[HOUSE OF LORDS]

REGINA v. BOW STREET METROPOLITAN STIPENDIARY MAGISTRATE and Another, *Ex parte* GOVERNMENT OF THE UNITED STATES OF AMERICA

1999 July 12, 13; 15;
Aug. 5

Lord Steyn, Lord Hutton, Lord Saville of Newdigate, Lord Hobhouse of Woodborough and Lord Millett

Crime - Computer misuse - Unauthorised access - Whether extending to improper use by authorised user - Computer Misuse Act 1990 (c. 18), ss. 1(1), 2(1), 17(5)

Extradition - Extradition crime - Computer misuse - Conspiracy to secure unauthorised access to computer system with intent to commit theft and forgery - Whether extradition crime - Extradition Act 1989 (c. 33), s. 1(3), Sch. 1, para. 20 - Computer Misuse Act 1990, s. 15 - United States of America (Extradition) Order 1976 (S.I. 1976 No. 2144), Sch. 1, art. III

The United States Government sought the extradition of the accused from England. The allegation was that he had obtained account information from an employee of a charge card company, who was authorised to access its computer records solely for the purposes of her employment, and had used that information to encode forged credit cards and obtain fresh personal identification numbers, so as to draw large sums of money from automatic teller machines. The Secretary of State for the Home Department made an order to proceed, pursuant to section 4(2) of Schedule 1 to the Extradition Act 1989, specifying two proposed charges of conspiring with the employee to commit an offence under section 2(1) of the Computer Misuse Act 1990,[1] namely securing unauthorised access to a computer system contrary to section 1(1) of the Act with the additional intent to commit theft and forgery. A third charge alleged the causing of an unauthorised modification of the contents of a computer system, contrary to section 3 of the Act. The section 2(1) and section 3 offences carried terms of up to five years' imprisonment. The magistrate declined to commit the accused on the first two charges on the ground that the term "unauthorised access," as defined in section 17(5) of the Act of 1990, did not extend to a person who was authorised to control the computer in question but misused the information thereby obtained. The magistrate held, however, that the provision of information leading to the issuing of a new personal identification number amounted to the causing of an unauthorised modification of the contents of a computer system and committed the accused in custody on the third charge to await the Secretary of State's decision on his extradition. The U.S. Government sought judicial review of the magistrate's refusal to commit on the first two charges. The accused applied for a writ of habeas corpus on the ground, inter alia, that offences under the Act of 1990 were not extraditable. The Divisional Court, refusing both applications, held that, by virtue of paragraph 20 of Schedule 1 to the Act of 1989,[2] read with article III of Schedule 1

[1] Computer Misuse Act 1990, ss. 1(1): see post, p.223B-C.
S. 2(1): see post, p. 223C-D.
S. 15: see post, p. 222D-E.
S. 17(5): see post, p. 223G-H.

[2] Extradition Act 1989, Sch. 1, para. 20: see post, p.221E-F.

On appeal by the U.S. Government:—

Held, (1) that although, by paragraph 20 of Schedule 1 to the Extradition Act 1989, the term "extradition crime" was to be construed in relation to a foreign state by reference to the Order in Council applying to that state on the coming into force of the Act and to "any amendments" thereafter made to that Order, and neither the United States of America (Extradition) Order 1976 nor any amendments thereto extended to computer crime, article III of Schedule 1 to the 1976 Order provided for extradition not only for offences set out therein but for "any other offence" punishable by more than one year's imprisonment and extraditable under the law of the United Kingdom; that the provision in section 15 of the Computer Misuse Act 1990 that offences under sections 2 and 3 thereunder, and any conspiracy to commit such an offence, were offences to which an Order in Council could apply was in itself sufficient to bring those offences within the 1976 Order; and that, accordingly, the Divisional Court had correctly refused the application for habeas corpus (post, pp. 219D-F, 222A-B, 227E).

