28

Computer misuse offences

28.1 Introduction

The impact of computer technology on society has been profound.[1] From simple beginnings in arithmetical calculations it has spawned immense data retrieval systems; systems controlling traffic by land, sea and air; systems indispensable to the functioning of industry, health care, education, banking and commerce. All this is to the common good or nearly all to the common good because, inevitably, some will use the technology for anti-social purposes. These may range from simple 'snooping', as where the hacker gains access to computer systems just for the fun of it (perhaps to demonstrate his computing ability), or for industrial or State espionage, or to perpetrate frauds, or disrupt systems with viruses, worms or Trojan horses[2] with serious commercial and possibly life-threatening consequences.

The law before the Computer Misuse Act 1990 could deal with some of these problems.[3] Appropriating property belonging to another is just as much theft[4] when it is done

[1] See E Brynjolfsson and A Mcafee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (2014); I Walden, *Computer Crimes and Digital Investigations* (2nd edn, 2016) Ch 3; D; I Lloyd, *Information Technology Law* (8th edn, 2017) 189–254. For more historical accounts see M Wasik, *Crime and the Computer* (1991) and 'The Computer Misuse Act 1990' [1990] Crim LR 767; Smith, *Property Offences*, Ch 11; N MacEwan, 'The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future' [2008] Crim LR 955.

[2] For a comparative analysis of legal regulation of viruses, see M Klang, 'A Critical Look at the Regulation of Computer Viruses' (2003) 11 Int'l J L & IT 162.

[3] See C Tapper, 'Computer Crime: Scotch Mist?' [1987] Crim LR 4.

[4] cf the problem of deceiving a machine, discussed at p 978.

by picking a pocket as by causing a computer to debit one account and to credit another. Should someone cause death or injury not with a blunt instrument but by interfering with a traffic control system, he would be equally liable to conviction for a homicide offence or an offence against the person. But there were gaps in the protection offered by the criminal law. The 1990 Act seeks to address these and is based on a Law Commission Report from 1989.

28.1.1 The background to the 1990 Act

A Law Commission Working Paper was published in 1988.[5] At that stage, the Law Commission was primarily concerned with unauthorized access to computing systems (hacking) though it noted other problems such as the inapplicability of deception offences to computers.[6] The problem with hacking was that 'snooping' (gaining unauthorized access to the correspondence, personal details, business records of another) was not generally an offence;[7] invasion of privacy and industrial espionage[8] are not, as such, offences. Could a special case be made for criminalizing snooping by way of hacking into a computer system? The Law Commission thought that it could and it was overwhelmingly supported by commentators on the Working Paper.

The proposal in the Law Commission's Working Paper to criminalize unauthorized access was thus generally applauded. But before the publication of its final Report,[9] the Commission conducted further discussions with computer and software manufacturers and with computer users in banking and commerce. These groups convinced the Commission of the need not only for an offence of unauthorized access (hacking) but also for two further offences of: (a) unauthorized access with intent to commit or facilitate the commission of further offences and (b) of unauthorized modification of computer material. These were enacted in the 1990 Act and have been a source of many problems.[10]

The first problem was that they were not flexible enough to deal with technological developments. Within a decade of enactment, commentators began to suggest that the 1990 Act had become rather dated, being drafted at a time when computers were relatively unsophisticated and the internet was in its infancy.[11] The pressure to extend the scope of the Act increased and[12] the Parliamentary All Party Internet Group reviewed the Act and made recommendations for reform.[13] The group concluded that many of the perceived problems with the Act actually stemmed from 'widespread ignorance of the current law'.[14] One concern that many expressed was that the Act should be capable of dealing with 'denial of

[5] Working Paper No 110, *Computer Misuse* (1988). See M Wasik, 'Law Reform Proposals on Computer Misuse' [1989] Crim LR 257.

[6] cf the similar problems in relation to forgery, Ch 29, and the discussion in the Fraud Act, Ch 22. On hacking see A Nehaluddin, 'Hackers' Criminal Behaviour and Laws Related to Hacking' (2009) 15 Computer and Telecommunications L Rev 135.

[7] Subject to the specific offences under the Data Protection Act 2018.

[8] See LCCP 150, *Legislating the Criminal Code: Misuse of Trade Secrets* (1997) and see J Hull, 'Stealing Secrets: A Review of the Law Commission's Consultation Paper on the Misuse of Trade Secrets' [1998] Crim LR 246.

[9] LC 186, *Computer Misuse* (1989) Cmnd 819.

[10] See MacEwan, n 1.

[11] See eg S Fafinski, 'Access Denied: Computer Misuse on an Era of Technological Change' (2006) 70 J Crim L 424.

[12] Though not all were in favour of reform, cf C Holder, 'Staying One Step Ahead of the Criminals' (2002) 10(3) IT Law 17.

[13] Discussed by G Fearon, 'All Party Internet (APIG) Report on the Computer Misuse Act' (2004) 15 Comps and Law 36.

