Computer Crime in Ireland: a Critical Assessment of the Substantive Law[*]

T.J. McIntyre[1]

Introduction

Irish law on computer crime is an afterthought. The principal offences in this area are contained in the Criminal Damage Act 1991 and the Criminal Justice (Theft and Fraud Offences) Act 2001: in both cases, the offences have been tacked on to an Act whose primary focus is elsewhere, and in both cases the drafting reflects this lack of attention. In addition, the offences are beginning to show their age: recent technological developments have resulted in new threats and responses which do not fit easily into the existing law.

Some reform of the law is overdue, and in any event will be necessary if Ireland is to implement the Council of Europe Convention on Cybercrime and the (proposed) Council Framework Decision on Attacks Against Information Systems. This article looks at the substantive law relating to computer crime with a view to identifying problems which currently exist, flagging some developing issues and offering some suggestions for reform.[2]

Background

> "It appears an inevitable feature of technological development that criminal applications follow legitimate uses with very little time lag."[3]

Although computer misuse soon followed the development of computers, laws dealing specifically with computer crime took somewhat longer to appear.[4] In part, this may be because many computer related crimes were essentially conventional crimes[5] which were merely facilitated by the use of computers: as such, they could be prosecuted under existing laws. As Kerr points out:

---

[*] This article originally appeared at 15(1) *Irish Criminal Law Journal* 13.

[1] BCL, LLM, BL. Lecturer in Law, University College Dublin.

[2] The article will confine itself to the substantive law relating to crimes directed against computer systems, such as hacking and viruses. It will not address the wider area of computer-related crimes (such as illegal filesharing, or the distribution of child pornography) nor the procedural issues associated with computer crime (such as jurisdictional issues, investigative procedures and data preservation / data retention).

[3] Lloyd, *Information Technology Law* (3rd ed. , 2000), p. 200.

[4] Kerr, "Cybercrime's scope: interpreting 'access' and 'authorization' in computer misuse statutes" (2003) *New York University Law Review* 1596, 1602-1607. Lloyd, *op. cit.*, ch. 12.

[5] Classification of the various forms of computer crimes is a subject of debate, but most authors recognise a distinction between those crimes which are unique to computers and other crimes which are merely facilitated by the use of computers. See, for example, Burstein, "A survey of cybercrime in the United States" (2003) *Berkley Technology Law Journal* 313, 318-320. This distinction is also recognised in the Convention on Cybercrime, which categorises crimes as follows: "offences against the confidentiality, integrity and availability of computer data and systems", "computer related offences", "content related offences" and "offences related to infringements of copyright and related rights".

> "For the most part, traditional crimes committed using computers raise few new issues for criminal law. The basic crimes remain the same regardless of whether wrongdoers use computers or some other means to commit them. For example, a death threat is still a death threat regardless of whether it is transmitted via email or a telephone call."[6]

Difficulties arose, however, when courts began to face situations involving issues unique to computers, particularly the early hacking cases. In these cases, prosecutors struggled to fit defendants' conduct within existing offences.[7]

Some success was achieved in conceptualising hacking as a form of criminal damage. In both *Cox v. Riley*[8] and *R v. Whitely*[9] prosecutors in England succeeded in arguing that changes to programs or data could be considered to be criminal damage to the physical medium on which that information was stored.

The limitations of this approach were, however, exposed in *Whitely*, where the Court of Appeal noted that in order for criminal damage to be made out, the changes would have to result in "an impairment of the value or usefulness of the disc to the owner". Changes of a lesser nature would not suffice: "[if] the hacker's actions do not go beyond, for example, mere tinkering with an otherwise 'empty' disc, no damage would be established". In *Whitely* itself, the necessary impairment was easily found, since the defendant's actions had led to the network slowing down and crashing. However, this logic led to the bizarre implication that, had the defendant been a more skilled hacker and avoided disrupting the ordinary operation of the network, he would not have been guilty of an offence, since the value and usefulness of the system would not have been impaired by his actions.[10]

Another approach was to treat the use of false usernames and passwords as a form of forgery. This was adopted in the English case of *R v. Gold.*[11] Here, two computer journalists secured access to the British Telecom Prestel computer network, by using the customer identification numbers and passwords of authorised users. They used this access to obtain information to which they were not entitled and to make changes to stored data, with the stated intention of exposing security flaws in the Prestel system. These changes notoriously included leaving messages in the personal account of Prince Philip, the Duke of Edinburgh, a factor which led to some official embarrassment at the time.

---

[6] Kerr, "Cybercrime's scope: interpreting 'access' and 'authorization' in computer misuse statutes" (2003) *New York University Law Review* 1596 at 1602.

[7] For an interesting discussion of the strategies adopted by United States prosecutors, see Kerr, "Cybercrime's scope: interpreting 'access' and 'authorization' in computer misuse statutes" (2003) *New York University Law Review* 1596 at 1605-1613.

[8] (1986) 83 Cr App R 54.

[9] (1991) 93 Cr App R 25.

[10] One could, of course, argue that the mere fact of a security breach impairs the usefulness of a system, since it may have to be shut down while evidence is gathered, countermeasures applied, backups restored, and so on. However, the reasoning in *Whitely* wouldn't appear to lend itself to this argument.

[11] [1988] 2 WLR 984.

The defendants were charged with a number of offences under the Forgery and Counterfeiting Act, 1981, on the theory that their use of others' customer identification numbers and passwords constituted the making of false instruments, contrary to section 1 of that act. At first glance, this appeared to be adequate to deal with this type of hacking since the 1981 Act expressly included in its scope false instruments which were "recorded or stored on disc, tape, soundtrack, or other device",[12] and the defendants were convicted at trial. On appeal, however, the House of Lords took the view that the passwords and customer identification numbers entered by the defendants, even if they were "false instruments", could not be said to be "recorded or stored" as was required by the act, since they were held only temporarily to be checked for validity and were deleted immediately afterwards.

More generally, the House of Lords strongly criticised this attempt to put new wine into old bottles:

> "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 a 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." (*per* Lord Brandon)

This case therefore exposed, in a very public way, the fact that existing criminal laws were not adequate to deal with computer hacking and the rebuke delivered by the House of Lords, coupled with pressure from the computer industry, led to the Law Commission Working Paper on Computer Misuse[13], which in turn led to the Computer Misuse Act, 1990.[14] This was a comprehensive piece of legislation, which created three new offences of unauthorised access to computer material, unauthorised access with intent to commit further offences, and unauthorised modification of computer material.

