ways to understand computer-related crime. The first sought to categorise resultant harms based on their analogous non-technology specific legal forms. In that sense, the existing legal framework was the starting position, and the potential uses of computers were constructed to fit pre-existing categories of conduct. This categorisation was summarised usefully by Yar as:[106]

1. Cyber-*trespass* – crossing boundaries into other people's property and/or causing damage; hacking, defacement, malware.
2. Cyber-*deceptions and thefts* – stealing money or property, and intellectual property violations.
3. Cyber-*pornography* – breaching laws on obscenity and decency.
4. Cyber-*violence* – doing psychological harm to, or inciting physical harm against others; hate speech, stalking.

Although not included in Wall's original work, Yar suggests we can also add a fifth category.

5. Cyber-*terrorism and warfare* – politically motivated activities targeted at States and/or critical national infrastructure.

Within this framing, the first and second category arise from analogy with crimes against property. The CMA would appear to target these categories, in particular, the construction of the offences set out in section 1 and section 2. Both are similar in form to the tort of trespass. We can consider the third category as constituting crimes against morality, and the fourth as crimes against the person. The fifth category exists as an aggravated category of crimes against the person where the State is the broader target, or some political motivation is present.[107]

---

[106] Majid Yar, *Cybercrime and Society* (Sage, 2013) 10.

[107] See, eg, Dan Verton and Jane Brownlow, *Black ice: The invisible threat of cyber-terrorism* (Osborne, 2003).

The CMA's section 1 and section 2 offences could, therefore, be considered directed at instances of 'cyber-trespass' and 'cyber-deceptions/thefts', and the recently inserted section 3ZA offence targets instances of 'cyber-terrorism/warfare'. Where such seemingly clear analogies exist, is the CMA needed? There is, of course, conduct that does not necessarily fit this construction. DDoS attacks, for example, do not easily fall within any of these categories, although to have the capabilities to launch such a DDoS attack a series of 'cyber-trespasses' would necessarily have occurred. On that basis, we could *prima facie* argue that legislative intervention, like that found in the section 3 offence, to cover conduct like DDoS is appropriate. There is no apparent clear analogy to existing general criminal law offences, and the resulting harm (for instance, the rendering inoperable of an online serve) moves beyond analogy to mere trespass.

The broad drafting of the section 1 offence, however, cuts across all of these categories. Wherever there is conduct capable of being considered 'unauthorised access' there is likely a crime committed on that basis alone. Indeed, it is precisely because of this that section 1 operates as a lesser included offence whenever prosecutors pursue a section 2 or section 3 offence. In practice, therefore, the CMA's application is not limited to instances of conduct analogous to 'trespass' and 'deceptions/thefts' as conceived in this model.

2 *The cybercrime matrix*

The development of the Cyber Crime Matrix has been Wall's second main contribution. Here, his approach bears a resemblance to the computer crime typology. Rather than starting from the existing categories of criminal offences, the matrix relies on first identifying the possible types of criminal harm resulting from conduct involving computers, before seeking to explain the relationship of that conduct to the criminal law. The matrix involves three categories of crimes: those against the machine, those using machines, and those concerned with the content of data stored on the machines.

The first two categories are analogous to the computer crime typology, with 'against the machine' being the equivalent of 'computer as the target', and 'using machines' the equivalent of 'use as a tool'. For Wall, 'using machines' also includes those circumstances where computers are merely incidental to the commissioning of a crime.

The final category represents a newer inclusion: content crimes. This category encompasses, for example, the use of computers to facilitate intellectual property infringement (as explored in Chapter 5) or the distribution of obscene material. Wall then divides these categories into three levels, or 'generations', of crime.

Level 1 focuses on instances of ordinary crimes: conduct that is criminal regardless of the medium used to commit it. Level 2 crimes are hybrid crimes, these have at their core conduct that is analogous to pre-existing crimes, but the advent of computing technology has increased or changed the nature of their commission, the potential victims, or the probable scale of harm. Level 3, what Wall calls 'true cybercrimes', consists of conduct that would not be possible without computers.

This is the typified construction of his matrix:[108]

	Crimes against the machine	**Crimes using machines**	**Crimes in the machine**
Level 1: Ordinary Crimes	Eg. Hacking a system	Eg. Fraud within banking system	Eg. Storing extreme pornography
Level 2: Hybrid	Eg. Hacking across networked computer systems	Eg. Fraud across banking systems and networks	Eg. Distributing extreme pornography
Level 3: True Cybercrimes	Eg. Automated hacking tools across networks	Eg. Theft of virtual artefacts	Eg. Networked content delivery of extreme pornography

This matrix represents a useful policy tool. It attempts to contextualise the way computers are used in crimes, while also factoring in the degree to which those uses reflect the modes of criminality. There is naturally a degree of overlap between categories, but the dual nature of the classification allows for greater nuance and clearer identification of the differing features of the conduct. It also permits a stronger foundation upon which to assess the levels of risk involved.

[108] Matthew Williams and David Wall, 'Cybercrime' in Chris Hale et al, *Criminology* (Oxford University Press, 2009) 246, 251.

It is unfortunate that this more nuanced model was not available to lawmakers when devising the CMA, nor has it seemingly been referenced during subsequent review and amendment. Whereas argument for the need for technology-specific criminal offences in respect of conduct capable of being properly classified as the targeting of a machine and falling within level three could be made based on this model, the offences within the CMA go beyond what might seem to be possible to be supported. While acknowledging that Wall's purpose is to describe behaviour from a criminological perspective, and in accepting that there may indeed be examples of 'true cybercrimes', the examples employed by Wall in his matrix, at least from a doctrinal criminal law perspective, are not convincing, nor particularly satisfying. This is likely due to the broad definition Wall provides for conduct that constitutes a 'true cybercrime': conduct that would not be possible without computers.

If the focus is merely on the 'conduct' of the accused, then it is quite acceptable to categorise, as Wall does, the theft of virtual artefacts and the networked distribution of child exploitation material, as true cybercrimes. Virtual or digital content could not be created, let alone accessed, manipulated, or distributed, without the use of computing technologies: the mere fact of its existence requires a computer. But merely describing the conduct in this form, with the focus on the involvement of computing technologies, does not make it uniquely criminal. These descriptors are devoid of a clear connection to the criminally wrongful harm underpinning them. When the focus shifts to the alleged harm, it is much easier to identify the general offence at issue. With virtual theft, as the name implies, the harm fits within the spectrum of the torts of trespass and conversion, and the offence of theft.[109] Networked distribution of child exploitation material involves offences of distributing child exploitation material; this form just increases the scale and potential severity of the harm.[110]

[109] See, eg, Sarah Green, 'Can a Digitized Product be the subject of conversion?' (2006) 1(M) *Lloyds Maritime and Commercial Law Quarterly* 568; Steven Hedley, 'Cybertrespass – A Solution in Search of a Problem?' (2014) 5(2) *Journal of European Tort Law* 165; Mårten Shultz, 'The Responsible Web: How Tort Law Can Save the Internet' (2014) 5(2) *Journal of European Tort Law* 182; Darren Read, 'Should the English Legal System Adopt the US Law of Cyber-Trespass? (2011) 8(1) SCRIPTed 46.

[110] See, eg, Henry Hillman, Christopher Hooper, and Kim-Kwang Raymond Choo, 'Online Child Exploitation: Challenges and future research directions' (2014) 30(6) *Computer Law & Security Review* 687.

Making these general observations, however, does not mean that these examples of conduct fall neatly within the bounds of these offences. Indeed, much of the challenges that prompted the formulation of the CMA rested on conduct not quite fitting the model of the general offences. But if the computer crime typology and the cybercrime matrix are considered on the basis of identifying conduct in the context of the criminal harm experienced, both can serve as a way to more clearly identify the relevant doctrinal issues. Take the theft example. As was observed earlier in this thesis,[111] courts have had difficulty in applying the general form offences of theft to conduct involving computers and digital artefacts. However, if we utilise a simplified version of the matrix to set out examples of different forms of 'theft' involving computers at the various levels, it becomes clearer that the issues relate to not only the question of an 'intention to permanently deprive', but also to the concept of data as *property*.

	Conduct involving a computer.
Level 1: Ordinary Crimes	The removal of a laptop from a café without the owner's consent.
Level 2: Hybrid Crimes	Theft of a car using relay attack against keyless entry system.[112]
Level 3: True Cybercrimes	Theft of digital artefacts.

Both the level 1 and level 2 forms of conduct clearly fall within the scope of the Theft Act:

> A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and 'thief' and 'steal' shall be construed accordingly.[113]

In the level 1 example, the physical laptop (the property) belonging to the victim is taken into the possession of the accused (appropriated) who, in treating the laptop as their

[111] See discussion in Chapter 2 at 54, and nn 36-7.

[112] See discussion in Chapter 4 at 166-7.

[113] *Theft Act 1968* s 1(1).

own[114] by removing it from the café (intention to permanently deprive) without the victim's knowledge or consent, acts beyond the bounds of reasonable behaviour (dishonesty). The mere fact the property involved is a laptop represents no challenge to the operation of the offence. The same can be said of the theft of the car in the level 2 example drawn from discussion in Chapter 4: the car is clearly property belonging to another. That access to the vehicle was enacted using a relatively sophisticated breach of the keyless entry system has no bearing on the harm to the victim, which was the dishonest appropriation of their property interest in the vehicle.

The level 3 example, however, does not fit so neatly, and in fact faces a number of doctrinal challenges. Data and digital artefacts are not property in the conventional sense: at least not in a form traditionally recognised by theft and the larceny offences upon which it is based.[115] While the definition of 'property' for the purposes of the Theft Act includes 'things in action and other intangible property',[116] this does not clearly include all forms of data. Even where intangible, the thing in question needs to be capable of attracting a property right.[117] There has been a general shift in the focus of the law of theft from the protection of possession to instead provide a broader protection to the right of property.[118] It is here that the data as information or property question becomes key.

Many cases involving the question of theft and data have focused on the nature of the *information* contained in the *data*: that is, the question of what form of legal right attaches to the information. Information granted protection by copyright gains the status of a proprietary interest in the copyright so created by the author's labour, skill, and

---

[114] The current approach to assessing the intention to permanently deprive appears to be that it extends to the treatment of the thing as the accused's own to dispose of, irrespective of the owner's rights or interests, and this includes an accused who 'deals with that property in such a manner that he knows he is risking its loss'. See, *Fernandes* [1996] 1 Cr App R 175 at 188. See, further, criticism of this broad approach in David Omerod and David Huw Williams, *Smith's Law of Theft* (9th ed, Oxford University Press, 2007) 116-23.

[115] For a useful discussion on this point, see Alex Steel, 'Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property' (2008) 30 *Sydney Law Review* 575, 577-82.

[116] *Theft Act 1968* s 4(1).

[117] See, eg, *Oxford v Moss* [1978] 68 Cr App R 183, 185-6; *R v Stewart* [1988] 1 SCR 963, 975-6.

[118] Wayne Rumbles, 'Theft in the Digital: Can you Steal Virtual Property? (2011) 17(2) *Canterbury Law Review* 354, 362; Stuart Green, *13 Ways to Steal a Bicycle* (Harvard University Press, 2012).

judgement.[119] Information that is confidential gains no proprietary interest: the right of confidence is a right to control publication. Confidential information, therefore, cannot be stolen. But, if the nature of the information contained in the data itself is set to one side, and instead the 'data' itself, in its intangible form as a particular configuration of particles, is regarded as attracting proprietary interests in the form of ownership and control, it is entirely possible for the offence of theft to apply to data. The actions of an accused in taking control over data (by copying, manipulating, erasing or other) could be conceived as them appropriating the right of the data owner to control and protect that data, treating it as their own to use and dispose of. This is thus not a question of interfering with a right of confidence or copyright, but instead an interference with a right of control and ownership in the make-up and use of data itself. Such an expansion could be provided, in a limited form, through the addition of interpretive guidance into the Theft Act that data be deemed to constitute property for the purposes of the offence of theft only, as has recently become the position adopted in New Zealand.[120]

However, this potential expansion of theft to apply to data presents its own challenges. Theft, in a similar vein to fraud as explored below, has been modified and expanded well beyond its traditional foundations, losing its focus on the possession of property while increasingly relying on dishonesty as the means of delimiting criminal from non-criminal interferences with property rights more generally. Neither offence takes into account competing interests and can apply to punish all interferences no matter how minor. There is continued criticism of the operation of these offences and their increasing breadth. As Steel observes, 'blanket criminalisation of misuse of uncertain

[119] See, Steel (n 115) 599-602. While an intellectual property interest may constitute 'property' for the purposes of theft, the offence is often not capable of being charged in practice as the nature of ownership of a copyright interest, for example, is not the property that is itself in fact dealt with or appropriated by an accused. Copyright is a separate right to the bundle of rights attached to the physical form of the work (with the courts divided on how this should be understood). Further, while copyright infringement can be an 'appropriation', it is incapable of being appropriated with a coincident intention to permanently deprive the owner of the copyright interest itself. Steel observes, at 602, that 'it is unsatisfactory that theft is defined in such a way that breaches of copyright can amount to all of the *actus reus* elements of theft, and liability is only avoided on the technical ground that the nature of the property right means that the intention of the accused cannot be defined as an intent of permanent deprivation'.