[14] Para 23.

service attacks'[15] which lead to commercial websites being rendered unavailable to legitimate users.[16] The courts had in fact interpreted the offences in the 1990 Act as capable of applying to a denial of service attack,[17] but it was widely recognized that a more specific offence designed to tackle that mischief was desirable. Further pressure for reform also derived from international treaty obligations.[18] In 2006, the Police and Justice Act made amendments to the 1990 Act offences and introduced additional offences related to computer misuse. These were further amended by those in the Serious Crime Act 2007 and the Serious Crime Act 2015.[19]

This chapter will focus on the offences created by the Computer Misuse Act 1990 as amended.[20] Analysis of the problem of what has become known as 'cybercrime'—offences against the person or property or of cyberobscenity—lies beyond the scope of this work.[21] Also out of scope for this chapter are the offences under the Data Protection Act 2018, such as that of knowingly or recklessly obtaining or disclosing personal data or procuring its obtaining without the consent of the data controller, and the offence of knowingly or recklessly *retaining* personal data (which may have been lawfully obtained) without the consent of the data controller,[22] as are the offences of making, possessing, distributing, etc indecent images of children.[23]

It seems safe to predict that the criminal law will continue to face difficulties in dealing with those individuals who choose to exploit the opportunities which computers, and more specifically the internet, provide for causing a wide range of harmful, or indeed illegal, activity: fraud, obscenity, paedophilia, espionage, piracy, money laundering, market

[15] A denial of service (DoS) attack occurs 'when a deliberate attempt is made to stop a machine from performing its usual activities by having another computer create large amounts of specious traffic. The traffic may be valid requests made in an overwhelming volume or specially crafted protocol fragments that cause the serving machine to tie up significant resources to no useful purpose. In a Distributed Denial-of-Service (DDoS) attack a large number of remote computers are orchestrated into attacking a target at the same time' (APIG, para 56). These are extremely common at over 4,000 reported instances a week. See further Walden, *Computer Crimes and Digital Investigations* (2nd edn, 2016) paras 3.284 et seq.

[16] A Private Members' Bill—the Computer Misuse (Amendment) Bill 2000—sought to introduce a new offence of causing or intending to cause a degradation, failure or other impairment of function of a computerized system. The offence was aimed at protecting computer systems from denial of service attacks.

[17] In *DPP v Lennon* [2006] EWHC 1201 (Admin) discussed later.

[18] See especially the Convention on Cybercrime, CETS No 185 (2001) discussed by S Room, 'Criminalising Cybercrime' (2004) 154 NLJ 950. See also I Walden, 'Harmonising Computer Crime Laws in Europe' (2004) 12 European J of Crime Criminal Law and Criminal Justice 321; Walden, *Computer Crimes and Digital Investigations*, Ch 5 on the broader issues of international harmonization.

[19] Section 61 of the 2007 Act. The Serious Crime Act 2015, ss 41–4 in force from 3 May 2015.

[20] See MacEwan [2008] Crim LR 955.

[21] See in particular Walden, *Computer Crimes and Digital Investigations*, Ch 2; the special edition of the Criminal Law Review [1998], edited by DS Wall; R Essen, 'Cybercrime: A Growing Problem' (2002) 66 J Crim L 269; O Ward, 'Information Technology Watch Out, There's a Hacker About' (2000) 150 NLJ 1812; D Thomas and BD Loader, *Cybercrime* (2000); Y Akdeniz, 'Cybercrime' in *E-Commerce Law & Regulation Encyclopaedia* (2003); M Wong, 'Cybertrespass and Unauthorized Access' (2007) 15 Int J L & IT 90. See also A Guinchard, 'Crime in Virtual Worlds: The Limits of Criminal Law' (2010) 24 Int'l Rev of Law, Computers & Technology 175 considering 'crimes' committed in virtual worlds, including: (a) the 'theft' of virtual property; (b) the 'murder', 'assault' or 'rape' of an avatar; (c) harassment by means of virtual world technology; and (d) extreme or child pornography using avatars.

[22] Section 170 of the 2018 Act. The retention element to the offence was added in the 2018 Act. The offence also differs from the 1998 Act by providing a public interest defence for which D bears a legal burden. See *Shepherd v Information Commissioner* [2019] EWCA Crim 2.

[23] See generally P Rook and R Ward, *Rook and Ward on Sexual Offences Law and Practice* (6th edn, 2021) Ch 8.

abuse, etc.[24] It is already an enormous topic and one which will grow exponentially as emerging technology develops—the internet of things, artificial intelligence and ever more automation of all aspects of life will offer all manner of opportunities for criminal activity. In many cases, the existing law will be easily applied to the conduct involved (eg where the unauthorized access is to some innovative use of a computer (with an autonomous vehicle being hacked)) but in others the law may have to develop rapidly to meet the new challenges.

It is difficult to assess the number of computer misuse offences committed. Businesses are reluctant to report offences against them as it reveals weakness in their security and might deter customers. It has been suggested that prosecutions are declining because the legislation is so complex.[25] However, when prosecuted, sentences are often substantial. Custodial sentences for committing offences contained in the Computer Misuse Act 1990 have become increasingly common. After reviewing the most recent authorities, the Court of Appeal in *Martin*[26] stated that: 'These offences are comparatively easy to commit by those with the relevant expertise, they are increasingly prevalent, and the public is entitled to be protected from them. In our view, it is appropriate for sentences for offences such as these to involve a real element of deterrence. Those who commit them must expect to be punished accordingly.'