The Criminal Damage Act, 1991

In Ireland, however, a different approach was taken. Although the need for reform was acknowledged, rather than draft dedicated legislation the Government decided to piggyback on the Criminal Damage Bill, 1990, by bringing computer crimes within its scope. That Bill, however, had been drafted in order to implement the Law Reform Commission Report on Malicious Damage.[15] It had not been designed with computer crime in mind, nor had the Law Reform Commission been asked to report on the matter. As such, the computer crime provisions appear to have been stuffed rather inelegantly into the draft Bill. As was said at the time by Senator Joe Costello:

---

[12] Section 8(1).
[13] Law Commission, *Computer Misuse*, Working Paper No. 110 (HMSO, 1988).
[14] Bainbridge, *Introduction to Computer Law* (5th ed., 2004), p. 382.
[15] LRC 26-1988.

> "[T]he Commission did not envisage that their report would be incorporated into another body of legislation which would include this new offence of computer hacking … [T]o incorporate as an update in the same Bill the offence of computer hacking makes the mind boggle. It seems as though somebody, somewhere, suddenly decided this was an opportunity, whether by stealth or otherwise, to get legislation on the Statute Book …That is a very bad way to produce legislation."[16]

In framing computer crime as a form of criminal damage, the drafters adopted two separate approaches. First, to circumvent the problem presented by *R v. Whitely*[17], *i.e.* that mere changes in stored information will not constitute damage to tangible property, section 1 defines the term "property" to include data, and gives an extended definition to "damage" in respect of data. It follows that the criminal damage offences created by the 1991 Act will apply equally to the deletion or modification of data. Secondly, to deal with the difficulty highlighted by *R. v. Gold*, section 5 creates a separate offence of unauthorised access. We will look at these two offences separately.

Criminal Damage to Data and Programs

The offence of criminal damage is created by section 2(1):

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

Under section 1, "data" is defined to mean "information in a form in which it can be accessed by means of a computer and [including] a program", while damage in respect of data is defined to mean:

> "(i) to add to, alter, corrupt, erase or move to another storage medium or to a different location in the storage medium in which they are kept (whether or not property other than data is damaged thereby), or
>
> (ii) to do any act that contributes towards causing such addition, alteration, corruption, erasure or movement"

The combined effect of these provisions is to create an offence which is remarkably broad, and applies not just to "damage" in the ordinary sense of the word, but to *any* modification of *any* information stored on a computer, whether or not that has any adverse effect, or indeed any act "contribut[ing] towards" such modification.[18] In

---

[16] Senator Joe Costello, 130 *Seanad Debates* Col. 1644. Senators Brendan Ryan and David Norris also had cogent and well-briefed criticisms of the Bill during its passage.

[17] (1991) 93 Cr App R 25.

[18] On the other hand, Clark points out that the definition of damage does not appear to extend to the mere inspection, copying or disclosure of data, even though this might cause substantial commercial loss or personal embarrassment. Clark, "Computer Related Crime in Ireland", (1994) *3 European Journal of Crime, Criminal Law and Criminal Justice* 252 at 262.

contrast, "damage" in respect of tangible property is defined in terms which require that such property be destroyed, defaced, dismantled, rendered inoperable, or the like.[19]

It is arguable whether innocuous changes or additions to data should be defined as damage; the Act itself equates data with tangible property, which would suggest that only harmful changes or additions should be criminalised. This was the approach taken in the United Kingdom: section 3 of the Computer Misuse Act 1990 creates a similar offence of unauthorised modification of computer material, but only where the defendant has an intention to bring about a harmful result, such as impairing the operation of a computer or the reliability of data.

It could be said that even seemingly harmless changes can involve substantial costs in investigating the extent of the security breach, restoring from backup systems, and taking steps to secure a system against future incursion. These costs, it might be said, themselves constitute a form of damage which should merit the severe penalties associated with the criminal damage offence. As against that, however, the same costs would be incurred in cleaning up after an unauthorised access offence, which carries a maximum penalty of six months. It is, therefore, difficult to say that these costs justify more severe penalties in one context, but not in the other.[20]

Will prosecutorial discretion ensure that a section 2(1) charge is not brought in respect of "damage" which does not have any harmful effect? Perhaps. But it is undesirable to criminalise conduct so broadly that it is necessary to rely on such discretion to avoid injustice.

In addition, the breadth of this offence brings about an undesirable overlap with the section 5 unauthorised access offence. In almost every case, access to a computer will bring about some changes to the data stored on that computer. For example, simply by turning on a personal computer, a user generally causes the computer to generate a log file which records the startup process.[21] Under section 2(1), this log file is "damage" – it is an addition to the data stored on that computer – so that the user in addition to the section 5 offence may also be guilty of criminal damage.[22] This undermines the legislative scheme, which was intended to differentiate between the less serious offence of unauthorised access and the more serious offence of actual damage.[23]

Unauthorised Access

The unauthorised access offence is created by section 5 of the 1991 Act:

---

[19] Section 1.

[20] Of course, this argument could be turned on its head. If cleaning up after an unauthorised access is a costly and difficult process, then it might be argued with some force that the unauthorised access offence should carry a higher maximum penalty.

[21] Kelleher and Murray, *Information Technology Law in Ireland* (1997), make a similar point at p. 203.

[22] The user probably would not intend to generate the log file; however, if they are aware that such a file is likely to be created then they will be subjectively reckless, which is sufficient to establish liability for the section 2(1) offence.

[23] See, for example, the comments of the Minister of State at 130 *Seanad Debates* Cols. 1621 and 1736.

> "(1) A person who without lawful excuse operates a computer—
>
> (a) within the State with intent to access any data kept either within or outside the State, or
> (b) outside the State with intent to access any data kept within the State,
>
> shall, whether or not he accesses any data, be guilty of an offence […]
>
> (2) Subsection (1) applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person."

It should be pointed out that, although universally referred to as the "unauthorised access" offence[24], this is properly described as an offence of operating a computer, without a lawful excuse, with intent to access data. Unusually for Irish criminal law, this is, in effect, an attempt offence: the offence is committed when a computer is used with a particular purpose in mind, and the offence is complete whether or not the offender does in fact access any data.

Defining "Operate"

The first difficulty with this offence is the use of the term "operate". This appears to be unique to the Irish legislation.[25] The Computer Misuse Act, 1990, which would have been looked to as an example by the drafters of the 1991 Act, refers instead to "caus[ing] a computer to perform any function".