(2) Allowing the appeal, that on its true construction section 17(5) of the Computer Misuse Act 1990 provided that access by a person to a computer was unauthorised for the purposes of sections 1(1) and 2(1) of the Act if that person was neither entitled to control, in the sense of authorising or forbidding, access to the actual data involved, nor had the consent of a person entitled to exercise such control; that authority to access one piece of data could not be treated as authority to access other data of the same kind; and that, accordingly, since the employee had been given authority to access only that part of the company's data relating to work assigned to her, the access by her of other data for the purpose of the alleged conspiracy with the accused was unauthorised access within section 1(1), and the decision to discharge the accused on the first two charges would be quashed (post, pp. 219D-F, 223D-E, 224A-E, 226D-F, 227E).

Dicta of Astill J. in *Director of Public Prosecutions v. Bignell* [1998] 1 Cr.App.R. 1, 12-13, D.C. disapproved.

Decision of the Divisional Court of the Queen's Bench Division[1999] Q.B. 847; [1998] 3 W.L.R. 1156 reversed in part.

The following cases are referred to in the opinion of Lord Hobhouse of Woodborough:

Director of Public Prosecutions v. Bignell[1998] 1 Cr.App.R. 1, D.C.

Reg. v. Secretary of State for the Home Department, Ex parte Gilmore [1999] Q.B. 611;[1998] 2 W.L.R. 618; [1998] 1 All E.R. 264, D.C.

The following additional case was cited in argument:

Reg. v. Governor of Pentonville Prison, Ex parte Chinoy[1992] 1 All E.R. 317, D.C.

[3] United States of America (Extradition) Order 1976, Sch. 1, art. III: see post, pp. 221G-222A.

Appeal from the Divisional Court of the Queen's Bench Division.

This was an appeal, by leave of the House of Lords (Lord Lloyd of Berwick, Lord Steyn and Lord Clyde), by the Government of the United States of America from the judgment of the Divisional Court (Kennedy L.J. and Blofeld J.) refusing its application for an order of certiorari to quash the decision of a metropolitan stipendiary magistrate, Mr. Nicholas Evans, made on 11 June 1997, not to commit the accused, Adeniyi Momodu Allison , to prison under the Extradition Act 1989 to await the Secretary of State's decision as to his extradition to the United States of America on two charges of conspiracy to gain unauthorised access to a computer system with intent to commit theft and forgery.

At the conclusion of the hearing Lord Steyn announced that the appeal would be allowed for reasons to be given later.

The facts are stated in the opinion of Lord Hobhouse of Woodborough.

James Lewis and *Andrew Brierley* for the Government of the United States of America. To escape liability under section 2 of the Computer Misuse Act 1990 a person who causes a computer to perform any function with intent to secure access to any program or data must be authorised to secure access "of the kind in question to the program or data:" see section 17(5) of the Act. Authorisation must be determined as a question of fact by reference to authority given by the person who controls access of the kind in question to the data in question. There is nothing in the Act to exclude from liability under section 2 a person whose access to the data did not require him to break though an inbuilt password barrier because the data was located in files made available to him for the purposes of his work. The contrary dictum inDirector of Public Prosecutions v. Bignell [1998] 1 Cr.App.R. 1, 12-13 is wrong.

Sections 2 and 3 of the Act of 1990 fall within article III of the Extradition Treaty between the United States and the United Kingdom, as incorporated by the United States of America (Extradition) Order 1976, since they deal with offences punishable by more than one year's imprisonment and in respect of which extradition may be granted under both countries' laws. By virtue of paragraph 20 of Schedule 1 to the Extradition Act 1989, an "extradition crime" is one set out in the Order in Council under section 2 of the Extradition Act 1870 applying to that state on the coming into force of the Act of 1989. Although neither the list of extraditable offences in the United States of America (Extradition) Order 1976 nor any amendment thereto contains anything which corresponds to section 2 or 3 of the Act of 1990, section 15 of that Act provides that offences under sections 2 and 3 of that Act are offences to which an Order in Council made under section 2 of the Extradition Act 1870 can apply. Thus, section 15 amends the Order of 1976 by allowing it to incorporate sections 2 and 3 of the Act of 1990 into the list of extraditable offences: see Reg. v. Governor of Pentonville Prison, Ex parte Chinoy [1992] 1 All E.R. 317, 334.