28.2 Unauthorized access to computer material

By s 1 of the Computer Misuse Act 1990 as amended:

(1) A person is guilty of an offence if—

  (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;[27]

  (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 that is the case.

(2) The intent a person has to have to commit an 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.

The offence carries a maximum sentence of two years' imprisonment on indictment.[28]

[24] See for discussion S Morris, *The Future of Netcrime Now: Part 1—Threats and Challenges* (2004) Home Office Online Report 62/04. On fraud, see A Doig, *Fraud* (2006) 62–3.

[25] See www.computing.co.uk/ctg/news/1835833/computer-misuse-act-prosecution-falling.

[26] [2013] EWCA Crim 1420. See eg *Coles-Day* [2015] EWCA Crim 2444 (hacking into and changing someone's Facebook account). See recently *Allsopp* [2019] EWCA Crim 95 (the 'TalkTalk' hack where the defendants received eight months' and 12 months' custody).

[27] The Police and Justice Act 2006, s 35 would, if implemented, have extended the offence to include cases where D enabled another to gain access. It was designed to ensure compliance with the European Union Framework Decision on Attacks Against Information Systems, adopted by the European Union and Justice and Home Affairs Council of Ministers on 24 Feb 2005.

[28] There are very few convictions under the Act. Between 1990 and 2006 there were 161: see MacEwan, n 1. The offence is underreported as organizations do not want to publicize failings in their security.

The idea behind this offence, in effect, is to close the door in the hacker's face. The offence is committed even if the hacker has no sinister purpose and is no more than a snooper.[29] The essence of the offence under s 1 is causing a computer to perform a function with intent to secure unauthorized access. No particular computer needs to be targeted by D.

The scope of the offence prompts the question why it should be an offence merely to access files held in the computer but not an offence to access paper files held in the filing cabinet.[30] The Law Commission thought it best to criminalize the hacker's conduct generally in order to deter those who *might* be contemplating fraud, or who *might* go on to commit some further offence or who *might*, because of their skills, be recruited by others with more sinister motives. With respect, these are not convincing reasons; conduct is not properly penalized because it *might* lead to different conduct that already amounts to the commission of an offence.[31]

One reason for criminalizing such conduct is that the proprietor of the system which is accessed by an unauthorized user may be put to considerable expense to repair his defences.[32] Of course, the proprietor of paper files incurs expense repairing his defences if an intruder breaks into his office to look through the files. There are, however, other important differences between the computer and the paper files: the person intruding into the filing cabinet must break into the office; he cannot access the files, as he can in the case of computer-held material, from a distant part of the country or, as is frequently the case, from the other side of the world.[33] The comparative ease of more extensive hacking makes this a more likely form of snooping with potentially more damaging consequences.

In addition, extensive sensitive personal information is now commonly stored on computers or online. As the Court of Appeal has recognized, someone accessing that information without authority causes distress to the victim and others.[34] Of course, the same could be said of letters secreted in a filing cabinet; however, it is often the further dissemination of this sensitive information that is the source of the distress and this is something that is especially easy to achieve if the information is stored digitally. Computer systems are always vulnerable to the determined hacker. In a world that is increasingly dependent on computers, and the integrity of computer systems, it appears entirely right that the criminal law should be employed to discourage the hacker.

28.2.1 Actus reus

The actus reus consists of causing a computer to perform any function.

[29] The offence was to be extended by the Police and Justice Act 2006 to include those whose intention is to enable someone else to secure unauthorized access to a computer or to enable secure unauthorized access to a computer at some later time. Those provisions were prospectively repealed by the Serious Crime Act 2007.

[30] Some regard the Act as overbroad and suggest that s 1 ought to be limited to conduct which breaches a 'security measure': S Room, 'Criminalising Cybercrime' (2004) 154 NLJ 950.

[31] For a contrary view that such specific offences of ulterior intent or endangerment are preferable to the government's likely alternative of creating general inchoate offences, see W Wilson, 'Participating in Crime: Some Thoughts on the Retribution/Prevention Dichotomy in Preparation for Crime and How to Deal With It' in A Reed and M Bohlander (eds), *Participating in Crime* (2013) 128.

[32] The Law Commission instanced a case where the restoration of a system following unauthorized access required 10,000 hours of the time of skilled staff. See *Baker* [2011] EWCA Crim 928 (£300,000 cost to employer); and see *Mangham* [2013] 1 Cr App R (S) 62 hacking into Facebook cost company $200,000 to investigate and repair.

[33] On jurisdictional issues see J. Hörnle, *Internet Jurisdiction: Law and Practice* (2021) Chs 4 and 5. There is a growing concern about the adequacy of the criminal law's response to jurisdictional challenges posed by online and digital crime.

[34] See *Crosskey* [2012] EWCA Crim 1645. See also *Khan* [2012] EWCA Crim 2032 (accessing social care records).

