Crimes Act 1961

[248 Interpretation

For the purposes of this section and **[[**sections 249to252]],—

access, in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system

[[authorisation includes an authorisation conferred on a person by or under an enactment or a rule of law, or by an order of a court or judicial process**]]**

History Note - Statutes of New Zealand

"authorisation": this definition was inserted, as from 13 July 2011, by s 4(2) Crimes Amendment Act 2011 (2011 No 29).

computer system —

(a) means—

(i) a computer; or

(ii) 2 or more interconnected computers; or

(iii) any communication links between computers or to remote terminals or another device; or

(iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and

(b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data.**]**

History Note - Statutes of New Zealand

Part 10 (comprising ss 217 to 305) was substituted by a new Part 10 (comprising ss 217 to 272), as from 1 October 2003, by s 15 Crimes Amendment Act 2003 (2003 No 39).

Section 248 was amended, as from 13 July 2011, by s 4(1) Crimes Amendment Act 2011 (2011 No 29) by substituting "sections 249 to 252" for "sections 249 and 250".

Commentary - Adams on Criminal Law

Cross references

s 249 accessing computers for dishonest purpose

s 250 damaging or interfering with computer system

s 251 making selling etc software for committing a crime

s 252 accessing computer system without authorisation

Government Communications Security Bureau Act 2003

s 17 issue of interception warrant

s 18 persons acting under warrant

s 19 authorisation to access computer system

New Zealand Security Intelligence Service Act 1969

s 4A issue of interception warrant

s 4D persons acting under warrant

Search and Surveillance Act 2012

s 98 application for search warrant

s 110 search powers

s 111 remote access search of thing authorised by warrant

CA248.01 "Access"

The definition of "access" is broad, as is that of "computer system". To "instruct" is to do something which causes the computer to undertake, or not undertake, certain functions, such as displaying further data, performing certain calculations or other transactions and the like. To "communicate with" will describe both passing information to and receiving information from a computer system. Both these concepts impliedly require that the person instructing or communicating with the computer system have some form of connection with the computer system through which instructions or communications may pass.

The next two elements of the definition use the word "data" which is not defined. The word "data" when used in reference to computers has been held to be restricted to information which is in a form that is computer readable; compare *R v Brown* [1996] 2 Cr App R 72 (HL). As such the data must exist in computer readable form, although such reading may be by electronic or optical means.

The general term "or otherwise make use of the resources of" the computer system should be interpreted consistently with the apparent class constituted by the other words in the section of communications or operations, using computer readable data or instructions or communications which are translated by the computer into computer readable format.

CA248.01A "Authorisation"

The concept of "authorisation" is critical to the definitions of the offences in s 252 and 250(2) and is also relevant to s 251. Normally the issue of authorisation will be determined by whether an accused either has express or implied authority or permission of any and all relevant parties who have a right to control or limit access to the computer or computer system. It is probable that access by an authorised person for

an improper purpose should be regarded as "unauthorised": *Salter v Director of Public Prosecutions (NSW)* [2011] NSWCA 190, (2011) 209 A Crim R 576. Difficulties of a different kind may arise where different parts of a single computer system are controlled by different persons, or various relevant parties have different rights in respect of the system or parts thereof, and only some of these affected parties affected by the relevant conduct have given authority for that conduct.

The statutory definition, added in 2011, is inclusive and provides that a person will be regarded as authorised to have access where, despite the wishes of the owner or controllers of the computer or computer system – or without their knowledge – authority to access the computer or computer system has been granted by an order of a court or judicial process or such authority is conferred by or under an enactment or a rule of law. The first element – authority under a court order or judicial process – will include access for law enforcement or national security reasons ordered in accordance with procedures provided by statute (for example under ss 110 and 111 of the Search and Surveillance Act 2012 where a search warrant has been granted).

Authorisation by or under a statute will include authority conferred by an authorisation to access a computer system under s 17 of the Government Communications Security Bureau Act 2003 or an interception warrant under s 19 of that Act or under s 4A of the New Zealand Security Intelligence Service Act 1969. In any case, the warrant will also extend authority to persons assisting with the execution of the warrant, see s 18 of the Government Communications Security Bureau Act 2003 and s 4D of the New Zealand Security Intelligence Service Act 1969.

Where authority to access a computer system might be conferred by a rule of the common law is unclear, but it is possible there might be authority in cases of emergency where access is needed to counter a serious risk to the life or health of a person or to prevent serious property damage. The Search and Surveillance Act 2012, s 14 confers a power on police to enter places or vehicles in such cases, but this does not extend to accessing a computer system. For recognition of general power to enter private property as an "agent of necessity", see [CA315.10C].

CA248.02 "Computer"

The definition of "computer system" is in broad terms.