Brierley followed.

Alun Jones Q.C. and *Helen Malcolm* for the accused. The Act of 1990 is primarily aimed at protecting the integrity of computers and computer systems, rather than the data they contain. The improper use of data is

---

In any event, crimes contrary to section 2 or 3 of the Act of 1990 are not "extradition crimes." Although section 15 of the Act of 1990 states that the offences to which an Order in Council under section 2 of the Act of 1870 "can" apply include offences under sections 2 and 3 of the Act of 1990, that is no more than a permissive or enabling provision. It confers the right to amend Orders in Council made under section 2 so as to include the further specified offences, but does not in itself effect the amendment. There are 12 states in respect of which such Orders are in force. Under section 2 of the Act of 1870 an Order in Council must recite or embody the terms of the arrangement between the two states. Parliament would not seek to unilaterally amend treaties with other states. [Reference was made to Reg. v. Secretary of State for the Home Department, Ex parte Gilmore [1999] Q.B. 611.]

[Lord Steyn. We shall refuse habeas corpus, quash the decision to discharge the accused on the first two charges and remit the matter to the magistrates' court for reconsideration. We shall report our reasons to the House in due course.]

Their Lordships took time for consideration.

5 August. Lord Steyn. My Lords, I have had the advantage of reading in draft the speech of my noble and learned friend, Lord Hobhouse of Woodborough. For the reasons he has given I would allow the appeal.

Lord Hutton. My Lords, I have had the advantage of reading in draft the speech which has been prepared by my noble and learned friend, Lord Hobhouse of Woodborough. I agree with it, and for the reasons which he gives I, too, would allow the appeal.

Lord Saville of Newdigate. My Lords, I have had the advantage of reading in draft the speech prepared by my noble and learned friend, Lord Hobhouse of Woodborough. I agree with it and, for the reasons he gives, I, too, would allow the appeal.

Lord Hobhouse of Woodborough. My Lords, on 18 March 1997 the accused, Mr. Allison , was arrested upon a provisional warrant issued under the Extradition Act 1989 at the request of the Government of the United States. It alleged that he had between 1 January 1996 and 18 June 1996 within the jurisdiction of the United States of America conspired with Joan Ojomo and others (1) to secure unauthorised access to the American Express computer system with intent to commit theft; (2) to secure unauthorised access to the American Express computer system with intent to commit forgery; and (3) to cause an unauthorised modification of the contents of the American Express computer system.

On 11 June 1997 the Bow Street metropolitan magistrate committed Mr. Allison on the third charge but declined to commit him on the first and second of the proposed charges. Mr. Allison brought habeas corpus proceedings challenging the view that any of the offences alleged were "extradition crimes" under the Act of 1989 and the United States of America (Extradition) Order 1976 (S.I. 1976 No. 2144). The U.S.

These challenges to the decision of the magistrate were heard by the Divisional Court (Kennedy L.J. and Blofeld J.), which gave judgment [1999] Q.B. 847 on 13 May 1998. The Divisional Court dismissed both the habeas corpus proceedings and the judicial review proceedings. They however certified a question of law of general public importance:

> "Whether, on a true construction of section 1 (and thereafter section 2) of the Computer Misuse Act 1990, a person who has authority to access data of the kind in question none the less has unauthorised access if: (a) the access to the particular data in question was intentional; (b) the access in question was unauthorised by a person entitled to authorise access to that particular data; (c) knowing that the access to that particular data was unauthorised."

This question was unhappily drafted; as will appear it perpetuates a confusion concerning the Act of 1990 which is implicit in the judgment of the Divisional Court.