What does "operate" mean? The term is left undefined by the 1991 Act, suggesting that the drafter thought it straightforward. However, in a computer context, even a cursory examination reveals ambiguities.[26] We can take the Oxford English Dictionary (OED) definition as our starting point – the relevant meaning of operate is defined as "to cause or direct the functioning of; to control the working of (a machine, boat, etc.)"[27]

Suppose that A attempts to log in to a computer. He encounters a username and password prompt. He enters several guesses at usernames and passwords, but all are unsuccessful and he gives up. Did A operate that computer? On a narrow view, the answer would be no: it could be argued that A did not in fact enjoy any control over the machine (as required by the latter part of the OED definition). By way of analogy, it might be said

---

[24] Including in the marginal note to the section itself.
[25] There does not appear to be any other legislation dealing with the operation of computers, while the only case dealing with the term "operate" in a computer context appears to be the less than helpful Scottish decision in *Ross v. HM Advocate* [1998] S.L.T. 1313, where a person was charged with "operating a bulletin board system".
[26] Kelleher and Murray, *Information Technology Law in Ireland* (1997), p. 203.
[27] *Oxford English Dictionary* (2nd ed., 1989).

that a person who attempted to steal a car but was defeated by an immobiliser did not operate that car.[28]

On the other hand, by entering usernames and passwords, A does cause the computer to execute programs checking those details: as such, A could be said to have operated the computer (in the wider OED sense of causing it to carry out a function).[29] This interpretation is supported by the wording of section 5, which refers to operation with intent to access any data, and the crime being complete whether or not the user does in fact access any data, suggesting that the legislature intended to criminalise preliminary conduct even though access might have been thwarted by a security measure. Indeed, at committee stage before the Seanad the Minister of State suggested that:

> "The offence will be committed either when access is achieved or when the computer is being operated with the objective of gaining access but no access is actually achieved. It will be committed even when the hacker merely looks around the system he has penetrated. Depending on the level of security in the system, a hacker may not get beyond a look at a list of what the system contains."[30]

This wider interpretation would, in essence, be the same as the Computer Misuse Act formula of "caus[ing] a computer to perform any function". (Which prompts the question: if this was the intended result, why did the drafter of the 1991 Act adopt a different wording?) This view will, no doubt, be attractive to prosecutors aiming to maximise the coverage of the 1991 Act. However, such an expansive interpretation would create significant uncertainty.

Suppose that A sends an email to B, which travels via C's computer. On the wide interpretation, A will have operated the computers belonging to B and C, since he will have caused them to execute programs to deliver and process his email.[31] This result, although inevitable if we take the wider meaning of operate, would come as a surprise to most users. It would also expand further what is already an overbroad offence.[32] If, for example, A were to send email to B, after B had indicated that the email was unwelcome, A could be said to have operated B's computer without lawful excuse and could be guilty of an offence under this section.[33]

---

[28] See the comments of Kerr, "Cybercrime's scope: interpreting 'access' and 'authorization' in computer misuse statutes" (2003) *New York University Law Review* 1596 at 1617-1621, discussing similar problems with the term "access".

[29] This is the view of Clark, "Computer Related Crime in Ireland", (1994) *3 European Journal of Crime, Criminal Law and Criminal Justice* 252 at 269.

[30] 130 *Seanad Debates* 1736.

[31] Kerr, "Cybercrime's scope: interpreting 'access' and 'authorization' in computer misuse statutes" (2003) *New York University Law Review* 1596 makes a similar point at 1622-1623.

[32] Kelleher and Murray, *Information Technology Law in Ireland* (1997), p. 203.

[33] Compare *Intel v. Hamidi* 30 Cal.4th 1342 (Supreme Court of California, 2003), where it was held that unwanted email could amount to a civil trespass, but only where the volume of the email was such as to interfere with the operation of the receiving computer.

"Lawful Excuse": Unauthorised Operation or Unauthorised Access?

The term "lawful excuse" in section 5 presents its own problems. The term is carried over from the criminal damage portions of the Act, although in a computer context it would be more appropriate for access to be described as either authorised or unauthorised, and most jurisdictions use this distinction as the basis for criminal liability.[34]

In particular, this section raises an issue as to whether it penalises unauthorised *operation* of a computer, or unauthorised *access* to data. In other words, does the phrase "without lawful excuse" qualify the operation or the access?

To illustrate this point, consider two hypotheticals. A uses B's computer, without B's permission, to access data he is entitled to access (a public web page, for example). This is unauthorised operation, but not unauthorised access. Conversely, C uses D's computer with D's permission, to access data he is not entitled to access (suppose C has a disk which contains confidential information belonging to another). This is authorised operation, but unauthorised access.

On the face of it, the section seems plainly to apply to unauthorised operation. The term "without lawful excuse" appears next to the term operate, while the term access is unqualified. The legislative history also supports this interpretation: at Committee Stage before the Seanad, an amendment to limit the offence to the accessing of private or confidential data was rejected.[35]

However, the position is complicated when we look to section 6, which provides a definition of lawful excuse:

> "(2) A person charged with an offence to which this section applies shall, whether or not he would be treated for the purposes of this Act as having a lawful excuse apart from this subsection, be treated for those purposes as having a lawful excuse—
>
> > (a) if at the time of the act or acts alleged to constitute the offence he believed that the person or persons whom he believed to be entitled to *consent to or authorise* the damage to (or, *in the case of an offence under section 5, the accessing of*) the property in question had consented, or would have consented to or authorised it if he or they had known of the damage or the accessing and its circumstances,
> >
> > (b) in the case of an offence under section 5, if *he is himself the person entitled to consent to or authorise accessing of the data concerned* …" (emphasis added)

[34] Compare the Computer Misuse Act, 1990. See also Kerr, *op. cit.*, at 1615-1624.
[35] 130 *Seanad Debates* Cols. 1696-1712.

This presents a drafting oddity. We have already seen that the offence created by section 5 is *operating a computer without lawful excuse*, not *accessing data without lawful excuse*. However, section 6 discusses lawful excuse in terms of consent or authority to access data, not to operate a computer. Section 6, therefore, is drafted in a way which assumes that section 5 creates an offence of unauthorised access, not unauthorised operation, and could be said to import a requirement of unauthorised access into section 5.