[120] See the recent New Zealand Supreme Court decision in *Jonathan Dixon v The Queen* [2015] NZSC 147 which in expressly rejecting the view taken in *Oxford v Moss* and observing that the 'digital file' of video footage was property for the purposes of the criminal code because it could not be said that such files were 'pure information'.

forms of property may well have unintended effects, and … may well amount to unintentional overcriminalisation'.[121]

While that may be true, the developments within the offences of theft and fraud have increasingly rendered the technical medium of an offence obsolete: the general offences have evolved to become increasingly, albeit certainly not completely, technology-neutral. And the risk of unintentional overcriminalisation caused by these offences ought to be considered in the context of considered exploration of their own broader operation and framing in respect of computing technologies. What has happened instead is that the buck was effectively passed to the CMA, which in its framing produces the very same unintentional overcriminalisation. The broad section 1 offence is capable of applying to almost all conduct within this matrix. Regardless of the severity, scope, or mode of conduct, the section 1 offence is applicable. Further, the obtaining of 'unauthorised access', in the form in which the CMA works to criminalise it, is a necessary pre-condition for many computer-related crimes.

What this preliminary analysis using the cybercrime matrix in respect of theft indicates is that the solution to the challenges presented to the offence of theft might be better found with deeper consideration of the implications of conduct involving computers to the general offence, and amendment of that offence. Indeed, as was introduced in chapter 5[122] and explored further below, this was unintentionally the case with the fraud offences. Such evolution can be better understood through the application of the computer crime typology to understand the role of computing technologies in a given circumstance. Pre-existing general crimes, where computers are merely used as tools, continue to evolve to become more capable of responding to the use of computers in their commission. As technology has changed, the amount of conduct capable of being considered as falling within this category has continued to expand, encompassing much of what the criminal law was originally believed incapable of responding to.

[121] Steel (n 115) 602.

[122] See Chapter 5 at 175.

On the one hand, this could simply be something left entirely to prosecutorial discretion: it should be left to prosecutors to determine which provision most accurately reflects the criminality in the case before them, irrespective of the degree of overlap between offence. But the inconsistencies that can arise between law and practice, between identified categories of conduct, and the increasingly broad set of circumstances where the section 1 offence interacts with inchoate formulations (including attempts and conspiracies) render this unsatisfactory. This is particularly an issue for the labelling function of the criminal law and to what it says more generally about the proper application and functioning of traditional criminal law offences.[123] A general criminal offence is not fully understood when it is assumed not to apply to computers, and the CMA offences are not understood where applied in circumstances general offences could equally apply.

These points can be further illustrated through revisiting the very cases relied upon to justify the creation of the CMA and applying the lens of the computer crime typology to identify the characteristics of the conduct involved, and the broader implications that identification of the role of a computer has on the arc of jurisprudential consideration.

3 *Applying the typology to R v Gold and Anor, and Cox*

The cases relied upon to justify the need for the creation of the CMA, *R v Gold and Anor* ('Gold')[124] and *Cox*, were introduced in chapter 2. *Gold* considered whether using another person's network access credentials could amount to forgery, and *Cox* concerned the extension of the offence of criminal damage to acts occasioning the inoperability of a software-controlled saw by way of data manipulation and deletion. Immediately, even from this brief summation, a clear difference between the categorisation of the resulting harm and the conduct normally falling within the bounds of such an offence arises. *Gold* dealt with legitimate credentials being used by those without authorisation, an act not correlated with the creation of a false instrument that purports to be genuine. *Cox*, however, dealt with data deletion, an act at least in some way synonymous with

[123] See, James Chalmers and Fiona Leverick, 'Fair Labelling in Criminal Law' (2008) 71(2) *Modern Law Review* 55.

[124] [1988] 2 All ER 186.

destruction and damage. This is not a coincidence. The selection of the charges and the resulting outcomes in these two influential prosecutions can be better understood by considering how the 'role' of the computer in the conduct was conceived at the time. That is, was the 'computer' the target of the conduct, or a tool?

(a) The role of the 'computer' in Gold

Gold involved a prosecution that would ultimately be described by the court as requiring, were it to be successful, the acceptance of a 'forced analogy'.[125] The failure of the prosecution as against the conduct of Mr Gold and Mr Schifreen in *Gold* served as a key motivator for exploring the need for computer-specific criminal legislation and stands as an example of where an analogy with pre-existing offences can fail. The use of legitimate access credentials was not the same as creating a false instrument. *Gold* has since been the subject of much discussion, both pre and post the implementation of the CMA. It has largely been relied upon as a contextual focal point to frame the 'problem' the CMA was designed to solve. Indeed, such was the purpose of the reference to the case in chapter 2.

Lloyd has observed that '[c]overage of cases such as *R v Gold*, although interesting and valuable … has lost much of its relevance because of the passage of the Computer Misuse Act'.[126] However, despite the attention *Gold* has continually received, none of that attention appears to engage substantively with, or question, the identification of the harm resulting from the defendants' actions. Nor the appropriateness of the selection of the offence of forgery for the ultimate prosecution. Much reference appears to proceed with an acceptance of the decision to prosecute the conduct in that form, rather than consider the effect if other avenues for criminal prosecution were pursued. On this basis, it may instead be the case that, contrary to Lloyd's assertion, *Gold* has not lost its contemporary relevance.

---

[125] Ibid 191, referring to the judgement of Lord Lane CJ in *R v Gold; R v Schifreen* [1987] 3 All ER 618, 622-3.

[126] Ian Lloyd, 'Crime and the Computer Book Review' (1992) 6(1) *International Review of Law, Computers & Technology* 225, 244.

Analysis of *Gold* often stops at the point of establishing that the use of otherwise genuine access credentials could not amount to a false instrument. The ultimate overturning of the initial convictions of Mr Gold and Mr Schifreen, the observations by the Court as to the difficulties in analogising the conduct before them with the statutory construction of the offence as charged, along with their unwillingness to be proactive in their interpretation, is viewed as adequate to support legislative intervention. However, those conclusions were based on framing the defendant's conduct as against the Prestel service itself. That is, as conduct falling within the first category of the computer crime typology: the Prestel service was the *target* of the wrongful conduct.

If the Prestel service was the target, then the harm was in the defendants gaining access: they breached the integrity of the system. Implicit in this identification is the acceptance that this conduct, at the time, was a new phenomenon. The focus was on access to the system, rather than the conduct that access enabled: for instance, the fraudulent sending of emails, or in the case of the first defendant who was not himself a paid subscriber to Prestel, the fraudulent obtaining of a service. However, the identification of the harm as the obtaining of access to the network meant that focus centred on finding a provision that might best fit that notion of gaining unauthorised access. When the analogy with forgery failed, the natural response was to suggest new legislation.

It remains appropriate that the conduct of the defendants ought not to have been deemed to contravene the *Forgery and Counterfeiting Act 1981*. That is a position accepted by many commentators[127] and the Law Commission report.[128] However, had the focus been on the conduct the defendants put that access to, charges for dishonestly obtaining services might have been pursued. The effect here is to shift the categorisation of the role of computing technology (the Prestel network) from the first category to the second: from

[127] See, eg, Kelly Stein, "Unauthorised access" and the UK Computer Misuse Act 1990: House of Lords "leaves no room" for ambiguity' [2000] *Computer and Telecommunications Law Review* 63; Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change' (2006) 70 *Journal of Criminal Law* 424, 427-29; but cf Li-Min Tan and M Newman, Computer Misuse and the Law (1991) 11 *International Journal of Information Management* 282, 284.

[128] Law Commission, 'Computer Misuse' (Report No 186 Cm 819, 1989), [2.3], [2.5].

target to *tool*. Such an offence existed at the time under the *Theft Act 1978*, which was repealed and replaced by the *Fraud Act 2006* (the 'FA').

Under the *Theft Act 1978*, it was an offence for a person 'by any deception dishonestly [to obtain] services from another'.[129] The Prestel network was a paid subscription-based telecommunications service. The defendants in using access credentials for which they were not authorised dishonestly obtained use of the Prestel network without payment. One of the reasons why such a charge was not pursued relates to the belief, explored in chapter 2, that any offence based on deception would fail if the conduct in question relied on a computer in making the relevant decision upon which a deception would be alleged. Relying on the obiter in *Davies v Flackett*[130] and *Holmes v Governor of Brixton Prison*,[131] it was assumed that the Prestel service, having no mind, could not be said to have been deceived by the use of genuine access credentials that were typed by users to whom those credentials did not belong.[132]

On this basis, while amendments to the FA would ultimately rectify this deficiency by removing the question of deception and separately specifying that it is indeed possible to commit fraud against machines,[133] it is unlikely that at the time that the conduct in *Gold* occurred a charge for 'obtaining services from another by deception' would have been successful. Adopting the prevailing opinion at the time, despite it not appearing to have been directly decided, the Prestel network would likely have been deemed incapable of being deceived.[134]

---

[129] section 1. Now, *Fraud Act 2006* s 11.

[130] [1973] RTR 8.

[131] [2005] 1 All ER 490.

[132] *Davies* [1973] RTR 8, [12].

[133] See, eg, *Fraud Act 2006* s 2(5): Fraud by misrepresentation:

> a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

[134] Interestingly, with the continued development of artificial intelligence and machine learning technologies we may be soon approaching the point where this initial distinction with respect to machines and 'being deceived', despite no longer being required, would be untenable. Computers can now arguable indeed be 'deceived'. New 'machines', or bots, designed to learn to play poker are

However, a fundamental difference between the potential response to that charge being unsuccessful arises when considered against the observations of the court in *Gold* itself. In identifying the conduct as belonging to the second classification, that the use of the Prestel service was as a tool to enable further criminal conduct, the failure of the provision to respond to the conduct would likely have been met with calls to reform, amend, or expand the existing provision. That is, the legal issue would have centred on the definition of 'deception'. Recommendations could have then come in the form of specifically accounting for computers and networks, or, as indeed subsequently occurred, the concept of deception could be abandoned. The most appropriate response to the problem of a machine being incapable of being deceived is to modify the notion that only a human can be the subject of deceptive acts.[135]

If these deception-based offences had been pursued in *Gold*, rather than the offence of forgery, it becomes unlikely that any subsequent calls for full-scale reform through the construction of a new legislative regime would be accepted or regarded as necessary to rectify the resulting prosecutorial failing. Indeed, the consolidation and amendments introduced in the FA independently achieved such a result. The amendment process that resulted in the implementation of the FA, without any consideration of the CMA,[136] was indirectly conceived to address this same problem.

The introduction of the FA sought to consolidate, unify and provide a statutory basis for the offences constituting fraud. The FA abolished crimes based on deception, and instead focused on the objective 'dishonesty' of the accused's actions. The tension between deception and machines was an important consideration in the reform of fraud. The Law Commission report observed that:

---

perhaps the best example of this. These machines learn to deceive players, and also make tactical errors themselves when deceived by the human they are playing with. See, Adam Kucharski, 'Why Power is the Ultimate Test for Thinking Machines' (2016) (Oct) *Wired* 53.

[135] See (n 133).

[136] Law Commission, 'Fraud' (Report No 276 Cm 5560, 2002) [4.6-4.7]. The CMA was mentioned once in the report recommending the adoption of the Fraud Act. That mention was not in relation to the question of the deception of a machine, but instead in relation to offences potentially applicable to the theft of trade secrets.