On 15 July 1999, following a hearing concluded on 13 July, your Lordships' House allowed the Government's appeal, set aside the order of the Divisional Court, quashed the discharge by the magistrate of Mr. Allison on the first and second of the proposed charges and remitted the cause back to the magistrate, with your Lordships' reasons to be given later.

The facts

Joan Ojomo was an employee of American Express. She was assigned to the credit section of the company's office in Plantation, Florida, as a credit analyst. In her daily work it was possible for her to access all customers' accounts but she was only authorised to access those accounts that were assigned to her. However she accessed various other accounts and files which had not been assigned to her and which she had not been given authority to work on. Having accessed those accounts and files without authority, she gave confidential information obtained from those accounts and files to, among others, Mr. Allison . The information she gave to him and to others was then used to encode other credit cards and supply P.I.N. numbers which could then be fraudulently used to obtain large sums of money from automatic teller machines.

The evidence concerning Joan Ojomo's authority to access the material data showed that she did not have authority to access the data she used for this purpose. At no time did she have any blanket authorisation to access any account or file not specifically assigned to her to work on. Any access by her to an account which she was not authorised to be working on would be considered a breach of company policy and ethics and would be considered an unauthorised access by the company. The computer records showed that she accessed 189 accounts that did not fall within the scope of her duties. Her accessing of these accounts was unauthorised.

Using these methods, she and her fellow conspirators defrauded American Express of approximately U.S.$1m. Mr. Allison was arrested

The proposed charges against Mr. Allison therefore involved his alleged conspiracy with Joan Ojomo for her to secure unauthorised access to data on the American Express computer with the intent to commit the further offences of forging cards and stealing from that company. It is Joan Ojomo's alleged lack of authority which is an essential element in the offences charged.

The Extradition Act 1989

The Act of 1989 was enacted following reports of the English and Scottish Law Commissions recommending revisions of the law of extradition. The Act consolidated the previous law with amendments to give effect to those recommendations. The Extradition Act 1870 (33 & 34 Vic. c. 52) was among those repealed by the Act of 1989. The Act of 1870 included a definition of "extradition crime" in section 26 as meaning "a crime which, if committed in England ... would be one of the crimes described in the first Schedule" to the Act. The Schedule, as would be expected having regard to its date, consisted of a relatively short list. Between 1870 and 1989 the list was extensively added to by later Acts. But none of these statutes included a reference to computer crime such as that made criminal by the Computer Misuse Act 1990.

The scheme of the Act of 1989 was that whilst repealing the Act of 1870, it effectively preserved Schedule 1 to that Act and the later amendments. It also preserved Orders in Council made under section 2 of the Act of 1870 and the power to amend them. Under such statutory instruments the relevant regime is that laid down in Schedule 1 to the Act of 1989. Paragraph 20 of this Schedule provides that "extradition crime" in relation to a foreign state:

> "is to be construed by reference to the Order in Council under section 2 of the Extradition Act 1870 applying to that state as it had effect immediately before the coming into force of this Act [26 September 1989] and to any amendments thereafter made to that Order ..."

The relevant Order in Council governing extradition to the United States of America is the Order of 1976. It gives effect to and schedules the Extradition Treaty between the respective governments of the United Kingdom and the United States. Article III of the Treaty provides:

> "(1) Extradition shall be granted for an act or omission the facts of which disclose an offence within any of the descriptions listed in the Schedule annexed to this Treaty, which is an integral part of the Treaty, or any other offence, if: (*a*) the offence is punishable under the laws of both parties by imprisonment or other form of detention for more than one year or by the death penalty; (*b*)the offence is extraditable under the relevant law, being the law of the United Kingdom or other territory to which this Treaty applies by virtue of sub-paragraph (1)(*a*) of article II; and (*c*) the offence constitutes a felony under the law of the United States of America. (2) Extradition shall also be granted for any attempt or conspiracy to commit an