This can be seen by reverting to our previous hypotheticals. A uses B's computer, without B's permission, to access data which he is entitled to access. This is, on the face of it, an offence under section 5. However, section 6 suggests that A has a lawful excuse if he had authority to access the data even though he had no authority to operate the computer. Meanwhile, C uses D's computer, with D's permission, to access information which he is not entitled to access. On the face of it, this is not an offence under section 5 (the operation of the computer is authorised). However, when section 6 is thrown into the mix, it could be argued to be a use without lawful excuse, since section 6 appears to frame lawful excuse solely in terms of permission to access data (although the definition of lawful use in section 6 is not exhaustive). Indeed, the Minister for State suggested in the Seanad that such a use would constitute a breach of section 5:

> "For example, an employee could take home with him a disc containing data he was not authorised to access and access the data by inserting the disc in his own computer."[36]

This confusion results from the use of a lawful excuse definition tailored for the criminal damage offence, which is not appropriate for the section 5 offence. Modifying the section to focus on whether a user is authorised, although it could present difficulties when a person exceeds their authority[37], would make it easier to ascertain the boundaries of this crime.

Dishonest Use of a Computer: Section 9 of The Criminal Justice (Theft and Fraud Offences) Act, 2001

The Law Reform Commission, in its 1992 *Report on the Law Relating to Dishonesty*[38], pointed out that there could be problems in applying the then-existing laws against dishonesty in a computer context.[39] Most notably, offences involving misrepresentation

[36] 130 *Seanad Debates* Col. 1702.
[37] As in *DPP v. Bignell* [1998] 1 Cr App R 1 and *R v. Bow Street Metropolitan Stipendiary Magistrate, ex p. Government of the United States of America* [1999] 4 All ER 1, where "insiders" accessed data for improper purposes. It might be desirable to follow the example of some United States jurisdictions and introduce a specific crime of exceeding authorised access. See Kerr, "Cybercrime's scope: interpreting 'access' and 'authorization' in computer misuse statutes" (2003) *New York University Law Review* 1596 at 1615 for examples.
[38] LRC 43-1992.
[39] *Report on the Law Relating to Dishonesty*, pp. 102-103.

(such as obtaining by false pretences) could be read as requiring deception of a human mind, not merely "an unsuspecting machine".[40]

Some of these difficulties would be resolved by other changes being recommended by the Commission. In particular the Commission noted that many computer related crimes would fall under their revised definition of theft:

> "A machine or computer can only respond to a physical shape or electronic impulse fed into it. There can be no question of a machine giving a meaningful consent. No mind is deceived. The machine or computer does what it is told or programmed to do. On that approach, if someone achieves unauthorised access to a machine or computer or having authority to use a machine or computer feeds in false information and obtains cash or a chattel, we have a straightforward case of theft or unlawful appropriation."[41]

Having said that, however, the Commission recognised that there would be other cases involving computers which might not fit into existing categories. In particular, it accepted the conclusion of the English Law Commission that there could be a gap where a machine was "deceived" in order to obtain a service or other benefit, or to cause a loss, and therefore recommended that a catch-all offence of dishonest use of a computer should be created.[42]

The Commission looked to two models for this offence: section 200 of the New Zealand Crimes Bill, and section 115 of the Australian Capital Territory Ordinance. The latter section was recommended by the Commission, and was ultimately adopted, with minor modifications, as section 9 of the Criminal Justice (Theft and Fraud Offences) Act, 2001:

> "A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence."

This offence, however, is difficult to interpret. Kelleher argues[43] that it appears to cover almost any use of a computer which could be said to be dishonest:

---

[40] *Report on the Law Relating to Dishonesty*, p. 103, citing the Scottish Law Commission, Consultative Memorandum No. 68, *Computer Crime*, paras 3.8–3.9 (1986). See also the discussion in Bainbridge, *Introduction to Computer Law* (5th ed., 2004), pp. 371-380. Compare the Australian decision in *R. v. Baxter* (1988) 84 ALR 537 where it was held that a false representation could include a representation made to a bank machine.

[41] *Report on the Law Relating to Dishonesty*, p. 243. This passage reflects the reasoning of the Australian High Court in *Kennison v. Daire* (1986) 64 ALR 17.

[42] *Report on the Law Relating to Dishonesty*, p. 243, citing Law Commission Working Paper 104, *Criminal Law: Conspiracy to Defraud*, para 4.14. See also Wasik, "Hacking, Viruses and Fraud" in Akdeniz, Walker and Wall (eds.), *The Internet, Law and Society* (2000), at p. 291, discussing the "deception" of computers.

[43] Kelleher, "Cracking down on the hack pack", *Irish Times*, 23 October 2003.

> "[S]omebody who dishonestly sells pirated music over the Internet using a computer could face a 10-year sentence under this proposal, but a competitor selling them out of a suitcase on O'Connell Street would face a maximum of only five years under the Copyright and Related Rights Act 2000."[44]

Murray makes a similar point[45], stating that even linking or framing without consent could be criminalised by this section. She gives the *Shetland Times* case[46] as an example:

> "If this Bill is implemented, this type of activity will become an offence … the defendant would have been acting dishonestly [*As the court found that he did not have the right to link in this way*] using a computer, and made a gain (the *de facto* acquirement of internet content) that caused a loss to the plaintiff (the *de facto* loss of those web pages and the loss of competitive advantage)." (Emphasis and parentheses in original.)

These fears are understandable, given the wording of the section, and are to some extent supported by the ambiguous legislative history on this point, with the Minister for Justice, Equality and Law Reform at one point stating that:

> "This offence contemplates dishonesty. The Bill deals with a situation in which a person lawfully has a computer, but uses it for a dishonest purpose."[47]

Nevertheless, these fears are, it is submitted, mistaken. The section does not refer to use of a computer for a dishonest purpose: it applies to a person who "dishonestly operates or causes to be operated" a computer. "Dishonestly" is defined in section 2 as meaning "without a claim of right made in good faith". Accordingly (and remembering that penal statutes must be given a strict interpretation) the correct interpretation appears to be that the section covers a person who operates a computer without a claim of right made in good faith: that is, without a belief that they were entitled to do so. In other words, the section will apply only where the operation of the computer is unauthorised. As such, this is essentially the same basic offence as section 5 of the 1991 Act, coupled with an intention to make a gain or cause a loss. This point was made at Committee Stage by Senator Brendan Ryan:

> "[A] reasonable reading of it would suggest that the offence is the dishonest operation of the computer. The section refers to someone who dishonestly operates a computer, but that could be interpreted as meaning that he or she should not have been using the computer. However, if someone honestly uses a

[44] Referring to the offences created by section 140 of the Copyright and Related Rights Act 2000.
[45] Murray, "The Criminal Justice (Theft and Fraud Offences) Bill 2000 and the Internet", (2001) 19 *Irish Law Times* 143. A similar point is made in McIntyre-O'Brien, "The Current Status of Computer Hacking Offences in Ireland and their Application to the Internet" [2004] *Cork Online Law Review* 7.
[46] *Shetland Times v. Willis* [1997] SLT 669.
[47] 168 *Seanad Debates* Col. 1130.