28.2.1.1 Computer

The Act does not define 'computer'. The Law Commission took the view that to have done so would be 'foolish'. Perhaps so, but a court, though it might be foolish to attempt a comprehensive definition, may be required to decide whether a particular article is a computer. Most obviously, a computer is something that computes, but computers have long since done more than merely mathematical calculations and may be used to store other information which can be processed for a wide variety of purposes, ranging from legal research (eg Lexis and Westlaw), traffic control or manufacturing purposes. It is tentatively suggested that the defining characteristics of a computer are the abilities of the appliance: (a) to store information; (b) to retrieve the information so stored; and perhaps most importantly (c) to process that information. Hence, the abacus and the slide-rule are not computers;[35] they can be used to make calculations but they have no 'memory' and they cannot themselves process information.[36]

It is submitted that it is insufficient to make it a computer that a machine is programmed to perform a function or number of functions. A washing machine may be programmed to perform several varieties of wash but is not, on this view, a computer; it can only obey instructions and not process them. With the advent of 'smart' devices, the courts are likely to have to address the interpretation of the Act in relation to alleged hacking of a wider range of devices. A computer can select a course of action on the basis of instructions given or information received. 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.

A computer may be thought of as any machine which responds to signals (now usually electronic) to perform programmed functions. On this view, the unauthorized user of the washing machine or microwave oven would commit the offence under s 1. But such machines were not, until very recently, sold as computers. The appropriate charge for the unauthorized user of a dishwasher or microwave oven would appear to be the dishonest abstraction of electricity contrary to s 13 of the Theft Act 1968[37] rather than unauthorized access to computer material under s 1 of the Computer Misuse Act. With smart versions of such devices that can be controlled remotely and even those that are part of the developing internet of things, it seems more likely that they will be treated as computers.

The offence is committed where D causes *any* computer to perform a function. Although the offence is often committed remotely via another computer, D also commits the offence by causing the target computer to perform a function directly.[38]

28.2.1.2 Performing a function

Once the machine in question is proved to be a computer, the actus reus is complete if it is caused to perform 'any' function. It is accordingly enough to switch on the computer though it may be difficult to prove mens rea if this is all that D has done. The strict requirements of proof are, anecdotally, reported to present difficulties in prosecution under the

[35] But not because these are mechanical; computers are now electronic but Babbage's computer was no less a computer because it was mechanical. See for detailed arguments about definition I Walden, *Computer Crimes and Digital Investigations*, paras 3.224–3.234.

[36] The Convention on Cybercrime uses the term 'computer system'. It defines a computer as a device that runs a 'program' to process 'data' but does not define these other terms. APIG concluded that there had been no difficulties with the (lack of) definition of any of the words in the Act. The Home Office reported that they had 'never come across a case' where the courts had failed to use a 'broad definition' (para 15). It recommended retaining the current approach.

[37] See Ch 18.

[38] *A-G's Reference (No 1 of 1991)* [1993] QB 94.

Act. It is not enough for D merely to view data that is already displayed on the monitor, but it is sufficient that D has, for example, accessed the internet by hitting the back key or return key when a computer has been left logged on to a network by the previous user.[39] Expert evidence will not always be necessary to establish that a computer performed a function.[40]

28.2.2 Mens rea

D must cause a computer to perform a function (a) with *intent* to secure access to any program or data held in any computer, and (b) *knowing* that the access he intends to secure is unauthorized.

28.2.2.1 Intent to secure access

Intention should, it is submitted, be interpreted consistently with other offences as discussed earlier.[41] Recklessness is insufficient.

By s 17, 'access' is widely defined and includes any 'use' of a computer, copying or moving of a file and altering or erasing data. There is no need to prove an intention in relation to any particular program. In practice, it will be common to establish that D has in fact secured access as so defined in order to establish mens rea but this is not a necessary element of the offence: it is complete on causing a computer to perform any function (eg switching it on) with intent to secure access.

28.2.2.2 Knowing it is unauthorized access

D must 'know'[42] that the access he intends to secure is unauthorized. By s 17(5), D's access is unauthorized if:

(1) he is not himself entitled to control access of the kind in question to the program or data; *and*

(2) he does not have consent to access of the kind in question to the program or data from any person who is so entitled.[43]

If D believes, even unreasonably, that he is entitled to control access or that his access is authorized by someone entitled to secure access, he cannot know that his access is unauthorized. Control in this context presumably means D has the power to 'authorise and forbid'.[44] More difficult is the case where D is unsure whether he is entitled to control access or, much more likely, he is unsure of the extent of his authorization to access a computer, but decides nonetheless to access the computer without checking the nature and extent of his authorization.[45] If, as will usually be the case, D could readily ascertain the nature and extent of his authority but chooses not to do so and decides to take the risk that his access is authorized, and his access is in fact unauthorized, it may be that he does not *know* his access is unauthorized but this is only because he does not want to know. It is submitted that wilful blindness of this kind is enough to constitute knowledge.[46] At the other extreme, the fact that it crosses D's mind that he might possibly be exceeding his authority would not suffice for knowledge.

[39] See *Ellis v DPP* [2001] EWHC 362 (Admin), where D argued unsuccessfully that such conduct was akin to reading a discarded newspaper.

[40] ibid. [41] Ch 3. [42] See generally, Ch 3. [43] Program includes part of a program: s 17(10).

[44] *Bow Street Metropolitan Stipendiary Magistrate, ex p Government of the USA* [2000] 2 AC 216 at 224; cf *Stanford* [2006] EWCA Crim 258, [2006] 2 Cr App R 5 (considering the term 'control' in the offence of unlawful interception under the Regulation of Investigatory Powers Act 2000).