The first key element is the word "computer", which is not itself further defined. Although there may be a small number of mechanical and analogue computers remaining in use, the word "computer" has come in common parlance to refer to electronic machines operating as digital computers. See *Pacific Software Technology Ltd v Perry Group Ltd* (2003) 7 NZBLC 103,950 (CA), at p 103,953;

"Digital computers rest on five functional elements: (i) input; (ii) storage of that input by a memory system; (iii) a control unit which receives data from memory and gives instructions for the necessary arithmetic; (iv) an arithmetic which carries out the control commands; (v) an output capacity."

As the Court of Appeal noted in *Pacific Software*, assistance with many of the key elements of computer programming and operations may be gained from the judgment of Pumphrey J in *Cantor Fitzgerald International v Tradition (UK) Ltd* [2000] RPC 95.

CA248.03 "2 or more interconnected computers"

The second key element is the term "interconnected", which appears in para (a)(ii). The meaning to be given to this term is crucial to the ambit of the definition and hence to the scope of the offences created by s 249 and s 250. The question is essentially whether interconnection is to be measured by reference to a computer user or consumer, or by reference to an operator or controller. It is possible for a computer user to access literally thousands of computers through the Internet by using the communications links which make the Internet possible. Are all these computers to be regarded as "interconnected", even though they may be owned by diverse peoples in different countries and operating on quite different technical specifications? The alternative is to treat "interconnected" as meaning that there is some form of connection between the computers which allows a single person with appropriate authority within the

system to determine how those computers will operate, and in appropriate cases to instruct one computer in such a way as to cause others to perform certain actions. The commonest such form is the so-called "local area network" of several linked computers which together provide computer services for a company, governmental agency or educational institution. It is suggested the latter, narrower, meaning is more appropriate, not least because it allows a more discriminating approach to the concept of "authorisation" which is a critical issue in relation to the offences created by s 250, in that we may distinguish between systems to which a person may have leave or authority to access as a user or consumer from those systems to which the same person has access or authority in the capacity of operator or controller or as authorised by law or judicial warrant.

It may also be argued that the inclusion of "communication links" in other parts of the definition points to the narrower meaning as being correct since there would be no need to refer to communications links between computers if the broader meaning of "interconnected" applied.

CA248.04 Communications links between computers or to remote terminals or other devices

As with other elements of the definition, the ambit of this part of the definition is not clear. The term "remote terminal" is in truth quite straightforward. It denotes a terminal, or point, where the system can be accessed and information or commands given by persons with appropriate authority, which is physically distanced from the main processing elements of the computer. EFTPOS machines in shops may be thought of as remote terminals (although their electronic componentry might itself bring them within the definition of a "computer"). The term "other devices" must be given a wide meaning, as there is an extraordinary diversity of instruments and machines which are in whole or in part operated by computers which are physically distanced from that computer. That diversity may be illustrated by the not uncommon examples of petrol pumps in self service stations, meteorological recorders, and traffic lights. A critical question may be whether the words "communication links" will be restricted to those links which are solely usable for the conveying of information or instructions between computers or between a computer and a remote terminal or other device, or whether it includes other links which may be used for both computer instructions and other communications. It is now commonplace for telephone subscribers to use the same telephone line for both oral communications and for electronic communications of a home computer to other computers by way of electronic mail or via the Internet. Many mobile phones are equally capable for being used for both oral and electronic communications. Does this mean a mobile phone or a telephone line is a "communication link" and therefore to be regarded as a part of a computer? There seems no reason why the courts should not adopt the broader meaning in appropriate cases, which might well be measured temporally — that is, if at the relevant time the telephone line or mobile phone was being used to link to a computer, it is relevantly part of a computer; if it is being used for other purposes it is not within the definition.

CA248.05 Paragraph (b)

Paragraph (b) includes any part of the items described in paragraph (a), and all related input, output, processing, storage, software, or communication facilities, and stored data.

The first part of the paragraph makes it clear that anything which is a part of a computer system or of a computer or a communications link, etc is itself to be regarded as a computer system. This is likely to be particularly relevant to the offences in s 250.

The second element of the paragraph relates to the key elements of a digital computer (see CA248.02). Input facilities relate to those facilities by which data or instructions can be conveyed to computer to be processed; the output facilities are those which allow the results of the processing to be conveyed to users of the computer, and will thus include terminal monitor screens, printers, and the like. Storage facilities are those elements of a computer system which allow for the permanent or temporary storage of relevant data or instructions. As to communications facilities, see CA248.04. "Software" is not defined in the section but may be described as the term which best encapsulates the sets of operating instructions for a computer system by which the computer system assembles and records data and instructions communicated to it, carries out any processing of data which it is instructed to perform, and communicates and/or stores the results of its processing. There is a helpful discussion of the key

components of computer programs in *International Business Machines Corp v Computer Imports Ltd* [1989] 2 NZLR 395 at p 408. The inclusion of “software” as part of a computer renders a little puzzling the specific inclusion of damage to software as elements of offences under s 250.

As to “data” see CA248.01