> computer, in other words he or she does so with a claim of right made in good faith, there is no offence no matter what he or she does with the computer."[48]

This conclusion is supported when we consider the peculiar outcomes which would result from the wider interpretation. For example, Murray argues[49] that the Copyright and Related Rights Act, 2000 "deliberately ensures that the individual who merely downloads a song will not be liable to criminal charges", while the wider interpretation of section 9 *would* criminalise use of a computer to download an MP3 without paying for it, thus exposing the user to a maximum penalty of ten years' imprisonment and an unlimited fine, and nullifying the scheme of the 2000 Act. It is hard to imagine that this could be an intended result of section 9.

Must the gain or loss be dishonest?

Section 9 appears to criminalise dishonest operation of a computer with intention to make a gain or cause a loss, even though there might be no element of dishonesty in relation to the gain or the loss itself. This point was raised by Senator Brendan Ryan:

> "Students in the college in which I work are required to meet certain conditions before they can use a computer. They may break the rules about how the computer should be used with the intention of making a personal gain. It could be argued that although the use of someone else's computer may be dishonest, the gain made may be legitimate. The computer could be dishonestly used to enter a quiz or to participate in on-line gambling, but the gain could be legitimate. A penalty of imprisonment of ten years in such circumstances, even though the gain was legitimate, is disproportionate … The word 'dishonestly' should refer to someone who dishonestly makes a gain or dishonestly causes a loss, but not to someone who dishonestly uses a computer."[50]

Is this interpretation correct? Or can the section be read so as to extend the requirement of dishonesty to the gain or loss? The legislative history is unhelpful on this point.[51] The Minister in reply to Senator Ryan initially seemed to contemplate an element of dishonesty in relation to the gain or the loss, by stating that: "[t]he Bill deals with a situation in which a person lawfully has a computer, but uses it for a dishonest purpose."[52] However, immediately after that, the Minister went on to assure the Senator

---

[48] 168 *Seanad Debates* Col. 1131.

[49] Murray, "The Criminal Justice (Theft and Fraud Offences) Bill 2000 and the Internet", (2001) 19 *Irish Law Times* 143. The reference is to the range of offences created by section 140 of the 2000 Act, which contains a number of exceptions in respect of "private and domestic use".

[50] 168 *Seanad Debates* Col. 1129-1131.

[51] The *Report on the Law Relating to Dishonesty* doesn't address this point directly. However, it indirectly supports the argument that the gain or loss must itself be dishonest, by referring (at p. 243-244) with approval to section 200 of the New Zealand Crimes Bill, which does require such an element. Under section 200, a person commits an offence who "accesses any computer … with intent *dishonestly to obtain* [any benefit] …; or having accessed (whether with or without authority) any computer … *dishonestly uses the computer … to obtain* [any benefit]." (emphasis added)

[52] 168 *Seanad Debates* Col. 1130.

that there would be "proportionality between the offence and the term of imprisonment or punishment"[53] and stated that: "Senator Ryan is correct to point out that there are varying degrees of seriousness. However, one must expect that the court will decide on the seriousness of an offence."[54] This passage suggests that the offence does extend to situations where the gain or loss is legitimate, but that the courts would be expected to impose a lesser penalty in such cases.

Given that there is room for argument on this point, the gravity of the offence and the principle that penal statutes should be strictly construed would suggest that the requirement of dishonesty should extend to the gain or the loss, not merely the operation of the computer. Having said that, it would be desirable to see this point clarified in any further legislation in this area.

Scope of the offence

Although the section 9 offence appears to be phrased quite widely, it applies only to offences of dishonesty: that is, where the defendant intends to make a gain or cause a loss. It will not apply to other situations where a computer is misused for an improper purpose. For example, suppose that A hacks into a telephone company computer, with the intention of gathering information to stalk a former partner.[55] In this case, A is not guilty of dishonest use of a computer, since there is no intention to make a gain or cause a loss.[56] Equally, if a paramilitary organisation were to access confidential Garda files with a view to committing a murder, only the (relatively minor) unauthorised access offence would be committed.[57] Arguably, therefore, it would be preferable to adopt an approach based on section 2 of the Computer Misuse Act, 1990, which creates a wider offence of unauthorised access with intent to commit (or facilitate the commission of) further offences.[58]

Developing Issues

Having briefly outlined current Irish law on computer crimes, our next step is to consider how existing rules might deal with some developing issues.

Denial of Service Attacks

---

[53] 168 *Seanad Debates* Col. 1130.
[54] 168 *Seanad Debates* Col. 1130.
[55] As happened in the case of Philip Nourse, discussed in Cullen, "Sex, text, revenge, hacking and Friends Reunited", *The Register*, 21 November 2002, http://www.theregister.co.uk/2002/11/21/sex_text_revenge_hacking/ (visited 14 September 2004).
[56] Section 2(3) of the Criminal Justice (Theft and Fraud Offences) Act, 2001, makes it clear that the terms gain and loss "are to be construed as extending only to gain or loss in money or other property."
[57] This example taken from Clark, "Computer Related Crime in Ireland", (1994) *3 European Journal of Crime, Criminal Law and Criminal Justice* 252 at 262 where he makes the same point in the context of the 1991 Act.
[58] Bainbridge, *Introduction to Computer Law* (5th ed., 2004), pp. 388-389.