> A machine has no mind, so it cannot believe a proposition to be true or false, and therefore cannot be deceived. A person who dishonestly obtains a benefit by giving false information to a computer or machine is not guilty of any deception offence. Where the benefit obtained is property, he or she will normally be guilty of theft, but where there is something other than property (such as a service), there may well be no offence at all.[137]

However, by shifting focus to an assessment of the dishonesty of an accused's actions, the presence or use of any technological medium involved becomes irrelevant. Criminality is determined on the dishonesty of accused's conduct, not on considering any subjective deception on the part of the victim/provider/service. The dishonesty of an accused's conduct is subject to a two-step test:[138] first, would the accused's behaviour be regarded as dishonest by the ordinary standards of reasonable and honest people? Second, was the accused aware that their conduct would be regarded as such?[139]

Most relevantly for our assessment of the underlying facts in *Gold*, the FA now includes a reformulated offence of 'obtaining services dishonestly'.[140] This reformulation provides:

> (1) A person is guilty of an offence under this section if he obtains services for himself or another—
> (a) by a dishonest act, and
> (b) in breach of subsection (2).
>
> (2) A person obtains services in breach of this subsection if—
> (a) they are made available on the basis that payment has been, is being or will be made for or in respect of them,
> (b) he obtains them without any payment having been made for or in respect of them or without payment having been made in full, and
> I when he obtains them, he knows—
> (i) that they are being made available on the basis described in paragraph (a), or
> (ii) that they might be,

[137] Ibid [3.34].

[138] *R v Ghosh* [1982] QB 1053.

[139] *Cf Ivey v Genting Casinos* [2017] UKSC 67 (especially [52]-[75]); Matthew Dyson and Paul Jarvis, 'Poison Ivey or Herbal Leaf?' (2018) 134 *Law Quarterly Review* 198; Graham Virgo, 'Cheating and Dishonesty' (2018) 77 *Cambridge Law Review* 18; Karl Laird, 'Dishonesty: Ivey v Genting Casinos UK Ltd (t/a Crockfords Club)' (2018) 5 *Criminal Law Review* 395.

[140] *Fraud Act 2006* s 11.

but intends that payment will not be made, or will not be made in full.

Arguably, this new formulation would likely have covered the actions of the defendants in *Gold* had it existed at the time. Their use of access credentials for which they had no authorisation was dishonest: honest and reasonable people would not expect the access credentials of a software engineer to be used by anyone other than that engineer, of which the defendants were clearly aware. The Prestel service was made available with the expectation that users would pay for access, and the defendants also knew that to be the case. They did not pay for their access. Perhaps most tellingly, current CPS guidelines for this offence lists as its first example of conduct envisaged to fall within its scope as 'obtaining chargeable data or software over the internet without paying'.[141]

Equally applicable if the same facts were to occur today, if not more so, would be the offence of fraud by false representation.[142] This offence provides:

> (1) A person is in breach of this section if he—
> (a) dishonestly makes a false representation, and
> (b) intends, by making that representati–n -
> (i) to make gain for himself or another, or
> (ii) to cause loss to another or to expose another to a risk of loss
> …
>
> (5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

Subsection 5 was specifically included in this offence to deal with, for example, potential avenues of fraud relating to the use of chip and pin debit and credit cards: the terminal validates the pin being entered against the information stored on the card without human intervention.[143] Interestingly, this is a similar mechanism for the validation of access credentials utilised in *Gold*. Indeed, many instances of unauthorised

---

[141] The Crown Prosecution Service, 'The Fraud Act 2006' *CPS Guidelines* <http://www.cps.gov.uk/legal/d_to_g/fraud_act/>.

[142] *Fraud Act 2006* s 2.

[143] Hansard, HL, 4 March 2006, col 1108 (Attorney General).

access to computer material would appear to fall within the scope of this offence, at least where legitimate passwords are used as representations of an entitlement to gain access.

It might be the case that the failure of the prosecution in *Gold*, while still the likely outcome even if the above alternatives were pursued, ultimately signified not a failure of the law to keep pace with technological change, but rather a failure to accurately identify the nature of the conduct involved. By identifying the Prestel service as the target, the selection of the charge of forgery was the most appropriate on the basis of analogy. Where the Prestel service was merely a tool, the most analogous offences were those of deception. This argument can, of course, only be made with the benefit of hindsight. However, the same pattern holds true in *Cox*.

(b) The 'role' of the computer in Cox

Cox, it will be recalled, involved a defendant who gained physical access to a saw that was controlled by software which allowed it to cut pre-determined patterns in an automated fashion as part of a production line. In the context of an employment dispute, the defendant erased the software, rendering the saw inoperable for the purpose of the production line, despite the saw still functioning manually. This case involved a successful prosecution for the intentional damage to the saw, contrary to the *Criminal Damage Act 1971* ('CDA') sub-section 1(1). In accepting and following the decision in the earlier case of *R v Henderson & Battley*[144] which involved damage to vacant land, the court determined that the accused had caused damage to the saw in the sense that the deletion of the software required 'time and labour and money to be expended' on the part the employer to rectify.[145] The CDA was expanded to apply in circumstances where software deletion inhibited the operation of personal property.

The conduct in *Cox* clearly falls within the second category of the computer crime typology: the use of a computer as a *tool*. The conduct of the defendant can be considered the functional equivalent of using a 'computer' when he erased the software. The

[144] (Unreported, Court of Appeal Criminal Division, 29 November 1984).

[145] Ibid 58.

defendant either intended to impair the operation of the saw directly or intended to cause economic loss to his former employer. Despite the saw's operation being controlled by software, it remained a saw. The existence of software merely expanded the ways in which the defendant could give effect to the harm he intended to cause.

Where conduct falls within this second category, the court appears more willing to take steps to find the necessary analogy and to interpret and apply the law accordingly. However, this willingness is again dependent on the identification of the appropriate harm and the relation of this harm to the charge that is ultimately selected. In *Cox*, the harm centred on the experienced damage to the operation of the saw: the fact the harm was occasioned by the deletion of software had no bearing on the harm experienced. A charge for criminal damage was thus the logical choice. That software was involved necessarily complicated the reasoning of the court given the offence of criminal damage is inherently centred on physical property. However, the further analogy to the value of the vacant land resolved this: causing damage to 'something' seemingly intangible that ultimately impacted upon another's use and enjoyment of tangible property, while convoluted, was not especially novel.

The response to *Cox* was not one of criticism of the outcome, but rather one that questioned the inherent complexity required in its reasoning. The decision in *Cox* did not provoke calls for legislative intervention in respect of computers but instead gave rise to calls to rethink and consider the offence of criminal damage carefully in respect of its interaction with computers. That these questions were ultimately taken up in the context of the development of the CMA was not, on the face of the decision, the foreseeable consequence. That, instead, was more the product of its proximity to the high-profile failure in *Gold*.

(c) The typology as a policy tool

As can be observed in this brief analysis of the *Gold* and *Cox*, the computer crime typology can be a useful tool to highlight the observable trends across the evolution of the criminal law and to observe and understand the subsequent effect of (mis)identifying the role of the computer in a given course of conduct. This is particularly the case when focus is placed on the identification of the harm alleged to have occurred. It further provides a

means of considering the appropriateness of a 'computer-specific' offence. A properly constructed offence ought to confine its scope to apply only to those situations that can be said to fall within the first category: where the computer is the target of the conduct in question.

IV WHAT THEN FOR THE CMA?

The CMA was formulated and justified on the basis that computing technology was new and unique; it created harms and opportunities unknown to the criminal law. This resulted in a gap in the ability of the criminal law to respond to the misuse of computers, and it would be difficult for the general criminal law to keep up as computing technologies evolved. These arguments, while logical at the time, would ultimately prove to lack a suitable degree of nuance. Indeed, general offences do not exist in a vacuum, and they too have continued to evolve independently to respond to the misuse of computers: in the case of fraud, the challenge of computers and 'deception' based offences would ultimately be resolved without any reference to challenges posed by 'hacking' or computer crime more generally.

The section 1 offence, as shown above, applies not only in circumstances where the general criminal may not reach, but also to those where it is clearly capable of applying effectively. If the degree of overlap is indeed impermissible, what is the solution? Theft, as briefly noted above, could be adapted to treat data as a limited form of property, as has been the approach adopted in New Zealand.[146] But what of the section 1 offence itself?

The arguments throughout this thesis would suggest that a renewed approach of offence-by-offence consideration be adopted; much like the one initially proposed by the Law Commission but ultimately not undertaken. That broader project, if properly carried out, will serve to more clearly identify and delimit the circumstances where there is legitimately no coverage of the criminal law for conduct deemed harmful. Further attention also needs to be placed on the interaction of the civil law and the criminal law with respect to computing technologies. This kind of analysis, however, requires a deeper

[146] See *Dixon v The Queen* [2015] NZSC 147; Katherine Hu, 'Property or not? Digital files under the criminal law' (2017) 4 *Public Interest Law Journal of New Zealand* 106.

consideration of the data vs information vs property tension, which remains fundamentally unresolved.

It may ultimately be that the section 1 offence ought to be curtailed through more clearly articulated interpretative guidance to limit its breadth, be it in the form, as suggested in Chapter 4, that a definition of 'computer' be adopted, or that the actus reus be restricted to circumstances where an 'access' beyond merely causing the computer to perform a function be required. Given the scale of non-harmful, or trivially harmful, conduct currently included within its scope, it may be proper to abolish the offence and leave such conduct to the civil law.

A proposal like this immediately raises questions as to how such a shift could impact the placing of the burden to take action against unlawful interference with computers and data. On the one hand, it might be suggested that it is proper that the obligation falls on the State to investigate and prosecute harmful conduct involving computers through the criminal law: the average citizen has neither the expertise nor resources to pursue those who would infringe their interests in the proper functioning of their computer, or the integrity of their data. However, the experience since the implementation of the CMA, that is the limited number of cases in which conduct constituting offences only under the CMA are pursued,[147] has arguably been that the State too is insufficiently resourced to respond appropriately. The effect is an enforcement gap. In focusing on giving the State the tools to pursue wrongdoing involving computers, individuals and corporations have been left without their own recourse. Were a form of civil action available, more opportunity would be created to respond in a meaningful way to the variety of cyber threats that presently exist, particularly those not undertake in the course of more serious criminal conduct that warrants the use of the resources of the State. Such a delineation, between civil and criminal, would also serve to better restrict and focus the bounds of legitimate criminalisation of computer misuse.

V CONCLUSION

The CMA was formulated in the period before substantive criminological work began apace. Its framing, therefore, did not benefit from consideration of the ways in

[147] See Chapter 3 at 123-8.

which computers and networks could be considered as being the target of criminal conduct, a tool in the commission of criminal conduct, or instead if their presence and use were merely incidental to the crime. It was also formulated before new and sophisticated methods and techniques arose to facilitate the commission of an ever-increasing spectrum of criminal conduct. The nature and effect of this criminal conduct, however, has increasingly evolved to resemble conduct already well known to the criminal law.

The continued development of computing technology and its implementation into many facets beyond those comprehended in 1989, has resulted in what might be described as a breaking down of the barriers of the application of the general law to those technologies. When computers were abstracted and disconnected from the result of the conduct, it made sense to treat computers as 'new' and 'unique'. The conduct did not always easily find an analogy with the existing law or particular elements of an offence (like the requirement of 'deception' in the pre-2006 formulation of fraud) which may have rendered a prosecution futile. This is largely no longer the case.

While the CMA's section 3 offence, and to a lesser extent its section 3A offences, address conduct largely unknown to the criminal law and thus warranting special treatment, we are left, however, with the CMA's section 1 offence that no longer operates as intended and as initially justified. The section 1 offence can apply irrespective of the 'role' a computer plays in the commission of a course of criminal law. It presumes wrongdoing, and now, with the networked, decentralised and sensor-based applications of computing technologies, has the potential to apply in circumstances well beyond that initially contemplated and intended. Its presumption of a criminal harm from the mere breach of a computer's integrity is no longer convincing given the breadth of harm possible; from the mere trivial harm which is on its face better dealt with by the civil law, to the dangerous, damaging, costly, or catastrophic, the proper realm of the criminal law.

Returning to the normative model established in chapter 1, the evolution of computing technologies and our understanding and experience of computer-related crime has resulted in the construction of the section 1 offence no longer properly defining a type of conduct and culpability commensurate with the harm experienced in a given

instance. Instead, it presupposes wrongdoing and is capable of being applied indiscriminately and without warning to those subject to the offence. The GDPR and the DPA have created incentives for companies and service providers to revisit and comprehensively redesign their privacy policies and terms of service, making them ever more explicit. The effect of this is to more clearly define the contractual boundaries of authorised conduct for all users of their networks or services. A breach of these contractual boundaries, however, is capable of being treated as a criminal offence by the operation of the CMA's section 1 offence, irrespective of a harmful intent. Without reform, there is a risk that it is only a matter of time before the section 1 offence becomes the default charge in any conduct involving a computer, or the access and use of personal data. Even if this risk does not materialise, the CMA is increasingly becoming unnecessary to fulfil its intended purpose: responding to breaches to the integrity of a computer. General criminal offences can be, and are, capable of achieving the same result.