The Schedule annexed to the Treaty does not include any reference to computer crime. Therefore if an offence under the Computer Misuse Act 1990 is to come within the terms of the Treaty it will have to be as some "other offence." There is no dispute in the present case that an offence under section 2 of the Act of 1990 comes within (1)(*a*)being punishable by imprisonment for more than one year. Similarly it is not disputed that the conduct charged would constitute felonies under the

law of the United States ((1)(*c*)). The question which has been raised by Mr. Allison on his habeas corpus application is whether the offences alleged are extraditable under the law of the United Kingdom ((1)(*b*)) and therefore as conspiracies come within paragraph (2) of the article.

In September 1989 there was no provision of the law of the United Kingdom which made computer crime extraditable; indeed, there was no such provision which made it (as such) criminal at all. At that time such conduct fell outside the scope of the criminal law of the United Kingdom and accordingly outside the scope of the Extradition Treaty.

The Treaty and the Order in Council have not been amended. The provision which has been relied upon by the Government of the United States as bringing offences under the Computer Misuse Act 1990 within the terms of the Treaty is section 15 of that Act, which provides:

> "The offences to which an Order in Council under section 2 of the Extradition Act 1870 can apply shall include—(*a*) offences under section 2 or 3 above; (*b*) any conspiracy to commit such an offence; and (*c*) any attempt to commit an offence under section 3 above."

The argument of Mr. Allison is that this provision does not suffice to satisfy the requirement of paragraph 20 of Schedule 1 to the Act of 1989: it is not an amendment of the Order of 1976. This argument, however, fails to give effect to the obvious and express intention of section 15. The section provides that the relevant offences are ones to which such an Order can apply; it therefore makes the offences ones which are extraditable for the purpose of that Order. The Computer Misuse Act 1990 does not purport to alter the Treaty or the Order nor does it need to; they include not only the offences listed in the Schedule annexed to the Treaty but also "any other offence." All that is needed is some provision of the law of the United Kingdom which provides, supplementing the provisions of the 1989 and earlier Acts, that computer crime shall both become an offence and be extraditable under the law of the United Kingdom; the Act of 1990 contains provisions that meet this need.

The Divisional Court rightly held that the offences charged did come within the terms of the Treaty and the Order of 1976. In Reg. v. Secretary of State for the Home Department, Ex parte Gilmore[1999] Q.B. 611, 619-620 the Divisional Court rejected an argument that the effect of the Act of 1989 was to free the Treaty from the constraints imposed by Schedule 1 to the Act of 1870. But that is not the question raised by the argument of Mr. Allison in the present case. The question is one of the construction of

The Computer Misuse Act 1990

Sections 1 and 2 of the Act provide:

> "1(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; (*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."

> "2(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ('the unauthorised access offence') with intent—(*a*) to commit an offence to which this section applies; or (*b*) to facilitate the commission of such an offence (whether by himself or by any other person) ..."

Section 2 is thus dependent on section 1.

On the evidence before the magistrate, the conduct of Joan Ojomo came fairly and squarely within the provisions of section 1(1). She intentionally caused a computer to give her access to data which she knew she was not authorised to access. The reason why the magistrate did not commit Mr. Allison on charges 1 and 2 was that he felt constrained by the provisions of section 17 of the Act of 1990 and the interpretation put upon them by the Divisional Court in Director of Public Prosecutions v. Bignell [1998] Cr.App.R. 1; the Divisional Court also followed and applied Bignell'scase.

The relevant subsections of section 17 read:

> "(1) The following provisions of this section apply for the interpretation of this Act. (2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—(*a*) alters or erases the program or data; (*b*) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; (*c*) uses it; or (*d*) has it output from the computer in which it is held (whether by having it displayed or in any other manner); and references to access to a program or data (and to an intent to secure such access) shall be read accordingly ... (5) Access of any kind by any person to any program or data held in a computer is unauthorised if—(*a*) he is not himself entitled to control access of the kind in question to the program or data; and (*b*) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled."