The "denial of service attack" presents particular problems for Irish law. A useful, non-technical definition is given by Burden and Palmer[59]:

> "Denial of service attacks aim to prevent 'legitimate' users from gaining access to or using a particular Internet service. These attacks can take various forms, including most commonly the swamping of an organizations' servers with millions of spoof messages, thus using up all available capacity/bandwidth within the target system. Frequently, such attacks cause servers to overload, resulting in them freezing or crashing. Other examples include creating excessive error messages that must be logged by the target system or sending oversized packets of information. The perpetrators will frequently use an innocent third party's computer as a host or 'zombie' from which to launch the attacks…"

While strictly speaking the term relates to any attack which results in a service becoming unavailable, in practice it is generally used to refer to techniques which flood a computer with what appears to be legitimate traffic, which has the effect of slowing or disabling it completely. Another common variant is to disrupt the network downstream from the target computer, so that the computer itself functions normally, but intending users are unable to contact it: in effect, isolating it from the Internet.[60]

These types of attacks do not fit neatly within our existing offences. Suppose that A operates a publicly accessible website. B, motivated by a grudge, decides to disrupt that site. B programs his computer to automatically and repeatedly download pages from A's site. This consumes a great deal of A's bandwidth and server capacity, which results in legitimate users being unable to access A's site. A suffers a financial loss as a result. What offence, if any, has B committed?

Unauthorised Access?

Can the denial of service attack be characterised as an unauthorised access within the terms of section 5 of the Criminal Damage Act 1991? The basic form of attack, outlined in the above hypothetical, will be difficult to prosecute under this section. Public web sites carry with them an implied permission to access the site: a defendant would no doubt argue that his activities in accessing the site were within the scope of this implied permission, and were therefore with lawful excuse.[61]

---

[59] Burden and Palmer, "Cyber Crime – A new breed of criminal?" (2003) 19 *Computer Law and Security Report* 222 at 223. For a discussion of denial of service attacks under United States law, see Nemerofsky, "The Crime of 'Interruption of Computer Services to Authorized Users': Have You Ever Heard of It?" (2000) 6 *Richmond Journal of Law and Technology* 23, available at http://www.richmond.edu/jolt/v6i5/article2.html (visited 20 December 2004).

[60] For a more detailed discussion of denial of service attacks see CERT Coordination Centre, "Denial of Service Attacks", http://www.cert.org/tech_tips/denial_of_service.html (visited 4 August 2004).

[61] Turner and Callaghan, "Denial of Service Attacks: APIG Report" (2004) 15 *PLC*, available at http://www.practicallaw.com/jsp/article.jsp?item=:4961982 (visited 13 September 2004), make the same point in relation to English law, noting that "[T]here must be some action (that is, access or modification) which is unauthorised. This may be difficult to prove given that most websites either expressly or impliedly invite visitors to access and interact with the website. This includes emails and also the behind the scenes

For the prosecution to rebut this defence, it would be necessary to show that any implied permission was limited in scope, to identify the boundaries of that implied permission, and to demonstrate that the defendant acted outside those boundaries. In most cases, this will be difficult to do. For example, how would we go about identifying the scope of the implied permission? Do we look to the "social norms in the community of computer users", as suggested[62] by Kerr? Or should we ask what a hypothetical reasonable user would understand themselves as being permitted to do? In addition, this approach will raise issues as to the fairness of criminalising conduct based on the vague boundaries of implied permission.

Alternatively, the prosecution might argue that the defendant's motive in accessing the site, in and of itself, meant that he lacked a lawful excuse within the meaning of section 5.[63] This might be a more promising approach. An analogy could be drawn with burglary, where it has been held that a person becomes a trespasser, even though they have permission to enter a building, where they enter for a purpose other than that for which the permission was given.[64] However, it is an open question as to whether the courts would adopt this reasoning.

Dishonest Use of a Computer?

The basic denial of service attack, although it may be intended to cause a loss, is unlikely to fall under the section 9 offence of dishonest use of a computer. That offence, as we have already seen, applies only to persons who operate a computer without a claim of right made in good faith. Consequently, in the case of a public web site, the defendant will be able to claim that he falls within the scope of the implied permission to access that site, presenting the same difficulties discussed immediately above.

Criminal Damage?

At first glance, a charge of criminal damage under section 2(1) of the Criminal Damage Act 1991 might seem appropriate. However, it is unrealistic to say that there has been

---

exchange of information between computers that is a necessary part of the technical functioning of the internet."

[62] Kerr, "Cybercrime's scope: interpreting 'access' and 'authorization' in computer misuse statutes" (2003) *New York University Law Review* 1596 at 1623.

[63] This situation has some similarities with *R v. Bow Street Magistrates Court ex p. Government of the United States of America* [1999] 3 WLR 620 (Allison's case). However, it is not on all fours with that case. In Allison's case, Mr. Allison had conspired with an employee of American Express to access confidential information in customer accounts. The employee was authorised to view certain accounts assigned to her, but accessed other accounts and gave confidential information to Mr. Allison. The case turned on whether her conduct amounted to unauthorised access within the meaning of the Computer Misuse Act 1990. The House of Lords held that it did, notwithstanding that she was an authorised user in respect of some data, holding that authority to access certain data did not authorise her to access further data of the same kind. In the denial of service example, however, we are concerned with a situation where a user does have authority to access particular data, but the question is whether their motive in so doing invalidates that authority.

[64] See Charleton, McDermott and Bolger, *Criminal Law* (1999), p. 842, discussing *People (DPP) v. McMahon* [1987] ILRM 87 and *DPP v. Jones and Smith* [1976] 1 WLR 672.

damage where the computer in question has not been permanently affected and the data stored on that computer has not been modified. (The aim of a denial of service attack is not to modify data, but to prevent access to it.) Burden and Palmer suggest that:

> "[I]t is doubtful whether a prosecution for criminal damage would at present be successful, given that there is no permanent damage caused to the target system. However, it may be possible to argue that because the 'usefulness' of the system had been impaired this in itself amounts to damage, although we suspect that this is likely to be seen by the courts as stretching the concept of criminal damage further than they are willing to contemplate."[65]

This argument has been persuasive in England, and the Computer Misuse (Amendment) Bill 2002 was introduced to deal with this lacuna and create a specific offence of denial of service. That Bill failed after running out of parliamentary time, but further legislation along the same lines has recently been recommended by the (United Kingdom) All Party Parliamentary Internet Group (unfortunately abbreviated as APIG).[66]

Indirect prosecution of denial of service attacks

In many cases, a defendant in carrying out a denial of service attack will carry out other crimes of unauthorised access or criminal damage. One variant in particular, the distributed denial of service attack, involves compromising a number of machines and using those machines as a launching point for the attack. This point was made by the APIG:

> "In general, where a [distributed denial of service attack] takes place then an offence will have been committed because many machines will have been taken over by the attacker and special software installed to implement the attack."[67]

Consequently, it will generally be possible to indirectly prosecute the denial of service attack, by prosecuting the other offences committed in the course of the attack. This was the approach taken in what appears to be the only English prosecution of a denial of service attack to date (*R v. Aaron Caffrey*[68]). In that case, the attack was charged as "unauthorised modification of computer material", contrary to section 3 of the Computer Misuse Act, 1990. Although a full report is not available, it appears that this charge related to the machines that were taken over in order to launch the attack.