Conclusion

The aim of this thesis was to argue that the justifications employed to support the formulation of the CMA's section 1 offence no longer hold true as computing technologies have evolved. The offence has been rendered unacceptably over-inclusive, permitting what can effectively be described as contracting out the ability to define the boundaries of criminal liability with respect to the use of computers to private entities.

The creation of any criminal offence ought to have regard to whether the proposed subject matter of the offence justifies the exercise of the State's power to criminalise. A suitable harm, or risk of harm, must be identified, along with a clear articulation of the wrongfulness of the conduct that brings about that harm, or risk of harm. The drafting of such an offence, ought to contain terms that are capable of clear definition and necessarily limited to forms of conduct and culpability commensurate with the harm, or risk of harm, so identified. However, with its adoption of poorly defined *technology-neutral* terms, an *actus reus* that centres on the 'causing a computer to perform a function', rather

than requiring the successful obtaining of access, a *mens rea* that delimits not on the basis of the risk of harm but on a broad conception of harm to the integrity of a computer despite the offence being defined in relation to data, the section 1 offence does not adequately balance these constraints.

The section 1 offence has the potential to operate in such an over-inclusive manner that it brings into its criminal purview conduct that would otherwise be considered sufficient grounds to amount to a mere civil wrong: conduct can become criminalised merely because it is carried out on a computer. There is no normative shift in the nature of a breach of contract, or an infringement of copyright, merely because it is facilitated by a computer. But, as the section 1 offence requires no intent beyond one to secure unauthorised access, regardless of motivation or context, such conduct is nevertheless criminalised.

The section 2 offence, while drafted with same *actus reus* as the section 1 offence, does not appear to exhibit such a degree of over-inclusivity. This is because the section 2 offence, while requiring the accused to have intended to secure unauthorised access, also requires the accused to be motivated by an ulterior criminal intent: the access intended to be secured must be pursued in the course of committing a further substantive offence. In this sense, the section 2 offence works to clarify that the malicious use of computing technologies shares that status of an 'attempt' of the substantive offence but provides clarity and works to bridge what might potentially be construed as a representative labelling gap. The character of the conduct of taking steps to secure unauthorised access is normatively transformed by operation of the further criminal intent.

The section 3 offence responds to circumstances where the operation of a computer, program or data is intentionally impaired. While the *actus reus* of the offence requires an accused to undertake an 'unauthorised act' in relation to a 'computer', adopting a similarly broad scope as to the section 1 offence, the *mens rea* requires an intention to cause an identifiable harm; to impair the operation of the computer, to prevent or hinder legitimate access or use of the computer, or to impact the reliability of data so held. The offence is thus confined to acts undertaken only where such an intent is evident. Further, the type of harm contemplated for the purpose of this offence is

delimited to the proper functioning of the computer. Serious loss and damage can arise from the intentional impairment of a computer. The section 1 offence, of course, remains applicable to the same conduct, but requires no consideration of harm or motivation.

The offences within the CMA were justified, at the time, based on the need for deterrence, the need for specific computer offences to serve a supplementary role to existing offences by criminalising conduct involving the use of computers that fell beyond their scope, that hacking was harmful in that it compromised the integrity of the target computer and this was a new harm that fell outside the experience of the criminal law, and that other jurisdictions had enacted similar provisions within their domestic criminal law. Leaving aside the validity of the claims that the offences provide a deterrence effect generally, it is difficult to accept that the section 1 offence could be said to contribute to this deterrence given the degree of 'normal' conduct that is capable of falling within its scope and not prosecuted. Indeed, were sufficient attention to be brought to the amount of conduct capable of falling within scope and yet not being prosecuted, the selective enforcement of the offence may instead work to undermine faith in the criminal law itself and could give rise to a justified sense of unfairness on the part of those who are prosecuted.[1]

In respect of the claim that the offences would operate in a supplementary role, ensuring wrongful conduct involving the use of computing technologies did not 'slip through the cracks' of the general criminal law, while the section 2 and 3 offences are capable of being viewed in such a light, the same cannot be said for the section 1 offence. The section 3 offence responds to harms elsewhere not recognised by the criminal, and the section 2 offence operates to criminalise steps taken to secure the unauthorised access to data where such access is intended to facilitate the commission of a further offence. The offence criminalises, for instance, the commencement of a course of conduct to commit fraud where that conduct relies on computing technologies. Here, the offence functions to ensure those who may not have undertaken enough steps to be prosecuted for attempted fraud do not escape criminal liability for their digital trespass, the character

[1] See, eg, Todd Haugh, 'SOX on Fish: A New Harm of Overcriminalization' (2015) 109 *Northwestern University Law Review* 835. A perception of injustice and inconsistent application of a broad offence can contribute to individuals being better placed to rationalise their decision to enter a course of conduct on the basis that the applicable law is wrong

of which is transformed by the further intent that the trespass facilitate fraud. While an argument may be made that the section 1 offence provides the same supplementary role, its application in practice extends significantly beyond this. Indeed, the offence in practice is beginning to operate to *supplant* existing offences, rather than supplement. This is likely the case with respect to data protection and more serious general offences. The CMA's section 1 offence risks becoming a 'useful' prosecutorial tool given its low burden of evidential proof.

'Hacking', the original target of the section 1 offence, is harmful. But the issue is not just whether or not hacking is harmful, this issue is whether it is sufficiently harmful to warrant the intervention of the criminal law. The section 1 offence, as drafted, does not attempt to distinguish the types of harm possible to enliven sanction, from mere nuisance or contractual breach to serious economic and social harm. Criminal culpability is presumed by mere fact of a digital trespass

While the Law Commission and Parliament were right to identify the misuse of computers as a subject for the criminal law, they were wrong to presume that any misuse ought to be criminal. While computing technology has continued to evolve, increasingly regulated by technical protection mechanisms, terms of service, policy documents and internal processes, the scope of the possible application of the offence goes beyond that supported by the claims made in implementing it. The same can be said for the subsequent amendments to substantially increase the available sentences. The CMA's section 1 offence is thus in need of reform.

The proposals listed below arise from the observations across chapters 4, 5, and 6. They are not comprehensive, nor are they suggested in and of themselves to be adequate, rather they lay the groundwork for future, targeted assessment of their suitability to respond to the section 1 offence's over-inclusivity. Further work is required.

On one view, the section 1 offence is not necessary, and ought to be repealed. It is over-inclusive and applies to conduct already covered by other offences within the CMA, as well as offences from elsewhere in the criminal law. In its place, opportunity should instead be provided for the civil law to respond, either through breach of contract or the

creation of a tort of *digital trespass* or *digital nuisance*. This thesis has not sought to establish the basis upon which such action in the civil law could be made, instead it has merely argued that the harm of digital trespass is not the proper subject of the criminal law. Future work should be directed at substantiating this possibility. It should build upon the discrete arguments already advanced,[2] and should be considered along with its potential to interact with the criminal law.[3] There is evidence that the English courts may at least be open to the idea.[4]

Alternative options for reform centre on resolving the issues with the drafting of the section 1 offence itself, highlighted throughout this thesis. In respect of the *actus reus* of the offence, the failure to provide a definition of 'computer' renders the scope of the offence uncertain, so reform aimed at attempting to limit its application is warranted. As was observed in Chapter 4, there has been a continued and sustained upwards trend in the level and degree of the incorporation of computing technologies into all manner of goods and services. The degree to which this has occurred has moved well beyond the possibilities foreseen when the CMA was drafted. The development of Internet of Things devices and the reliance on various sensor technologies is beginning to represent a fundamental shift in the way computers are interacted with. Computing technologies are no longer just 'used' in the sense envisaged by the CMA.

---

[2] See, eg, Steven Hedley, 'Cybertrespass – A Solution in Search of a Problem?' (2014) 5(2) *Journal of European Tort Law* 165; Mårten Shultz, 'The Responsible Web: How Tort Law Can Save the Internet' (2014) 5(2) *Journal of European Tort Law* 182; Darren Read, 'Should the English Legal System Adopt the US Law of Cyber-Trespass? (2011) 8(1) SCRIPTed 46; Sarah Green, 'Can a Digitized Product be the subject of conversion?' (2006) 1(M) *Lloyds Maritime and Commercial Law Quarterly* 568; Gilad Yadin, 'Beyond unauthorized access: laws of virtual reality hacking' in Woodrow Barfield and Marc J Blitz (eds), *Research Handbook on the Law of Virtual and Augmented Reality* (Elgar, 2018) 340.

[3] *Cf* Paul Barton and Viv Nissanka, 'Cyber-crime – criminal offence or civil wrong?' (2003) 19(5) *Computer Law & Security* Report 401, where some rudimentary attempts were made, however being practice oriented the authors concluded, at 405, that a civil option would not be attractive to businesses 'for the sole reason that the would-be computer hacker or virus writer will not necessarily have sufficient resources to pay any worthwhile damages for losses suffered by the business'. This hardly seems an acceptable reason as to why such conduct should remain in the realm of the criminal law.

[4] See, *Arquiva Ltd v Everything Everywwhere Ltd* [2011] EWHC 1411, where at [207] Ramsey J, in obiter, stated 'it is hard to see why a deliberate attempt through the internet unlawfully to manipulate data on a computer should not amount to trespass to that computer'; *Patchett v SPATA* [2009] EWCA Civ 717, where the majority of the Court of Appeal appeared willing to give contractual legal effect to website disclaimers.

The increased 'computerisation' of devices not only increases the bounds of the potential application of the section 1 offence, but also creates new avenues for the commission of criminally wrongful conduct. The theft of cars can be enabled by 'relaying' the signal from a radio frequency 'key' to activate a computerised lock; both simple and sophisticated forms of fraud can be facilitated; computing technology can be used to harass, intimidate, and blackmail. However, these types of conduct can be categorised by the ultimate harms produced, not the method in bringing that harm about. The target of the conduct isn't the computing technology itself, instead that technology operates as a tool in enabling that conduct. The existing offences of theft, fraud, and blackmail, amongst others, can suitably apply. The section 1 offence, in criminalising the use of computing technologies as a tool, overlaps unnecessarily with these general offences.

To reduce this overlap, clear attention needs to be directed to limiting the operation of the section 1 offence to circumstances where the computer is the target, rather than the tool. A definition thus needs to be provided to the *types* of computer to fall within the scope of the offence. Such a definition could be achieved by clearly excluding particular forms of computing technologies from the scope of the offence, especially in respect to the volume of Internet of Things devices continuing to be developed. Or the same result may be achieved indirectly by providing clarity as to the meaning of the term 'access'. As it is currently defined, 'access' includes a wide variety of conduct, including 'use'. If 'access' were limited to include a notion of 'unrestricted' or 'privileged' access, this could go some way to limiting the scope of the offence. In this sense, 'unrestricted' or 'privileged' access could imply the need to circumvent some form a technical barrier; that is, it would apply only to computing technologies and systems for which differing levels of 'access' were possible. Restrictions along these lines may go some way to limiting the application of the section 1 offence to those instances where a 'gap' in the criminal law may remain.

Additionally, the adoption of the drafting of the offence in the inchoate mode, requiring that the accused merely 'cause a computer to perform a function', gives rise to criminality too early in the chain of conduct. The offence should therefore be redrafted if it is to continue functioning on the basis that harm to the integrity of a computer is in itself sufficiently wrongful to justify criminal liability. Instead, it should at least require that the accused successfully *obtain* access. While not a comprehensive solution, such a

shift would go a significant way to reducing the offence's over-inclusiveness, and work to somewhat limit the offence to those circumstances where the computer itself is the target of the conduct. An amendment in this form would not, however, work to reduce the policy inconsistencies that can arise between other areas of the law: namely intellectual property law and data protection law. The obtaining of access to a computer or data where that access is controlled by a terms or service agreement, or is otherwise by its nature personal data, would continue to fall within the scope of the offence.