Section 17 is an interpretation section. Subsection (2) defines what is meant by access and securing access to any programme or data. It lists

---

Subsection (5) therefore has a plain meaning subsidiary to the other provisions of the Act. It simply identifies the two ways in which authority may be acquired—by being oneself the person entitled to authorise and by being a person who has been authorised by a person entitled to authorise. It also makes clear that the authority must relate not simply to the data or programme but also to the actual kind of access secured. Similarly, it is plain that it is not using the word "control" in a physical sense of the ability to operate or manipulate the computer and that it is not derogating from the requirement that for access to be authorised it must be authorised to the relevant data or relevant programme or part of a programme. It does not introduce any concept that authority to access one piece of data should be treated as authority to access other pieces of data "of the same kind" notwithstanding that the relevant person did not in fact have authority to access that piece of data. Section 1 refers to the intent to secure unauthorised access to any programme or data. These plain words leave no room for any suggestion that the relevant person may say: "Yes, I know that I was not authorised to access that data but I was authorised to access other data of the same kind."

Bignell's case

Director of Public Prosecutions v. Bignell [1998] 1 Cr.App.R. 1 was decided in 1997. The leading judgment was given by Astill J., with whom Pill L.J. agreed. Two police officers had been convicted before the stipendiary magistrate of an offence under section 1 of the Act of 1990. They had for their own private purposes caused a police computer operator to obtain for them from the police national computer information about the ownership and registration of two cars. They had no authority to make that request or to obtain that information for that purpose. They were only permitted to make such a request for police purposes; indeed, to obtain the information, they had to misrepresent to the computer operator the purpose of their request. The computer operator acted under an authorisation from the Commissioner of the Metropolitan Police. He was authorised to use the computer to access the data on the database at the request of police officers; he was required to ascertain and log the reason for the request.

The magistrate convicted the two officers of an offence under section 1. Their appeal to the Crown Court was allowed but the prosecution requested the Crown Court to state a case for the Divisional Court. The four stated questions of law are set out in the report, at p. 8. They asked whether the Crown Court had been right in law to allow the appeal. The Divisional Court upheld the decision of the Crown Court.

The conclusion of the Divisional Court was probably right. It was a possible view of the facts that the role of the defendants had merely been to request another to obtain information by using the computer. The computer operator did not exceed his authority. His authority permitted him to access the data on the computer for the purpose of responding to requests made to him in proper form by police officers. No offence had been committed under section 1 of the Act of 1990. The Divisional Court rightly stated that the defendants could have been prosecuted for an offence under the Data Protection Act 1984.

However, in the course of his judgment Astill J., as he had been invited to by the Crown Court and the argument of counsel, expressed views about the purpose of the Act of 1990 and the effect of section 17(5). Thus, he treated the primary issue as being "whether a police officer who secures access to the police national computer for a non-police purpose secures unauthorised access" for the purposes of section 1. The submissions, at p. 8, which he accepted were that the defendants "were authorised to control access to the computer within the meaning of section 17(5) because they were authorised to obtain the material on the computer by causing the computer to function" and that "controlling access is different from defining or restricting authority to access and section 17(5)(*b*) provides for the position of a person who enjoys a restricted level of access and is, therefore, barred from other levels of access without the consent of someone who is entitled to access at that "level." This acceptance, at pp. 12-13, introduces a number of glosses which are not present in the Act. The concept of control is changed from that of being entitled to authorise to authorised to cause the computer to function. The concept of access to a program or data is changed to access to the computer at a particular "level." He also accepted the submission that the purpose of the Act was to criminalise the breaking into or hacking of computer systems which he understood to mean preserving the "integrity of computer systems." He accordingly characterised the defendants as persons who had "control access" (using the word "control" as a noun) "of the kind in question."