In practical terms, therefore, Irish law will probably cover the majority of denial of service attacks. Nevertheless, an argument can be made that a specific offence to deal

---

[65] Burden and Palmer, "Cyber Crime – A new breed of criminal?" (2003) 19 *Computer Law and Security Report* 222 at 223.
[66] All Party Parliamentary Internet Group, *Revision of the Computer Misuse Act* (2004), available at http://www.apig.org.uk/CMAReportFinalVersion1.pdf (visited 14 September 2004).
[67] All Party Parliamentary Internet Group, *Revision of the Computer Misuse Act* (2004), para. 65.
[68] Southwark Crown Court, 17 October 2003. (Unreported but discussed at http://news.bbc.co.uk/1/hi/technology/3202116.stm) (visited 14 September 2004)

with denial of service attacks should be enacted to deal with the problems outlined above. (This approach is favoured by the Convention on Cybercrime, which requires[69] parties to implement an offence of system interference.) On the other hand, the APIG correctly points out that such an approach may present its own difficulties:

> "Are we to lay a broadcaster open to prosecution if they mention a website on the air and several million people suddenly decide to have a look at it? … We are also aware of a growth in 'cyber-protest' where it is arranged for supporters of a cause to all access a website at the same time – with the aim of ensuring that it becomes available for a short period. Where such protestors are simply fetching web pages using standard browsers we can see significant dangers in creating a framework for criminalising their behaviour."[70]

Self Help, Self Defence and Software Bombs

Technological responses to computer crime can go beyond passive defence to active countermeasures. Karnow has pointed out that:

> "There is a growing interest in 'self help' mechanisms to counter internet mediated threats. Content providers such as record labels and movie studios favor federal legislation that would allow them to disable copyright infringers' computers. Software licensors endorse state laws that permit the remote disabling of software in use by the licensee when the license terms are breached. Internet security professionals debate the propriety and legality of striking back at computers which launch worms, viruses, and other intrusions"[71]

This interest is, unsurprisingly, encouraged by perceived deficiencies in the legal system's capability to respond to computer crime. However, such responses may themselves be illegal.[72]

One area where this issue has arisen is in relation to "software bombs" – that is, means of unilaterally disabling software. These are sometimes built into software by developers as a means of enforcing payment in the event of a dispute. However, in a number of English cases, software developers have been convicted of unauthorised modification of the contents of a computer, contrary to section 3 of the Computer Misuse Act 1990, where

---

[69] Article 5. The proposed Council Framework Decision (COM(2002) 173 final) takes a similar approach in article 4.

[70] All Party Parliamentary Internet Group, *Revision of the Computer Misuse Act* (2004), paras. 69-70.

[71] Karnow, "Launch On Warning: Aggressive Defense of Computer Systems", 8 *Cyberspace Lawyer* 4 (2003), also published as Strike and Counterstrike: The Law on Automated Intrusions and Striking Back, Counterpane, CRYPTO-GRAM (April 15, 2003). Available at http://islandia.law.yale.edu/isp/digital%20cops/papers/karnow_newcops.pdf (visited 12 September 2004).

[72] As well as impractical. Karnow points out that difficulties in identifying the source of an attack, and in disabling that source without impacting on other users, mean that counter attacks will seldom be feasible. Karnow, "Launch On Warning: Aggressive Defense of Computer Systems", 8 *Cyberspace Lawyer* 4 (2003),

they have activated software bombs, even though they have done so in order to enforce a payment which they believe in good faith is owed to them.[73]

Under English law, that result would appear to be inevitable: the Computer Misuse Act prohibits any unauthorised access or modification, and does not contain an exception for actions intended to protect the rights of the defendant. By analogy, counter attacks aimed at disabling attacking computers would themselves also amount to criminal acts.[74]

Under Irish law, however, the result might be different. The offences of criminal damage and unauthorised access under the Criminal Damage Act, 1991, are subject to a defence of lawful excuse. Section 6(2)(c) expressly includes the defence of property as constituting a lawful excuse:

> "A person charged with an offence to which this section applies shall … be treated … as having a lawful excuse –
>
> (c) if he damaged or threatened to damage the property in question … in order to protect … property belonging to himself or another or a right or interest in property which was or which he believed to be vested in himself or another and, at the time of the act or acts alleged to constitute the offence, he believed
>
> (i) that … the property, right or interest was in immediate need of protection, and
> (ii) that the means of protection adopted or proposed to be adopted were or would be reasonable having regard to all the circumstances."

It follows that a person who counter attacks an attacking computer may have a lawful excuse, provided that their actions are reasonable.[75] Reasonableness in this context is subjective: section 6(3) specifies that: "it is immaterial whether a belief is justified or not if it is honestly held". One problem with this defence is that section 6(2), by its terms, applies only to the criminal damage offences, not to the unauthorised access offence. However, section 6 does not provide an exhaustive definition of lawful excuse; and it would be surprising if the more serious offence of criminal damage was justified by the defence of property while the less serious offence of unauthorised access was not.

---

[73] Sewart, "Dropping the Bomb", 14 (4) *Computers and Law* 22. A good example of a software bomb, albeit in a civil context, is *Rubicon Computer Systems v. United Paints Limited* (2000) 2 TCLR 453. Such a bomb could only be treated as authorised where the software purchase has been notified of it and consented to its use.

[74] A related issue concerns whether Internet Service Providers would be justified in monitoring or scanning subscribers' computers for security issues before allowing them to connect to the Internet. This point was noted by the All Party Parliamentary Internet Group: "BT asked us to consider revising the CMA to address the extent to which a system owner can take 'active measures' to secure their system without committing an offence. They clearly envisage situations where they 'scan' their customers for security holds or make a reverse connection as a check before granting access to an incoming requestor. We do not see a need for revision here since ISPs can address these matters via contract with their own customers." (para. 47)

[75] Kelleher and Murray, *Information Technology Law in Ireland* (1997), pp. 226-227.