Requiring the accused to 'obtain access' before criminal liability arises would also not necessarily work to entirely limit the potential breadth of the offence. As the section 1 offence operates as an indictable offence, it would be possible to charge an accused with attempting this reformulated section 1 offence. On that basis, no effective change to the substance and application of the offence would have been achieved in practice. Therefore, the offence should also simultaneously be reverted to its previous form as a summary offence. In instances where the accused possesses an ulterior criminal intent, or an intent to impair, or was reckless as to the possibility of that impairment, the section 2 and 3 offences would remain available.

The final avenue for amendment contemplated by the observations in this thesis centres on reconsidering the notion of 'unauthorised access'. It is not sufficient to accept that that the operator of a computer, platform or service should be able contractually to define the boundaries of the conduct qualifying as criminal by ever granular data-specific terms of service. Instead, a reversion to the initial, even if erroneous, approach in *DPP v Bignell*[5] may be worth considering. If the harm is conceived as being to the integrity of the computer, then the 'class of access' or 'data of the same kind' approach is perhaps more suitable. This could serve to limit the applicability of the offence to the examples explored in chapter 5 in respect to terms of service agreements and the particular 'method' of approved access. Where an act was specifically identified as done with an intent to impair the computer, then the section 3 offence would still suitably apply. Where the data is personal data, the offences under the *Data Protection Act 2018* would apply with their non-custodial sentences. If there are other forms of particular data whose inherent qualities

[5] (1998) 1 Cr App R 1.

warrant a criminal response, than these should be specifically identified and pursued in their own respect.

The continued expansion of the application of computing technologies to new facets of everyday life have contributed to drastically expanding the scope of the section 1 offence. Without further reform of some kind, centred on the perspectives offered by criminalisation theory and criminological work rather than a desire to simplify the work of prosecutors, the *status quo* treatment of computers as warranting special criminal protection in the absence of an intended further harm beyond mere digital trespass will become ever increasingly untenable.

The CMA was formulated and justified on the basis that computing technology was new and unique; it created harms and opportunities unknown to the criminal law. This resulted in a gap in the ability of the criminal law to respond to the misuse of computers, and it would be difficult for the general criminal law to keep up as computing technologies evolved. These arguments, while logical at the time, would ultimately prove to lack a suitable degree of nuance. Where new harms have arisen with respect to actions impacting the proper operation of the computer itself, the newness was the impairment of the computer and the development of tools to enable that to happen: the target of the section 3 and 3A offences respectively. Where computers create new opportunities for known harms to occur, the challenge is not necessarily with the substantive criminal law itself. While the section 2 offence operates to bridge a potential gap in establishing what would otherwise constitute an attempt of a general offence where the necessary conduct required the misuse of a computer, those general offences (in their inchoate or completed forms) can suitably apply where the intended conduct is carried out, or moves beyond the merely preparator. Indeed, general offences do not exist in a vacuum and they too have continued to evolve independently to respond to the misuse of computers: in the case of fraud, the challenge of computers and 'deception' based offences would ultimately be resolved without any reference to challenges posed by 'hacking' or computer crime more generally.

Traditional criminal law offences are constructed to address conduct of an accused that directly caused, or risks causing, some form of sufficiently wrongful harm. In the

most general of senses, when computers operated as external/independent devices they acted as a barrier to drawing a clear connection between the conduct of the accused in interacting with a computer and the experienced effect in a form contemplated by the criminal law. As computing technologies continue to develop and that barrier is lowered, the opportunities for general criminal offences to apply increase. In that sense, rather than the criminal law struggling to keep up with technology, when it comes to computer specific offences it may instead be the case that technology is beginning to catch-up with the law.

BIBLIOGRAPHY

A *Articles/Books/Reports*

Ablon, Lillian, et al, *Markets for cybercrime tools and stolen data: Hackers' bazaar* (Rand Corporation, 2014).

Albonetti, Celesta A, 'Prosecutorial Discretion: The Effects of Uncertainty' (1987) 21(2) *Law & Society Review* 291.

All Party Internet Group, *Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group*, 2004, London, HMSO. <https://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf>.

Alldridge, Peter, 'Computer Misuse Act 1990' (1990) 9(6) *International Banking Law* 339.

Alldridge, Peter, 'Making Criminal Law Known' in Stephen Shute and Andrew Simester (eds) *Criminal Law Theory: Doctrines of the General Part* (Oxford University Press, 2002) 103.

Anderson Ross, and Tyler Moore, 'The Economics of Information Security' (2006) 314(5799) *Science* 610.

Argy, Philip, (ed), *Computers for Lawyers* (Longman Professional, 1986).

Arthur, Raymond, 'Sending a naked selfie can be a criminal offence – but not many teenagers know this' (27 September 2017) *The Conversation* <https://theconversation.com/sending-a-naked-selfie-can-be-a-criminal-offence-but-not-many-teenagers-know-this-84149>.

Ashford, Warwick, 'UK Hit by 70 Cyber Espionage Campaigns a Month, says GCHQ' *Computer Weekly* (1 July 2013) <http://www.computerweekly.com/news/2240187230/UK-hit-by-70-cyber-espionage-campaigns-a-month-says-GCHQ>.

Ashworth, Andrew, 'Crime, Community and Creeping Consequentialism' [1996] *Criminal Law Review* 220.

Ashworth, Andrew, 'Is the criminal law a lost cause' (2000) 116 *Law Quarterly Review* 225.

Ashworth, Andrew, 'The Criminal Law's Ambivalence About Outcomes' in Rowan Cruft et al (eds) *Crime, Punishment, and Responsibility: The Jurisprudence of Antony Duff* (Oxford University Press, 2011) 159.

Ashworth, Andrew, and Jeremy Horder, *Principles of Criminal Law* (Oxford University Press, 7th ed, 2013)

Ashworth, Andrew, and Lucia Zedner, *Preventive Justice* (Oxford University Press, 2014).

Ashworth, Andrew, Lucia Zedner and Patrick Tomlin (eds), *Prevention and the Limits of the Criminal Law* (Oxford University Press, 2013).

Ashworth, Andrew, *Principles of Criminal Law* (Oxford University Press, 4th ed, 2003)

Asp, Peter, 'Preventionism and Criminalization of Nonconsummate Offences' in Andrew Ashworth, Lucia Zedner and Patrick Tomlin (eds) *Prevention and the Limits of Criminal Law* (Oxford University Press, 2013) 23.

Audal, Joseph, Quincy Lu and Peter Roman, 'Computer Crime' (2008) 48 *American Criminal Law Review* 233.

Bainbridge, David, 'Hacking – the unauthorised access of computer systems: the legal implications' (1989) 52 *Modern Law Review* 236.

Bainbridge, David, *Introduction to Information Technology Law* (Longman, 6th ed, 2007).

Baker, Denis, 'The Moral Limits of Criminalising Remote Harms' (2007) 10(3) *New Criminal Law Review: An International and Interdisciplinary Journal* 370.

Bamforth, Nicholas, *Sexuality, Morals and Justice* (Cassell, 1997).

Bangs, Greg, 'New Ransomware and Cyber Extortion Schemes Hold Businesses Hostage' (2014) 61(8) *Risk Management* 30.

Barton, Paul, and Viv Nissanka, 'Cyber-crime – criminal offence or civil wrong?' (2003) 19(5) *Computer Law & Security* Report 401.

Baxter, William F, 'Separation of Powers, Prosecutorial Discretion, and the "Common Law" Nature of Antitrust Law' (1981-2) 60 *Texas Law Review* 661.

BBC News, 'Sexting boy's naked selfie recorded as crime by police' (3 September 2015) <http://www.bbc.com/news/uk-34136388>.

BBC, 'The Computer Literacy Project Archive' (27 June 2018) <https://computer-literacy-project.pilots.bbcconnectedstudio.co.uk>.

Bennet Moses, Lyria, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (2007) 7 *University of Illinois Journal of Law, Technology and Policy* 239.

Bennett Moses, Lyria, 'Agents of Change: How the Law "Copes" with Technological Change' (2011) 20(4) *Griffith Law Review* 763.

Bennett Moses, Lyria, 'How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target' (2013) 5(1) *Law, Innovation and Technology* 1.

Bently, Lionel, 'Copyright and the Victorian Internet: Telegraphic Property Laws in Colonial Australia' (2004) 38 *Loyola of Los Angeles Law Review* 71.

Beyer, Kurt, *Grace Hopper and the Invention of the Information Age* (MIT Press, 2012).

Bijker, Wiebe E, *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change* (MIT Press, 1995).

Bijker, Wiebe E, Thomas P Hughes and Trevor Pinch (eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (MIT Press, 1987).

Bowles, Stephen, and Julio Hernandez-Castro, 'The first 10 years of the Trojan Horse defence' (2015) (Jan) *Computer Fraud & Security* 5.

Braithwaite, John, and Philip Pettit, *Not Just Deserts: A Republican Theory of Criminal Justice* (Clarendon Press, 1990).

Brenner, Susan, 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9(4) *Virginia Journal of Law and Technology* 13.

Brenner, Susan, 'Is There Such a Thing as "Virtual Crime"?', (2001) 4(1) *California Criminal Law Review* 3.

Brenner, Susan, *Law in an Era of Smart Technologies* (Oxford University Press, 2007).

Brenner, Susan W, Brian Carrier and Jef Henninger, 'The Trojan Horse Defence in Cybercrime Cases' (2004) 21(1) *Santa Clara High Technology Law* Journal 1.

Brock, Deborah R, et al, *Criminalization, Representation, Regulation: Thinking Differently About Crime* (University of Toronto Press, 2014).

Bronitt, Simon, and Bernadette McSherry, *Principles of Criminal Law* (Thomson Reuters, 3rd ed, 2010).

Bronitt, Simon, and Bernadette McSherry, *Principles of Criminal Law* (Thomson Reuters, 4th ed, 2017).

Broome Williams, Kathleen, and James C Bradford, *Grace Hopper: Admiral of the Cyber Sea* (Naval Institute Press, 2013).

Brown, Darryl K, 'Criminal Law's Unfortunate Triumph Over Administrative Law' (2011) 7(4) *Journal of Law, Economics and Policy* 657.

Brown, Darryl, 'Prosecutors and Overcriminalization: Thoughts on Political Dynamics and a Doctrinal Response' (2009) 6 *Ohio State Journal of Criminal Law* 543.

Brown, Geoffrey, 'Is there an Ethics of Computing?' (1991) 8 *Journal of Applied Philosophy* 19.

Brownsword, Roger, 'Code, Control, and Choice: Why East is East and West is West' (2005) 25 *Legal Studies* 1.

Bywater, André, 'Cybercrime & Security Update: Prosecutors confirm 702 hacking cases charged', *Cordery Legal Compliance* (24 November 2014) <http://www.corderycompliance.com/cybercr ime-security-update-prosecutors-confirm-702-hacking-cases-charged/?>.

Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (London, 2011).

Cahill, Michael T, 'Inchoate Crimes' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 513.

Carvalho, Henrique, *The Preventive Turn in Criminal Law* (Oxford University Press, 2017).

Chalmers, James, and Fiona Leverick, 'Fair Labelling in Criminal Law' (2008) 71(2) *Modern Law Review* 55.

Charlesworth, Andrew, '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.

Child, JJ, 'The Structure, Coherence and Limits of inchoate liability: the new ulterior element' (2014) 34(4) *Legal Studies* 537.

Child, JJ, and A Hunt, 'Mens rea and the general inchoate offences: another new culpability framework' (2012) *NI Legal Q* 245.

Christie, Anna Louise, 'Should the Law of Theft Extend to Information?' (2005) 69 *Journal of Criminal Law* 349.

Clarkson, Christopher M.V., 'Attempt: The Conduct Requirement' (2009) 29(1) *Oxford Journal of Legal Studies* 25.

Clough, Jonathan, 'Data Theft? Cybercrime and the Increasing Criminalisation of Access to Data' (2011) 22 *Criminal Law Forum* 145.

Clough, Jonathan, *Principles of Cybercrime* (Cambridge University Press, 2nd ed, 2015).

Collingridge, David, *The Social Control of Technology* (Printer, 1980).

Computer Crime and Intellectual Property Section, US Department of Justice, The National Information Infrastructure Protection Act of 1996, *Legislative Analysis* (1996) <http://www.irational.org/APD/CCIPS/1030_anal.html>.

Confederation of British Industry, 'Submission to the Law Commission on Working Paper No. 110 on Computer Misuse--The CBI Submission Part II' (1990) 6(2) *Computer Law and Security Report* 23.