[45] This gave rise to difficulty in some early high-profile prosecutions: see P Davies, 'Computer Misuse' (1995) 145 NLJ 1776.

[46] See p 118.

The offence may be committed where D has authority to use a computer, but not a particular program.[47] It may be committed where D is authorized to access one computer, computer X, but he does so to access another, computer Y, to which he does not have authorized access. The offence is complete when D has accessed computer X with intent to access computer Y. It was held in *Bignell* that police computer operators who extracted from the Police National Computer details of the registration and ownership of cars for their private purposes were not guilty of this offence,[48] though they may have been guilty of an offence under the Data Protection Act 1984.[49] Subsequently, in *Bow Street Magistrate, ex p Government of USA*[50] Lord Hobhouse cast doubt on *Bignell*. The House held that the offence may be committed when D has limited authority to access the computer and he exceeds his authorization,[51] so, an employee of American Express committed the offence when, having authority to access only specified accounts, she accessed other accounts.[52]

The offence requires both: (a) that the access intended by D is in fact unauthorized; and (b) that D knows that his access is unauthorized. If D believes his access is unauthorized when it is in fact authorized he does not commit the offence. Since the offence is now triable either way, he can be convicted of an attempt.

28.2.2.3 Defences

In *Coltman*,[53] the Court of Appeal confirmed that there is no public interest defence under s 1 of the Computer Misuse Act 1990. D, an NHS employee, used the computer of a colleague to access a file to which he had no authorized access. D passed the material from that file to a news agency. D was charged with the offence under s 1 of the Act. In his defence statement, D said that he had disclosed the material because it was in the public interest to do so. The Court of Appeal considered an interlocutory appeal on the issue of whether the 1990 Act should be read so as to allow for a potential 'public interest' defence. The court held that nothing in the ECHR required a public interest defence to be read into s 1 of the Act.[54]

28.3 Unauthorized access with intent to commit or facilitate further offences

By s 2 of the Act:

> (1) A person is guilty of an offence under this section if he commits an offence under section 1 above ('the unauthorized 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 any other person);
>
> and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

[47] See *Ellis v DPP* [2001] EWHC 362 (Admin).

[48] *DPP v Bignell* [1998] 1 Cr App R 1. Criticized in P Spink, 'Misuse of Police Computers' (1997) 42 Juridical Review 219.

[49] See now the Data Protection Act 2018.

[50] [2000] 1 Cr App R 61.

[51] This interpretation of s 17(5) was followed in *R (Begley) v Chief Constable of West Midlands Police* [2001] EWCA Civ 1571 and *Stanford* [2006] EWCA Crim 258. We are grateful to David Cook for discussions on this section.

[52] *Bow Street Magistrate, ex p Government of the USA* [2000] 2 AC 216, disapproving the *dictum* in *Bignell*, n 48, see commentary at [1999] Crim LR 971.

[53] [2018] EWCA Crim 2059.

[54] See, by contrast, the offence under the Data Protection Act 2018, s 170, n 22.

The 'further offences' to which the section applies are those for which the sentence is fixed by law; or for which a person over 21 *with no previous convictions* may be sentenced to imprisonment for a term of five years.[55] The offence requires proof of the s 1 offence together with an intent to commit the further offence or to facilitate the commission of such an offence by another. By s 2(3) it is immaterial whether the further offence is to be committed at the time of access or on some future occasion. For example, D gains unauthorized access to a computer in order to copy V's bank details so that he can subsequently perpetrate a fraud if the opportunity arises.

There is no requirement that the intended further offences will involve the use of a computer. The further offence need not be committed; it is enough that D intends one. In practical terms, the offences most likely to be intended or facilitated by D will be offences against property involving dishonesty but s 2 is not restricted to those offences.[56] Arguably, at the time the 1990 Act was enacted, the Theft Acts (with an extra offence to deal with deception of machines[57]) would probably have been adequate to deal with this problem where the further offences were ones of dishonesty.[58] This was how the Law Commission initially viewed the matter when drafting the 1990 Act but it had second thoughts and concluded that it would be preferable to extend the criminal law to the hacker before he had committed a substantive offence under the Theft Acts or had reached the stage of an attempt. Like s 1, s 2 of the 1990 Act is accordingly aimed at preparatory conduct. Thus, to take examples given by the Law Commission, the hacker who, with intent to steal, is searching for the password to enter an account might not be guilty of an attempt to steal, and the hacker who seeks confidential information in order to blackmail would clearly not be guilty of an attempt to blackmail.[59] Both, however, would commit the substantive offence under s 2. It is not just the hacker in the usual sense who is caught by this offence; the employee who accesses bank data and discloses those to accomplices to enable them to commit frauds also commits the offence.[60]

The Law Commission thought that the s 2 offence bore 'some relation to an attempt'[61] in that the ulterior offence needs only to be intended and not completed and accordingly s 2(4) provides that the offence may be committed even though commission of the ulterior offence is impossible. It is submitted that this provision is unnecessary but it may save argument. It will apply if D accesses V's computer to obtain his bank details, but unknown to D, that bank account was already closed by V.