Of course, the existence of a lawful excuse defence does not mean that it would be wise for Irish computer users to engage in counter attacks. It will be difficult to show that a counter attack was reasonable and proportionate (in many cases, as Karnow points out, there will be alternatives such as simply removing the affected computer from the network, blocking the incoming traffic or patching the affected computer[76]). In addition, the attacking computer may well be located in another jurisdiction which does not share the same view as to the legality of counter attacks.[77]

International Developments: The Convention on Cybercrime and the Proposed Council Framework Decision[78]

Computer crime is necessarily international in its scope, and any reform of Irish law will take place against the background of international attempts to harmonise national laws and in particular the Council of Europe Convention on Cybercrime[79] and the Commission's proposed Framework Decision on Attacks Against Information Systems.[80]

The Cybercrime Convention, agreed in 2002 and entering into force on 1 July 2004, is an ambitious document which covers not just "offences against the confidentiality, integrity and availability of computer data and systems" (such as unauthorised access and denial of service attacks) but also "computer related offences" (such as forgery and fraud), "content related offences" (child pornography), and "offences related to infringement of copyright and related rights" (such as illegal file sharing). It also deals with attempts, aiding and abetting, and corporate liability issues, before turning to procedural matters which parties are obliged to implement in national law, including rules for the interception, collection, preservation and disclosure of computer data. It seeks to promote international cooperation by dealing with extradition, mutual assistance between police forces and designated points of contact for computer crime issues. Finally, a protocol to the Convention deals with the question of so-called hate crimes committed via computer.[81]

Detailed consideration of the Convention is beyond the scope of this article (although it should be noted that the secretive drafting process leading to it and the substance of the Convention itself have been the subject of heavy criticism by civil liberties groups, particularly the provisions relating to the interception of communications and traffic data[82]). However, the "offences against the confidentiality, integrity and availability of

---

[76] Karnow, "Launch On Warning: Aggressive Defense of Computer Systems", 8 *Cyberspace Lawyer* 4 (2003).
[77] Which raises the difficult question of the territorial and extraterritorial effect of computer crime laws. See Bainbridge, *Introduction to Computer Law* (5th ed., 2004), p. 390 for an introduction.
[78] See Walden, "Computer Crime", in Reed and Angel (eds.), *Computer Law* (5th ed., 2003), pp. 314-317.
[79] CETS No. 185.
[80] COM(2002) 173 final.
[81] Protocol on the Criminalization of Act of a Racist and Xenophobic Nature Committed Through Computer Systems.
[82] See, for example, Carr and Williams, "Criminalization and the Council of Europe (Draft) Convention on Cyber-Crime", (2002) 18 *Computer Law and Security* Report 83; Bowden, "CCTV For Inside Your Head: Blanket Traffic Data Retention And The Emergency Anti Terror Legislation" (2002) 8(2) *Computers and*

computer data and systems" must be mentioned, since at least three of those offences will require further legislation if they are to be implemented into Irish law: the article 3 offence of illegal interception of data[83], the article 5 offence of system interference (which will include denial of service attacks), and the article 6 offence of misuse of devices intended to facilitate computer crime (dealing with "cracking" tools).

Similarly, the proposed Framework Decision on Attacks Against Information Systems (which has now been approved in general terms by the Justice and Home Affairs Council of Ministers and is expected to be finalised shortly[84]) will approximate national laws on computer crime and require member states to establish specific offences of illegal access to and interference with information systems. The Decision is relatively narrow in its scope, compared with the Convention (it does not, for example, deal with issues such as child pornography or copyright infringements) and has been tailored to be compatible with the Convention. As with the Convention, it will require a number of changes to Irish law, in particular to implement the article 4(a) offence of "hindering or interrupting the functioning of an information system".

Conclusion

The Convention and the Framework Decision, between them, seem set to force the issue of computer crime onto the legislative agenda over the next two years or so. Irish law already covers (albeit imperfectly) the majority of the issues presented by both instruments, so there will inevitably be a temptation to adopt a minimalist approach to reform: to tinker around the edges of the current law, making only those changes necessary for compliance.

The current law is, however, a very shaky foundation on which to build. As we have seen, existing offences have been compromised by the failure to adopt a systematic approach to this area, and by the attempt to categorise computer crime either as a form of

---

Technology Law Review 21; Godwin, "An International Treaty on Cybercrime Sounds Like A Great Idea, Until You Read The Fine Print", *IP Worldwide*, 4 April 2001, available at http://cryptome.org/cycrime-godwin.htm (visited 20 December 2004).

[83] Irish law on interception is currently rooted in laws enacted with telephone voice calls in mind, and seems to leave substantial gaps when applied to email and other internet traffic. The relevant law is to be found in section 98 of the Postal and Telecommunications Services Act, 1983, the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 and section 7 of the Postal and Telecommunications Services (Amendment) Act, 1999. The European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations, 2003 (S.I. No. 535 of 2003) do not address the area of interception as such, leaving section 98 to control this area. One particular problem is that section 98 is limited to messages transmitted by "licensed operators", leaving interception of data transmitted by other means in a grey area. For Irish law on interception of communications generally, see: Collins, "Telephone Tapping and the law in Ireland" (1993) *Irish Criminal Law Journal* 31; Hall, *The Electronic Age: Telecommunication in Ireland* (1993), Ch. 28; Hall, "Recording Telephone Conversations" (1997) 91 (7) *Law Society Gazette* 4; and Hall, "Are Mobile Telephone Conversations Inviolable" (1998) 92 (7) *Law Society Gazette* 9.

[84] Wearden, "Europe 'near agreement' on cybercrime fight", http://news.zdnet.co.uk/internet/security/0,39020375,39156968,00.htm (visited 17 September 2004). See also the Home Office, "Internet Crime", http://www.homeoffice.gov.uk/crime/internetcrime/compmisuse.html (visited 17 September 2004).

criminal damage (under the Criminal Damage Act, 1991) or as a form of dishonesty (under the Criminal Justice (Theft and Fraud Offences) Act, 2001) when the evidence suggests that computer crime is *sui generis* and requires special attention in its own right.

Instead, the Convention and the Framework Decision present an opportunity for comprehensive reform of the law relating to computer crime. This would be consistent with the long-standing Government commitment[85] to promoting an Information Society and establishing Ireland as a suitable location for software and other information technology businesses, and it would be disappointing if the criminal law changes which would support these objectives should again be neglected.

[85] See, for example, the Information Society Commission at the Department of the Taoiseach, http://www.isc.ie/ (visited 20 December 2004).