Constant, Sarah A, 'The Computer Fraud and Abuse Act: A Prosecutor's Dream and a Hacker's Worst Nightmare – The Case Against Aaron Swartz and the Need to Reform the CFAA' (2013) 16 *Tulane Journal of Technology and Intellectual Property* 231.

Copeland, Duncan G, and James L McKenney, 'Airline Reservation Systems: Lessons from History' (1988) 12(3) *Management Information Systems Quarterly* 353.

Cornwall, Hugo, (alias Peter Sommer), 'Hacking away at computer law reform' (1988) 138 *New Law Journal* 702.

Crofts, Thomas, and Eva Lievens, 'Sexting and the Law' in M Walrave et al (eds), *Sexting: Palgrave Studies in Cyberpsychology* (Palgrave Macmillan, 2018) 119.

Danymol, R, et al, 'Real-time communication system design using RTL-SDR and Raspberry Pi' (Paper presented at the 2013 International Conference on Advanced Computing and Communication Systems, Coimbatore, India, 19 December 2013).

Denning, Peter J, 'Computer Viruses', *NASA Research Institute for Advanced Computer Sciences* (21 March 1988) <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19890017050.pdf>.

Devlin, Patrick, *The Enforcement of Morals* (Oxford University Press, 1965).

Donovan, Tristan, *Replay: The History of Video Games* (Yellow Ant, 2010).

Downing, Richard, 'Shoring Up the Weakest Link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime' (2005) 43 *Columbia Journal of Transnational Law* 705.

Dubber, Markus D, 'The Possession Paradigm: The Special Part and the Police Model of the Criminal Process' in RA Duff and Stuart Green (eds) *Defining Crimes: Essays on The Special Part of the Criminal Law* (Oxford University Press, 2005) 91.

Dubber, Markus, 'Criminal Law Between Public and Private Law' in RA Duff et al (eds) *The Boundaries of the Criminal Law* (Oxford University Press, 2010) 191.

Dubber, Markus, 'Policing Possession: The War on Crime and the End of Criminal Law' (2001) 91(4) *Journal of Criminal Law & Criminology* 829.

Duff, RA, 'Harms and Wrongs' (2001) 5 *Buffalo Criminal Law Review* 13.

Duff, RA, 'Intentions Legal and Philosophical' (1989) 9(1) *Oxford Journal of Legal Studies* 76.

Duff, RA, 'Towards a Theory of Criminal Law' (2010) 84(1) *Aristotelian Society Supplementary* 19.

Duff, RA, *Criminal Attempts* (Oxford University Press, 1996).

Duff, RA, et al 'Towards a Theory of Criminalization' in RA Duff et al (eds) *Criminalization* (Oxford University Press, 2014) 1.

Duff, RA, *Punishment, Communication, and Community* (Oxford University Press, 2001).

Dunn, John E, 'Watch our ads or we'll use your CPU for cryptomining', *naked security by SOPHOS* (14 February 2018) <www.nakedsecurity.sophos.com/2018/02/14/watch-our-ads-or-well-use-your-cpu-for-cryptoming/>.

Durumeric, Zakir, et al, 'The Matter of Heartbleed' in *Proceedings of the 2014 Conference on Internet Measurement*, November 5-7, 2014, Vancouver, Canada.

Dworkin, Ronald, *Law's Empire* (Fontana, 1986).

Dwyer, John P, 'The Pathology of Symbolic Legislation' (1990) 17 *Ecology Law Quarterly* 233.

Dyson, Matthew 'Tortious Apples and Criminal Oranges' in Matthew Dyson, (ed), *Comparing Tort and Crime* (Cambridge University Press, 2015) 416.

Dyson, Matthew, 'The Timing of Tortious and Criminal Actions for the Same Wrong' (2012) 71(1) *Cambridge Law Journal* 86.

Dyson, Matthew, and John Randall, 'England's splendid isolation' in Matthew Dyson (ed), *Comparing Tort and Crime* (Cambridge University Press, 2015) 18.

Dyson, Matthew, and Paul Jarvis, 'Poison Ivey or Herbal Leaf?' (2018) 134 *Law Quarterly Review* 198.

Easterbrook, Frank, 'Cyberspace and the law of the horse' (1996) *University of Chicago Legal Forum* 7.

Eckert, John Presper, et al, 'The UNIVAC System' (Conference Paper, 1951 International Workshop on Managing Requirements Knowledge, 10 December 1951) 6.

Edwards, James, 'Uses and Misuses of Criminalisation' (DPhil Thesis, The University of Oxford, 2011).

Eisikovits, Nir, 'Moral Luck and the Criminal Law' in Joseph Campbell et al (eds) *Law and Social Justice* (2005, MIT Press) 105.

European Union Agency for Network and Information Security, 'ENISA Threat Landscape Report 2012' (2013) available at <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/ENISAThreatLandscape>.

European Union Agency for Network and Information Security, 'ENISA Threat Landscape Report 2018' (2019) available at <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>.

Fafinski, Stefan, 'Access Denied: Computer Misuse in an Era of Technological Change' (2006) 70 *Journal of Criminal Law* 424.

Fafinski, Stefan, 'Computer Use and Misuse: The Constellation of Control' (PhD Thesis, University of Leeds, September 2008).

Fafinski, Stefan, *Computer Misuse: Response, Regulation and the Law* (Willan Publishing, 2013) 7.

Fanning, Kurt, 'Minimizing the Cost of Malware' (2015) 26(3) *Journal of Corporate Accounting & Finance* 7.

Farmer, Lindsay, *Making the Modern Criminal Law* (Oxford University Press, 2016).

Feinberg, Joel, *Harm to Others: The Moral Limits of the Criminal Law* (Oxford University Press, 1987).

Feinberg, Joel, *Offence to Others* (Oxford University Press, 1988).

Feinberg, Stephen, 'Memories of Election Night Predictions Past: Psephologists and Statisticians at Work' (2007) 20(4) *CHANCE* 8.

Felten, Edward, et al, 'Web Spoofing: an Internet Con Game' (Paper presented at the 20th National Information Systems Security Conference, Baltimore, United States of America, 7 October 1997).

Finifter, Matthew, et al, 'An Empirical Study of Vulnerability Rewards Programs' (Paper presented at the 22nd USENIX Security Symposium, Washington DC, United States of America, 14 August 2013).

Finkelstein, Claire, 'Is Risk a Harm?' (2003) 151 *University of Pennsylvania Law Review* 963.

Finnis, John, *Natural Law and Natural Rights* (Oxford University Press, 1980).

FireEye, 'M-Trends 2019', *FireEye,* (2019) <https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html>, 7-8.

Fletcher, George, *Rethinking Criminal Law* (Little, Brown & Co., 1978).

Gamero-Garrido, Alexander, et al, 'Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research' (2017) *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* 150.

Garland, David, 'The Rise of Risk' in Richard V Ericson and Aaron Doyle (eds) *Risk and Morality* (University of Toronto Press, 2003) 48.

Glazebrook, Peter, 'Should We Have a Law of Attempted Crime?' (1969) 85 *Law Quarterly Review* 28.

Goodman, Marc, and Susan Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 10(2) *International Journal of Law and Information Technology* 139.

Grabosky, Peter, 'Virtual Criminality: Old Wine in New Bottles' (2001) 10 *Social & Legal Studies* 243.

Green, Sarah, 'Can a Digitized Product be the subject of conversion?' (2006) 1(M) *Lloyds Maritime and Commercial Law Quarterly* 568.

Green, Stuart, 'Just Deserts in an Unjust Society' in RA Duff and Stuart Green (eds) *Philosophical Foundations of Criminal Law* (Oxford University Press, 2011) ch 16.

Green, Stuart, *13 Ways to Steal a Bicycle* (Harvard University Press, 2012).

Gringas, Clive, 'To be Great is to be Misunderstood: The Computer Misuse Act 1990' (1997) 3 *Computer and Telecommunications Law Review* 213.

Grout, Vic, and Nigel Houlden, 'Taking Computer Science and Programming into Schools: The Glyndŵr/BCS Turing Project' (2014) 141 *Procedia Social and Behavioural Science* 680.

Guinchard, Audrey, 'Crime in virtual worlds: The limits of criminal law' (2010) 24(2) *International Review of Law, Computers & Technology* 175.

Halbert, Debora, 'Discourses of Danger and the Computer Hacker' (1997) 13(4) *The Information Society* 361.

Hamin, Zaiton, 'Insider Cyber-Threats: Problems and Perspectives' (2000) 14(1) *International Review of Law, Computers and Technology* 105.

Hancock, Douglas, 'To What Extent Should Computer Related Crimes Be the Subject of Specific Legislative Attention' (2001) 12 *Albany Law Journal of Science and Technology* 97.

Harcourt, Bernard, 'The Collapse of the Harm Principle' (1999) 90 *Journal of Criminal Law & Criminology* 109.

Haugh, Todd, 'SOX on Fish: A New Harm of Overcriminalization' (2015) 109 *Northwestern University Law Review* 835.

Heart, HLA, *The Concept of Law* (Clarendon Press, 1961).

Heath, Alex, *A 10-year-old hacked Instagram and Facebook paid him $10,000* (3 May 2016) Tech Insider <http://www.techinsider.io/10-year-old-hacks-instagram-facebook-pays-him-10k-2016-5>.

Hedley, Steven, 'Cybertrespass – A Solution in Search of a Problem?' (2014) 5(2) *Journal of European Tort Law* 165.

Highfield, Malcolm, 'The Computer Misuse Act 1990: Understanding and Applying the Law' (2005) 5(2) *Information Security Technical Report* 51.

Hillman, Henry, Christopher Hooper, and Kim-Kwang Raymond Choo, 'Online Child Exploitation: Challenges and future research directions' (2014) 30(6) *Computer Law & Security Review* 687.

HM Government, 'National Cyber Security Strategy 2016 to 2021' (2016) <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>.

Hobbes, Thomas, 'A Dialogue Between a Philosopher and a Student, of the Common Laws of England' in Sir William Molesworth, Bart. (ed), *The English Works of Thomas Hobbes of Malmesbury: Now First Collected and Edited by Sir William Molesworth, Bart. Vol VI* (London: Bohn, 1839-45).

Hodges, Andrew, *Alan Turing: The Enigma* (Princeton University Press, 2014).

Home Office, 'Home Office Circular: Serious Crime Act 2015' (March 2015) <https://www.crimeline.info/uploads/docs/seriouscrimeact2015.pdf>.

Home Office, 'The National Crime Agency: A Plan for the Creation of a National Crime-Fighting Capability' (Cm 8097, 2011); Cabinet Office, 2010-2015 Government Policy: Cyber Security (London, 2013).

Home Office, 'Trespass in Residential Premises' (1982).

Hong, Jason, 'The State of Phishing Attacks' (2012) 55(1) *Communication of the ACM* 74.

Horder, Jeremy, 'A Critique of the Correspondence Principle in Criminal Law' (1995) *Criminal Law Review* 770.

Horder, Jeremy, 'Crimes of Ulterior Intent', in Andrew Simester and Tony Smith (eds) *Harm and Culpability* (Oxford University Press, 1996).

Horder, Jeremy, 'How Culpability Can, and Cannot, Be Denied in Under-age Sex Crimes' (2001) *Criminal Law Review* 15.

Horder, Jeremy, *Ashworth's Principles of Criminal Law* (Oxford University Press, 8th ed, 2016).

Horder, Jeremy, *Excusing Crime* (Oxford University Press, 2004).

Hörnle, Tatjana, 'Theories of Criminalization' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 679.

Hu, Katherine, 'Property or not? Digital files under the criminal law' (2017) 4 *Public Interest Law Journal of New Zealand* 106.

Hubbell Nycum, Susan, 'Legal Problems of Computer Abuse' [1977] *Washington University Law Quarterly* 527.

Hughes, Thomas, 'Technological Momentum' in Leo Marx and Merritt Roe Smith (eds), *Does Technology Drive History? The Dilemma of Technological Determinism* (MIT Press, 1994).

Husak, Douglas, 'A Liberal Theory of Excuses' (2005) 3 *Ohio State Journal of Criminal Law* 287.

Husak, Douglas, 'Reasonable Risk Creation and Overinclusive Legislation' (1998) 1 *Buffalo Criminal Law Review* 599.

Husak, Douglas, 'Strict Liability, Justice, and Proportionality' in Andrew Simester (ed) *Appraising Strict Liability* (Oxford University Press, 2005) 81.

Husak, Douglas, 'The Costs to Criminal Theory of Supposing that Intentions are Irrelevant to Permissibility' (2009) 3(1) *Criminal Law and Philosophy* 51.