Since the offence under s 2 is a substantive offence, there may, in turn, be a liability for conspiracy, attempt or assisting and encouraging the offence. These would represent extremely broad offences. D could agree with E that they would in the future access V's computer to gain information that they would, yet further in the future, use to perpetrate a crime. Given the preparatory nature of the offence, however, there is little scope for the operation of attempt in practice.[62]

The offence is triable either way and on conviction on indictment the offence carries a maximum sentence of five years' imprisonment.

[55] Or might be so sentenced but for the restrictions imposed by s 33 of the Magistrates' Courts Act 1980.

[56] A traffic or air traffic control system might be entered with intent to injure or even kill. Hacking with intent to commit treason is, perhaps, somewhat fanciful.

[57] As now in the Fraud Act 2006.

[58] See the recognition of the availability of the charge in the case of *Holmes* [2005] Crim LR 229. The APIG endorsed the need for a new fraud offence to deal with this problem (para 35) and recommended further reform on the misuse of trade secrets so as to develop a suitable framework to adequately criminalize the unlawful 'theft of data'.

[59] As in *Zezev* [2002] Crim LR 648.

[60] *Delamare* [2003] All ER (D) 127 (Feb).

[61] LC 186, para 3.58.

[62] Would D be liable under s 2 by reaching for the computer power switch?

28.4 Unauthorized acts with intent to impair or recklessness as to impairment of a computer

Section 3 is one of the most important in the Act. Section 3 of the Act, as substituted by s 36 of the Police and Justice Act 2006 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 data held in any computer; [or[63]]
  (c) to impair the operation of any such program or the reliability of any such data; . . .[64]

(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.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—
  (a) any particular computer;
  (b) any particular program or data; or
  (c) a program or data of any particular kind.

(5) In this section—
  (a) a reference to doing an act includes a reference to causing an act to be done;
  (b) 'act' includes a series of acts;
  (c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

On conviction on indictment the maximum sentence is ten years' imprisonment or a fine or both; on summary conviction six months or a fine up to the statutory maximum or both: s 3(6). This is a significant increase in the sentencing powers from the original s 3.

28.4.1 Background to the s 3 offence

It is, and remains, an offence under the Criminal Damage Act 1971 to destroy or damage a computer or its software as by, for example, taking a hammer and causing damage by breaking them.[65] Where there is physical damage to tangible property there is no problem in using the 1971 Act. What, though, of the case where there is damage to tangible property, but that damage cannot be perceived by the senses? Say D interferes with programs so as to render the computer incapable, or less capable, of carrying out the functions the programs

[63] As inserted by the Serious Crime Act 2007, s 61(3)(a)(i).

[64] The Serious Crime Act repealed s 3(2)(d) (which applied if D intended 'to enable any of the things mentioned in paragraphs (a) to (c) above to be done'), as such conduct will be covered by the offences under that Act of encouraging or assisting the commission of an offence or offences, see Ch 9.

[65] See generally on the old offence, Y Akdeniz, 'Section 3 of the Computer Misuse Act 1990—An Antidote for Computer Viruses' [1996] Web JCLI.

are designed to perform. This may be done without causing any physical damage that can be perceived by the senses.

In *Cox v Riley*,[66] it was held that D was guilty of criminal damage where he erased the program from a plastic circuit card which operated a saw to cut wood to programmed designs. D argued that the program was not 'property of a tangible nature' within the Criminal Damage Act. In this he was no doubt right but, in the view of the court, it failed to take account of the fact that D was charged not with damaging the program but with damaging the plastic card. And in *Whitely*,[67] it was held that D was properly convicted of criminal damage to computer disks where he gained unauthorized access to an academic computer system and by altering their magnetic particles caused them to delete and add files. His argument that only intangible information on the disks had been damaged was rejected; the disks had been damaged because their usefulness had been impaired.

These decisions might be viewed as bringing computer misuse, because of its obvious potential for harm, within the Criminal Damage Act by procrustean means,[68] but it is submitted that both decisions were defensible under the 1971 Act. The plastic circuit card in *Cox v Riley*, though it may not have been rendered useless and could have been reprogrammed to perform its original function, was temporarily unable to perform the function it was designed to perform. Though the disk was not damaged, it was rendered incapable of performing one of its programs and the case seems indistinguishable from *Fisher*.[69] Similarly, in *Whitely*,[70] the computer, though not itself damaged, had been rendered inoperable by tampering with its control mechanisms, namely the programs on the disks. That the disks could be restored is irrelevant since temporary impairment suffices for damage under the 1971 Act.

The Law Commission, however, took the view that the problem of computer misuse should be tackled more directly. It might have been possible to deal with the problem by amending the Criminal Damage Act to include interference with data and programs,[71] but the Commission decided on the creation of a new offence for two reasons. One was that 'the theoretical difficulties posed by applying the concept of damage to intangible property such as data or programs'[72] would render the law unacceptably uncertain. The other was that criminal damage may be committed recklessly[73] and the Commission did not think that the new offence should extend to a person who recklessly modified computer material.[74] In addition, as will appear, the Commission sought to clarify the relationship between the modification offence under s 3 of the Computer Misuse Act 1990 and the offence of criminal damage under the Criminal Damage Act.

The 1990 Act version of the offence was narrower than under the current law. It was restricted to modifications of the computer. That form of the offence was nevertheless construed very broadly by the courts. In *Zevez*,[75] it was held that if a computer is caused to record information (an email) which shows that it comes from one person, when it in fact comes from someone else, that manifestly affects its reliability.[76] This was seen as a significant extension of the offence. The email clearly tells a lie about itself, but it is submitted that it does not

66 (1986) 83 Cr App R 54. 67 [1991] Crim LR 436.

68 See Wasik, *Crime and the Computer*, 137–45.

69 (1865) LR 1 CCR 7, p 1098. 70 [1991] Crim LR 436.

71 Following the amendment by the Police and Justice Act 2006, s 10(5) of the Criminal Damage Act 1971 was amended to exclude 'modification of the contents of a computer' from the definition of damage unless the effect is to impair its physical condition.

72 LC 186, para 3.62. 73 The new s 3 does extend to recklessness.

74 See p 1098. 75 [2002] Crim LR 648.

76 D had placed in the files of a computer a bogus email purporting to come from a person which it had not. This was held to have caused a modification of the computer within what was s 17(7): 'A modification of the contents of any computer takes place if . . . any . . . data is added to its contents . . .'

affect the reliability of other data on the computer or the functioning of the computer. The court further extended the ambit of the offence by holding that denial of service attacks were also caught. In *DPP v Lennon*,[77] D used a 'mail-bombing' program to send five million emails to his former employer. The Divisional Court, disagreeing with the District Judge, held that D had 'caused an unauthorised modification' by adding data. The owner of a computer able to receive emails would ordinarily be taken to have consented to the sending of emails to his computer. However, such implied consent was not without limits, and the consent did not cover emails that had been sent not for the purpose of communication with the owner but instead to interrupt his computer system. The court suggested that this could be tested by asking whether if D had rung his employer she would have consented to the receipt of five million emails. The new substituted s 3, as above, ensures that denial of service attacks are caught by the section,[78] and puts beyond doubt *some* of the concerns raised in the *Lennon* case.[79]

28.4.2 The current offence

There must be an unauthorized act in relation to a computer. The *extended* meaning of 'authorized' is set out in s 17(8). The impairment of the computer, program, data, etc need not actually occur. The offence is complete on the carrying out of the unauthorized act with intent or recklessness to achieve that impairment, etc.

Essentially, s 3 is concerned with the sabotaging or impairing of computer systems by any act or series of acts specified in s 3(2). The most obvious instances will be by transferring viruses,[80] Trojan horses or worms to computer systems or by corrupting websites.[81] It is sufficient that the conduct would prevent or hinder the access of others—as, for example, by a denial of service attack or mail bomb attack which incapacitates a server.[82] There is no longer a requirement of erasure of data or modification of anything and in that respect the offence is made much wider than as originally enacted. The concept of impairment might prove difficult to apply in some cases—how much slower must D intend the program to operate before it is properly said to be impaired? Unauthorized use may be sufficient if, for example, D intends or is reckless as to causing impairment to the reliability of the data. Causing a computer to debit V's bank account and credit D's[83] is sufficient because the data concerning V's account is now unreliable. The impairment intended or about which D is reckless need only be temporary. Again, this is a significant extension of the offence.[84]

The offence requires:

(1) that D intends by the unauthorized act to bring about one of the consequences listed in s 3(2) (impairment, etc) or is reckless as to whether such consequences would occur; and

(2) knowledge that the act by which he intends or is reckless about bringing about the impairment etc is unauthorized. The knowledge must relate to the unauthorized nature of the act from which impairment is intended. It is not necessary to prove knowledge of the unauthorized nature of the impairment (as was the case with the old form of s 3 which required knowledge as to the unauthorized modification).

77 [2006] EWHC 1201 (Admin). See also the comment by S Fafinski (2006) 72 J Crim L 474.

78 The amendment ensures that English law complies with Art 3 of the EU Framework Decision on Attacks Against Information Systems.

79 It does not deal with challenges based on consent.

80 See eg *Vallor* [2004] 1 Cr App R (S) 54, spreading the third most virulent virus in the world.

81 See eg *Lindesay* [2002] 1 Cr App R (S) 370, disgruntled sacked employee corrupting firm's website.

82 cf *Martin* [2013] EWCA Crim 1420.

83 cf *Thompson* [1984] 1 WLR 962.

84 See MacEwan, n 1, and S Fafinski, 'Computer Misuse: The Implications of the Police and Justice Act 2006' (2006) 72 J Crim L 53.

Intention should bear its ordinary meaning.[85] Recklessness should be understood in its subjective sense as defined in *G*.[86] The ability to commit the offence recklessly represents a significant extension by the 2006 Act. In its original form, recklessness was insufficient because the Law Commission[87] endorsed a strict mens rea requirement, expressing concern that people could inadvertently modify the contents of a computer.

D's intent or recklessness need not be directed at the proscribed impairment etc of a particular computer or program. There is concern that this offence will criminalize legitimate activities by IT security consultants.

28.5 Section 3ZA: impairing a computer such as to cause serious damage

Section 41 of the Serious Crime Act 2015 inserted a new s 3ZA into the 1990 Act creating an offence of impairing a computer such as to cause serious damage. It is an offence of considerable breadth, in terms of elements, jurisdictional reach and sentence. Its potential application to a broad range of criminal activities does not seem to have been appreciated.