Husak, Douglas, 'The De Minimus 'Defence' to Criminal Liability' in RA Duff and Stuart Green (eds) *Philosophical Foundations of Criminal Law* (Oxford University Press, 2011) 328.

Husak, Douglas, *Overcriminalisation: The Limits of the Criminal Law* (Oxford University Press, 2007).

Ingraham, Donald, 'On charging computer crime' (1980) 2(1) *Computer and Law Journal* 429.

Joint Committee on Human Rights, *Third Report of Session 2005-6, Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters* (2005-06, HC 561-I) 17-8.

Kerr, Orin S, 'Vagueness Challenges to the Computer Fraud and Abuse Act' (2009-10) 94 *Minnesota Law Review* 1561.

Kersten, Jason, 'How Two Pakistani Brothers Created the First PC Virus, *Mental Floss* (2 November 2013) <http://mentalfloss.com/article/12462/going-viral-how-two-pakastani-brothers-created-first-pc-virus>.

Klang, Mathias, 'A critical look at the regulation of computer viruses' (2003) 11 *International Journal of Law and Information Technology* 162.

Klang, Mathias, 'Virtual Sit-Ins, Civil Disobedience and Cyber Terrorism' in Mathias Klang and Andrew Murray (eds), *Human Rights in a Digital Age* (Routledge, 2005) 135.

Kleinig, John, 'Crime and the Concept of Harm' (1978) 15(1) *American Philosophical Quarterly* 27.

Klosowski, Thorin, *Build a Magic Mirror with a Raspberry Pi and an Old Monitor* (2 January 2016) Lifehacker <http://lifehacker.com/build-a-magic-mirror-with-a-raspberry-pi-and-an-old-mon-1750468358>.

Klosowski, Thorin, *How to Build a Portable Hacking Station with a Raspberry Pi and Kali Linux* (20 October 2015) Lifehacker <http://lifehacker.com/how-to-build-a-portable-hacking-station-with-a-raspberr-1739297918>.

Klosowski, Thorin, *Use a Raspberry Pi as a Tor/VPN Router for Anonymous* Browsing (28 January 2015) Lifehacker <http://lifehacker.com/use-a-raspberry-pi-as-a-tor-vpn-router-for-anonymous-br-1682296948>.

Krebs, Brian, *Mirai IoT Botnet Co-Authors Plead Guilty* (17 December 17) Krebs on Security <https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/>.

Krishnamurthy, Sandeep, and Arvind K Tripathi, 'Bounty Programmes in Free/Libre/Open Source Software' in Jürgen Bitzer and Philipp J H Schröder (eds) *The Economics of Open Source Software Development* (Elsevier, 2006) 165.

Kucharski, Adam, 'Why Power is the Ultimate Test for Thinking Machines' (2016) (Oct) *Wired* 53.

Kuehn, Andrew, and Milton Mueller, 'Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities' (August 1, 2014). 2014 TPRC Conference Paper.

Lacey, Nicola, 'Historicising Criminalisation' (2009) 72 *Modern Law Review* 936.

Lacey, Nicola, 'Legal Constructions of Crime' in M Maguire et al (eds), *The Oxford Handbook of Criminology* (Oxford University Press, 4th ed, 2007) 193

Lacey, Nicola, et al., *Reconstructing Criminal Law* (Cambridge University Press, 4th ed, 2010).

Lacey, Nicola, *In Search of Criminal Responsibility: Ideas, Interests, and Institutions* (Oxford University Press, 2016).

Lacey, Nicola, *Unspeakable Subjects* (Hart Publishing, 1998).

Laird, Karl, 'Dishonesty: Ivey v Genting Casinos UK Ltd (t/a Crockfords Club)' (2018) 5 *Criminal Law Review* 395.

Lavington, Simon, *Early British Computers*, (Digital Press, 1980).

Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988).

Law Commission, 'Consent in the Criminal Law' (Consultation Paper No 139, 1995) 245-283.

Law Commission, 'Conspiracy and Attempts' (Law Com No 318, 2009).

Law Commission, 'Conspiracy to Defraud' (Working Paper No 104, Cm 228, 1987).

Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989).

Leader-Elliot, Ian, 'Benthamite reflections on codification of the general principles of criminal liability: towards the panopticon' (2005) 9 *Buffalo Criminal Law Review* 391.

Lean, Tom, 'Prestel: The British Internet That Never Was?, *History Today* (23 August 2016) <http://www.historytoday.com/tom-lean/prestel-british-internet-never-was>.

Lean, Tom, *Electronic Dreams: How 1980s Britain Learned to Love the Computer* (Bloomsbury Sigma, 2016)

Lessig, Lawrence, 'The law of the horse: what cyberlaw might teach' (1999) 113 *Harvard Law Review* 501.

Levy, Steven *Hackers: Heroes of the Computer Revolution* (2nd ed, Penguin Books, 2001).

Leyden, John, 'UK prosecutions for hacking appear to be dropping', *The Register* (18 May 2012) <https://www.theregister.co.uk/2012/05/18/uk_hacking_prosecutions_decline/>.

Leyden, Jon, 'Car repair worker jailed over data privacy breach', *The Daily Swig* (13 November 2018) <https://portswigger.net/daily-swig/car-repair-worker-jailed-over-data-privacy-breach>.

Leydon, John, 'It may be illegal to run Heartbleed health checks – IT Lawyer', *The Register* (11 April 2014) <http://www.theregister.co.uk/2014/04/11/heartbleed_health_checking_services_may_be_illegal/>.

Lloyd, Ian, 'Crime and the Computer Book Review' (1992) 6(1) *International Review of Law, Computers & Technology* 225.

Luna, Erik, 'The Overcriminalization Phenomenon' (2005) 54 *American University Law Review* 703.

MacCormick, Neil, *Legal Right and Social Democracy* (Oxford University Press, 1982).

Macdonald, Elizabeth, 'The Council, the Computer and the Unfair Contract Terms Act 1977' (1995) 58 *Modern Law Review* 585.

MacEwan, Neil, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (2008) 12 *Criminal Law Review* 995.

Maillart, Thomas, et al, 'Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs' (2017) 3(2) *Journal of Cybersecurity* 81.

Marchant, Gary E, Braden R Allenby and Joseph R Herkert (eds), *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight, vol 7* (International Library of Ethics, Law and Technology, Springer, 2011).

Marechal, Simon, 'Advances in password cracking' (2008) 4(1) *Journal in Computer Virology* 73.

Mason, Anthony, 'The Courts as Community Institutions' (1998) 9 *Public Law Review* 83.

McCutcheon, Paul, 'Morality and the Criminal Law: Reflections on Hart-Devlin' (2002) 47 *Criminal Law Quarterly* 15.

McMillan, Robert, '*From the Flying Car to the Giant R2-D2: The Greatest MIT Hacks of All-time*' (30 March 2013) Wired <www.wired.com/2013/03/mit-hacks/>.

McSherry, Bernadette, 'Expanding the boundaries of inchoate crimes: the growing reliance on preparatory offences' in Bernadette McSherry et al (eds) *Regulating Deviance – The redirection of Criminalisation and the Futures of Criminal Law* (Hart Publishing, 2009) 141.

Melissaris, Emmanuel, 'Theories of Crime and Punishment' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 356.

Michaels, Alan, 'Constitutional Innocence', (1999) 112 *Harvard Law Review* 828.

Mill, JS, *On Liberty* (Penguin, 1974).

Milsner, Robert L, 'Recasting Prosecutorial Discretion' (1996) 86(3) *Journal of Criminal Law and Criminology* 717.

Mirkovic, Jelena, and Peter Reiger, 'A Taxonomy of DDoS attacks and DDoS Defence Mechanisms' (2004) 34(2) *ACM SIGCOMM Computer Communication Review* 39.

Mollenhoff, Clark R, *Atanasoff: Forgotten Father of the Computer* (Iowa State University Press,1988).

Moore, Michael S, 'Liberty's Constraint on What Should be Made Criminal' in Duff et al (eds) *Criminalization* (Oxford University Press, 2014) 182.

Morris, Monique W, *Pushout: The Criminalization of Black Girls in Schools* (The New Press, 2017).

Muir, James, and Pail Van Oorschot, 'Internet Geolocation: Evasion and counterevasion' (2009) 42(1) *ACM Computing Surveys* 4.

Murray, Andrew, *Information Technology* Law (3rd ed, Oxford University Press, 2016).

Nehaluddin, Ahmad, 'Hackers' criminal behaviour and law related to hacking' (2009) 15(7) *Computer and Telecommunications Law Review* 159.

New York Times, 'Goldblum Among 6 Sentenced to Jail in Equity Funding Case (Online Archive, 19 March 1975) <http://www.nytimes.com/1975/03/19/archives/goldblum-among-6-sentenced-to-jail-in-equity-funding-case.html?_r=o>.

Nicholson, Lisa H, 'Sarbanes-Oxley's Purported Over-Criminalization of Corporate Offenders' (2007) 2 *Journal of Business & Technology Law* 43.

Nissenbaum, Helen, 'Hackers and the Contested Ontology of Cyberspace' (2004) 6(2) *New Media & Society* 195.

Norrie, Alan, *Crime, Reason and History: A Critical Introduction to Criminal Law* (Cambridge University Press, 2014).

Olivenbaum, Joseph, '<CTRL> <ALT> <DEL>: Rethinking Federal Computer Crime Legislation' (1996-1997) 27 *Seton Hall Law Review* 574.

Omerod, David, 'The Fraud Act 2006: Criminalising Lying' [2007] *Criminal Law Review* 193.

Omerod, David, and David Huw Williams, *Smith's Law of Theft* (9th ed, Oxford University Press, 2007).

Omerod, David, and Karl Laird, *Smith and Hogan's Criminal Law* (14th ed, Oxford University Press, 2015).

Orford, Anne, 'Liberty, Equality, Pornography: The Bodies of Women and Human Rights Discourse' (1994) 3 *Australian Feminist Law Journal* 72.

Oriol, Taiwo A., 'Bugs for Sale: Legal and Ethical Properties of the Market in Software Vulnerabilities' (2011) 28 *Journal of Computer & Information Law* 451.

Parikka, Jussi, *Digital Contagions A Media Archaeology of Computer Viruses* (Peter Lang Publishing, 2007).

Perlis, Alan J, 'The Synthesis of Algorithmic Systems' (1967) 14(1) *Journal of the Association for Computing Machinery* 1.

Poole, Oliver, and Justin Davenport, 'Scotland Yard starts new team to look into hacking', *London Evening Standard* (10 June 2011) < https://web.archive.org/web/20110614082416/http://www.thisislondon.co.uk/standard/article-23959562-scotland-yard-starts-new-team-to-look-into-hacking.do>.

Porcar, Esteban, Alvaro M Pons, and Amalia Lorente, 'Visual and Ocular Effects from the Use of Flat-Panel Displays' (2016) 9(6) *International Journal of Ophthalmology* 881.

Potter, H, *Pornography* (Federation Press, 1996).

Press Association, 'UK hacker jailed for six years for blackmailing pornography site users', *the Guardian*, (9 April 2019) <https://www.theguardian.com/uk-news/2019/apr/09/uk-hacker-jailed-six-years-blackmailing-pornography-website-users>.

Price, Monroe E, 'The Newness of New Technology' (2001) 22 *Cardozo Law Review* 1885.

Purdy, Kevin, 'How Apple Co-Founder Steve Wozniak Gets Things Done', *Lifehacker* (Interview, 23 April 2009) <https://www.lifehacker.com.au/2 009/04/how-apple-co-founder-steve-wozniak-gets-things-done/>.

Quinn, Katie, 'Computer Evidence in Criminal Proceedings: Farewell to the ill-fated s 69 of the Police and Criminal Evidence Act 1984' (2001) 5(3) *International Journal of Evidence and Proof* 174.

Ramage, Sally, and Edward Wheeler, 'The criminal offence of computer hacking' (2011) 203 *Criminal Lawyer* 3.

Ramsay, Peter, 'Democratic Limits to Preventative Criminal Law' in Andrew Ashworth, Lucia Zedner and Patrick Tomlin (eds), *Prevention and the Limits of the Criminal Law* (Oxford University Press, 2013) 214.

Rawlinson, Kevin, 'Police report sharp rise in sexting cases involving children in England and Wales' (6 November 2017) *The Guardian* <https://www.theguardian.com/media/2017/nov/06/police-report-sharp-rise-in-sexting-cases-involving-children-in-england-and-wales>.