D commits the offence if he undertakes an unauthorized act in relation to a computer and that act causes, or creates a significant risk of causing, serious damage of a 'material kind' and D knows that it is an unauthorized act and intends the act to cause serious damage of a material kind or is reckless as to whether such damage is caused. It is a jury question whether damage is 'material' but the section makes clear that damage includes 'damage to human welfare, the environment, the economy or national security'. The offence is triable on indictment and carries a maximum sentence of life for threat to life, loss of life or damage to national security or 14 years for damage to the economy or the environment.

Section 3ZA 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 causes, or creates a significant risk of, serious damage of a material kind; and
  (d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.

(2) Damage is of a 'material kind' for the purposes 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 purposes 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;

[85] See p 93. [86] [2004] AC 1034. See p 104. [87] LC 186, para 3.62.

(e) disruption of facilities for transport, or

(f) disruption of services relating to health.

(4) It is immaterial for the purposes of subsection (2) whether or not an act causing damage—

(a) does so directly;

(b) is the only or main cause of the damage.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) 'act' includes a series of acts;

(c) a reference to a country includes a reference to a territory, and to any place in, or part or region of, a country or territory.[88]

The offence has the potential to tackle organized crime groups or others seeking to ransom state organizations such as the NHS, private organizations such as rail or air service providers, and financial institutions. It also has the potential to apply in an espionage context where, for example, D in North Korea gains unauthorized access to a computer in the UK with intent to damage national security. The jurisdictional reach is extremely wide, subject to proof that there was a 'significant link' with England and Wales. For example, D who was abroad in country X and was targeting a computer in country Y is triable in England.

28.6 Making, supplying or obtaining articles for use in offences under s 1 or s 3: s 3ZA

Section 37 of the Police and Justice Act 2006 introduced three new forms of offence. The maximum sentence on conviction on indictment is two years' imprisonment or a fine or both; on summary conviction six months' imprisonment or a fine up to the statutory maximum or both.

By s 3A(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'. This form of the offence mirrors closely that in s 7 of the Fraud Act 2006.[89] 'Intention' should be construed in the normal manner.

By s 3A(2), it is an offence to supply or offer to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under s 1, 3 or 3ZA. 'Belief' should be construed as elsewhere in the criminal law, to mean a state of mind greater than one of mere suspicion but without constituting knowledge.[90] The question whether the article is 'likely to be' used for an offence under ss 1 to 3 may give rise to some difficulty in application. According to the Explanatory Notes, if D is charged in relation to a quantity of articles, the prosecution must prove their case 'in relation to any particular one or more of those articles; it would not be enough to prove that the person believed that a certain proportion of the articles was likely to be used in connection with an offence under section 1 or 3' (and presumably now s 3ZA).

Section 3A(3) provides an offence where a person obtains any article 'with a view to' its being supplied for use to commit, or to assist in the commission of, an offence under s 1, 3 or 3za.

[88] The Serious Crime Act 2015, s 41(2), inserted s 3ZA. The section came into effect on 3 May 2015 (SI 2015/820). The section is designed to ensure compliance with Directive 2013/40/EU on attacks against information systems.

[89] At p 1013. [90] See p 118.

It is submitted that the mens rea element may be read restrictively to mean purposive intent, as the Court of Appeal held in a different context.[91] This is a relatively unusual form of offence, criminalizing an intermediary. It is not sufficient that D merely obtains; nor is it sufficient if he possesses. This offence requires an obtaining with an ulterior purpose. It extends further than s 3A(1) by capturing D's conduct before he has got as far as to offer to supply or in fact supply the article.

For all three forms of the offence, 'article' includes any program or data held in electronic form: s 3A(4). The mens rea is crucial in each of these offences since the articles which could possibly be used in the commission of computer misuse offences are incredibly wide ranging—from a screwdriver to complex software, or a computer password.

The new forms of offence were explained by the government as being necessary to combat the market in 'hacker tools' for hacking into computer systems. The provisions also ensure UK compliance with Council of Europe obligations.[92] Concerns have been raised about the possible criminalization of those engaged in legitimate research into computer security systems.[93]

By s 42 of the Serious Crime Act 2015, s 3A was amended so that it extends subs (3) to include obtaining a tool for use to commit a s 1 or 3 or 3ZA offence. There is no need to prove that D has intention to supply that tool.[94]

(1) A person is guilty of an offence if he obtains any article—

  (a) intending to use it to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA, or

  (b) with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

Further reading

I Walden, *Computer Crimes and Digital Investigations*

I Lloyd, *Information Technology Law*

J. Hörnle, *Internet Jurisdiction: Law and Practice* (2021)

91 See *Dooley* [2005] EWCA Crim 3093, p 1026.

92 Art 6(1)(a) of the 2001 Council of Europe Cybercrime Convention.

93 See House of Lords Science and Technology Report, *Personal Internet Security* (2007). See, however, the government's subsequent response which was heavily criticized: T Wright and D Hodgkinson, 'Government Response to House of Lords Science and Technology Committee Report on Personal Internet Security' (2008) 14 Computer and Telecommunications L Rev 65.

94 This ensures compliance with European Parliament and European Council Directive 2013/40/EU on attacks against information systems.