Raz, Joseph, 'Autonomy, Toleration and the Harm Principle', in Ruth Gavison (ed), *Issues in Contemporary Legal Philosophy*: *The Influence of HLA Hart* (Oxford University Press, 1987) 155.

Raz, Joseph, *The Morality of Freedom* (1986).

Read, Darren, 'Should the English Legal System Adopt the US Law of Cyber-Trespass? (2011) 8(1) SCRIPTed 46.

Richardson, M, 'Breach of Confidence, Surreptitiously or Accidently Obtained Information and Privacy: Theory versus Law' (1994) 19 *Melbourne University Law Review* 673.

Ripstein, Arthur, 'Beyond the Harm Principle' (2006) 34(3) *Philosophy & Public Affairs* 215.

Roberts, Siobhan, 'Christopher Strachey's Nineteen-Fifties Love Machine', *The New Yorker – Annals of Technology* (14 February 2017) <https://www.newyorker.com/tech/annals-of-technology/christopher-stracheys-nineteen-fifties-love-machine>.

Robinson, Paul H, 'A functional analysis of criminal law' (1994) 88 *Northwestern University Law Review* 857.

Robinson, Paul H, 'A Theory of Justification: Societal Harm as a Prerequisite for Criminal Liability' (1975) 23 *University of California Los Angeles Law Review* 266.

Robinson, Paul H, 'The Criminal-Civil Distinction and the Utility of Desert' (1996) 76 *Boston University Law Review* 201.

Rosenzweig, Paul, 'Overcriminalization: An Agenda for Change' (2005) 54 *American University Law Review* 809.

Rowe Burks, Alice, *Who Invented the Computer? The Legal Battle that Changed History* (Prometheus Press, 2003).

Rowland, Diane, et al, *Information Technology Law* (Routledge, 4th ed, 2012).

Royzman, Edward B, and Jonathan Baron 'The Preference for Indirect Harm' (2002) 15(2) *Social Justice Research* 165.

Rumbles, Wayne, 'Theft in the Digital: Can you Steal Virtual Property? (2011) 17(2) *Canterbury Law Review* 354.

Ryder, Barbara, et al, 'The impact of software engineering research on modern programming languages' (2005) 14(4) *ACM Transactions on Software Engineering and Methodology* 431.

Ryder, Bryce, 'The Harms of Child Pornography Law' (2003) 36 *University of British Columbia Law Review* 101.

Sadurski, Wojciech, 'Racial Vilification, Psychic Harm and Affirmative Action' in Tom Campbell and Wojciech Sadurski (eds), *Freedom of Communication* (Dartmouth, 1994) 77.

Sandberg, Samuel, and Mathias Larsson, *En Raspberry Pi som Tor-Gateway* (Thesis, University West, 2015).

Sauter, Molly, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience* (Bloomsbury, 2014).

Schonsheck, Jonathan, *On Criminalisation: An Essay in the Philosophy of the Criminal Law* (Springer, 1994).

Schulhofer, Stephen J, 'Harm and Punishment: A Critique of Emphasis on the Results of Conduct in the Criminal Law' (1974) 122 *University of Pennsylvania Law Review* 1497.

Scottish Law Commission, 'Report on Computer Crime' (Report No 106, Cm 174, 1987).

Shultz, Mårten, 'The Responsible Web: How Tort Law Can Save the Internet' (2014) 5(2) *Journal of European Tort Law* 182.

Silva, Reginaldo, *2015 Highlights: Less Low-Hanging Fruit* (9 February 2016) Facebook <https://www.facebook.com/notes/facebook-bug-bounty/2015-highlights-less-low-hanging-fruit/1225168744164016>.

Simester, AP, and Andreas von Hirsch, *Crimes, Harms, and Wrong: On the Principles of Criminalisation* (Hart Publishing, 2011).

Simester, AP, and Andrew von Hirsch, 'Rethinking the Offence Principle' (2002) 8 *Legal Theory* 269.

Simons, Kenneth, 'The Crime/Tort Distinction: Legal Doctrine and Normative Perspectives' (2007-8) 17 *Widener Law Journal* 719.

Simpson, Robert Mark, 'Dignity, Harm, and Hate Speech' (2013) 32 *Law and Philosophy* 701.

Singer, Richard, and Douglas Husak, 'Of Innocence and Innocents: The Supreme Court and *Mens Rea* Since Herbert Packer' (1999) 2 *Buffalo Criminal Law Review* 859.

Singleton, E. Susan, 'Computer Misuse Act 1990 – recent developments' (1993) 14(1) *Company Lawyer* 22.

Skibell, Reid, 'Cybercrimes & Misdemeanours: A Re-evaluation of the Computer Fraud and Abuse Act' (2003) 18(3) *Berkeley Technology Law Journal* 909.

Skoudis, Ed, and Lenny Zeltser, *Malware: Fighting Malicious Code* (Prentice Hall Professional, 2004).

Smart, Carol, *Law, Crime and Sexuality* (Sage, 1995).

Smiley, Jane, *The Man Who Invented the Computer* (Doubleday, 2010).

Smith, Stephen F, 'Overcoming Overcriminalization' (2012) 102(3) *The Journal of Criminal Law & Criminology* 537.

Smith, Stephen, 'Is the Harm Principle Illiberal?' (2006) 51 *American Journal of Jurisprudence* 1.

Solntseff, N, and A Yezerski, 'A Survey of Extensible Programming Languages' in Mark Halpern et al (eds) *Annual Review in Automatic Programming: International Tracts in Computer Science and Technology* (Elsevier, 2014) 267.

Sommer, Joseph H, 'Against Cyberlaw' (2000) 15 *Berkeley Technology Law Journal* 1145.

Spears, Donna, 'The Criminal Justice System and the rule of law' (2008) 84 *Precedent* 18.

Steel, Alex, 'Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property' (2008) 30 *Sydney Law Review* 575.

Stein, Kelly, '"Unauthorised access" and the UK Computer Misuse Act 1990: House of Lords "leaves no room" for ambiguity' [2000] *Computer and Telecommunications Law Review* 63.

Steinmetz, Kevin, *Hacked: A Radical Approach to Hacker Culture and Crime* (New York University Press, 2016).

Stewart, Hamish, 'The Limits of the Harm Principle' (2010) 4(1) *Criminal Law and Philosophy* 17

Stuntz, William J, 'The Pathological Politics of Criminal Law' (2001) 100(3) *Michigan Law Review* 505.

Stychin, Carl, 'Unmanly Diversions: The Construction of the Homosexual Body (Politic) in English Law' (1994) 32 *Osgoode Hall Law Journal* 503.

Sullivan, GR, 'Bad thoughts and bad acts' (1990) *Criminal Law Review* 559.

Sun Beale, Sara, 'The Many Faces of Overcriminalization: From Morals and Mattress Tags to Overfederalization' (2005) 54(3) *American University Law Review* 747.

Symantec, '2019 Internet Security Report', *Symantec* (2019) <www.symantec.com/en/uk/security-center/threat-report/>.

Tadros, Victor, *Wrongs and Crimes* (Oxford University Press, 2016).

Tan, Li-Min, and M Newman, 'Computer Misuse and the Law' (1991) 11 *International Journal of Information Management* 282, 284.

Tapper, Colin, 'Computer crime: Scotch mist?' (1987) (Jan) *Criminal Law Review* 4.

Tasmanian Law Reform Commission, *Computer Misuse* (Report No 47, 1986).

Thales, '2019 Thales Data Threat Report – Global Edition', *Thales* (2019) <www.thalesesecurity.com/2019/data-threat-report/>.

The Crown Prosecution Service, 'The Fraud Act 2006' *CPS Guidelines* <http://www.cps.gov.uk/legal/d_to_g/fraud_act/>.

The Guardian, *The Guardian view on the Raspberry Pi: small is beautiful* (9 September 2016) <https://www.theguardian.com/commentisfree/2016/sep/08/the-guardian-view-on-the-raspberry-pi-small-is-beautiful>.

Tyle, Tom, *Why People Obey the Law* (Yale University Press, 1990).

US Senate Governmental Affairs Committee, *Problems Associated with Computer Technology in Federal Programs and Private Industry* (18 June 1976).

van Asselt, Marjolein, Ellen Voss and Tessa Fox, 'Regulating Technologies and the Uncertainty Paradox' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf, 2010) 259.

Verton, Dan, and Jane Brownlow, *Black ice: The invisible threat of cyber-terrorism* (Osborne, 2003).

Vinall, Jeff, 'The Criminal Law's Treatment of Twenty-First Century Copyright Pirates: A Treacherous New Frontier for Property Offences' (2013) 2 *Oxford University Undergraduate Law Journal* 57.

Virgo, Graham, 'Cheating and Dishonesty' (2018) 77 *Cambridge Law Review* 18.

von Hirsch, Andrew, *Censure and Sanctions* (Oxford University Press, 1993).

Wall, David, 'Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime' (2008) 11(6) *Information, Communication and Society* 861.

Wall, David, 'Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime' (2008) 22 *International Review of Law, Computers & Technology* 45.

Wall, David, *Cybercrime: The Transformation of Crime in the Digital Age* (Polity Press, 2007).

Walton, Richard, 'The Computer Misuse Act' (2006) 11(1) *Information Security Technical Report* 39.

Wasik, Martin, 'Computer Misuse' (1992) 8(1) *Computer Law & Security Review* 25.

Wasik, Martin, 'The Computer Misuse Act 1990' (1990) (Nov) *Criminal Law Review* 767.

Wasik, Martin, 'The Law Commission Working Paper on Computer Misuse' (1989) 5 *Computer Law and Security Report* 2.

Wasik, Martin, *Crime and the Computer* (Oxford: Clarendon Press, 1991).

Weiner, Norbert, *Cybernetics: Or Control and Communication in the Animal and the Machine* (MIT Press, 2nd ed, 1965).

Wertheimer, Alan, 'Victimless Crime' (1977) 87(4) *Ethics* 302.

Westen, Peter, 'The Ontological Problem of 'Risk' and 'Endangerment' in Criminal Law' in RA Duff and Stuart Green (eds) *Philosophical Foundations of Criminal Law* (Oxford University Press, 2011) 304.

Westen, Peter, *The Logic of Consent* (Ashgate, 2004).

Wheeler, Tom, *From Guttenberg to Google: The History of Our Future* (Brookings Institution Press, 2018).

Whiteside, Thomas, *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud* (4th ed, Ty Crowell Co., 1978).

Wilkes, Maurice, *Memoirs of a Computer Pioneer* (MIT Press, 1985).

Williams, Matthew, and David Wall, 'Cybercrime' in Chris Hale et al. (eds) *Criminology* (Oxford University Press, 2013) 250.

Winterbotham, Frederick William, *The Ultra Secret: Inside the Story of Operation Ultra, Bletchley Park and Enigma* (Orion Books, 2000).

Wong, Mary, 'Cyber-trespass and Unauthorized Access as Legal Mechanisms of Access Control: Lessons from the US Experience' (2007) 15(1) *International Journal of Law and Information* 90.

Woolf, Emile, 'The Equity Funding Story', in Emile Woolf and Moira Hindson, *Audit and Accountancy Pitfalls: A Casebook for Practicing Accountants, Lawyers and Insurers* (Wiley, 2015) 294.

Worthy, John, and Martin Fanning, 'Denial-of-Service: Plugging the legal loopholes?' (2007) 23 *Computer Law & Security Report* 194.

Wright, Ronald and Marc Miller, 'Honest Opacity in Charge Bargains' (2003) 55(4) *Stanford Law Review* 1409.

Yadin, Gilad, 'Beyond unauthorized access: laws of virtual reality hacking' in Woodrow Barfield and Marc J Blitz (eds), *Research Handbook on the Law of Virtual and Augmented Reality* (Elgar, 2018) 340.

Yaffe, Gideon, *Attempts in the Philosophy of Action and the Criminal Law* (Oxford University Press, 2010).

Yar, Majid, *Cybercrime and Society* (Sage, 2013).

Zaibert, Leo, 'Philosophy' in Markus Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal* Law (Oxford University Press, 2014) 132.

Zanghellini, Aleardo, 'Jurisprudential Foundations for Anti-Vilification Laws: The Relevance of Speech Act and Foucauldian Theory' (2003) 27 *Melbourne University Law Review* 458.

Zuckerberg, Mark, *Mark Zuckerberg's Letter to Investors: The Hacker Way* (1 February 2012) Wired < https://www.wired.com/2012/02/zuck-letter/>.