It was this use of language, departing from the language of the statute and unnecessary to the decision of that case, which misled the magistrate and the Divisional Court in the present case.

The decision of the Divisional Court

My Lords, what I have already said serves to identify the points upon which the Divisional Court fell into error. The certified question refers to "authority to access data of the kind in question." The use of the phrase "data of the kind in question" seems to derive from a simple misreading of section 17(5) and a confusion between kinds of access and kinds of data. Nor is section 1 of the Act concerned with authority to access kinds of data. It is concerned with authority to access the actual data involved. Because section 1(1) creates an offence which can be committed as a result

The key passage in the judgment of Kennedy L.J. [1999] Q.B. 847, 857, with which Blofeld J. agreed, follows on his quotation of section 17(5):

> "Miss Montgomery [for Mr. Allison] submits that it is clear from the evidence that Joan Ojomo was entitled to control access of the kind in question to the program or data, just like the police officers inBignell's case, so the access was not unauthorised even though she misused the information she obtained. Mr. Lewis [for the government] submits that her access was unauthorised because it was intentional, unauthorised by a person entitled to authorise access to that particular data and carried out when she knew that the access to that data was unauthorised. I confess that I found Mr. Lewis's approach to be the more attractive but at the end of the day it seems to me that it fails to do justice to the words 'of the kind in question' which qualify the word access in section 17(5). Joan Ojomo was entitled to control access of the kind in question. She was operating in a regular way at her authorised level. As Astill J. said inBignell's case [1998] 1 Cr.App.R. 1, 12b, the Act of 1990 was enacted to criminalise the 'hacking' of computer systems and the Data Protection Act 1984 was enacted to criminalise improper use of data."

Thus, Kennedy L.J. is making the same elisions as Astill J. He treats the phrase "entitlement to control" as if it related to the control of the computer as opposed to the entitlement to authorise operators to access to programs and data. He adopts the extraneous idea of an authorised level of access without considering whether, on the facts of the case, it corresponds to the relevant person's authority to access the data in fact accessed. He confines section 1 of the Act to the "hacking" of computer systems as opposed to the use of a computer to secure unauthorised access to programs or data. Upon a misreading of section 17(5), he fails to give effect to the plain words of section 1. The meaning of the statute is clear and unambiguous. But it is right that I should briefly say something about the argument based upon the Law Commission's Working Paper No. 110, "Computer Misuse" and its report, "Computer Misuse" (Law Com. No. 186) (1989) (Cm. 819) which (together with the Scottish Law Commission's Report on Computer Crime (Scot. Law Com. No. 106) (1987) (Cm. 174)) led to the passing of the Act of 1990. The argument was influential in the Divisional Court both inBignell's case and in the present case and was further relied on by the respondent before your Lordships. The respondent quoted passages from the working paper and the report to the effect:

> "It should be made clear that 'unauthorised' refers to the obtaining of access to a computer system. Our preliminary view is that it would be undesirable for a hacking offence to extend to an authorised user who is using the computer system for an unauthorised purpose:" working paper, paragraph 6.24(iv).

> "if an employee deliberately seeks to enter part of his employer's system from which he is clearly debarred his conduct is of the same

> "if the hacking offence is to be aimed at protecting the integrity of the computer (and our view is that it should), then there is no justification for exempting employees who threaten that integrity:" report, para. 3.36.

Read as a whole, the report makes it clear that the term "hacking" is used conveniently to refer to all forms of unauthorised access whether by insiders or outsiders and that the problem of misuse by insiders is as serious as that by outsiders: paragraph 3.5. The offence should cover a person who causes the computer to perform a function when he "should know that *that* access is unauthorised:" paragraph 3.33 (emphasis added). An employee should only be guilty of an offence if his employer has clearly defined the limits of the employee's authority to access a program or data: paragraph 3.37. Similar passages are to be found in the Report of the Scottish Law Commission.

Whilst the Report of the Law Commission supports the correctness of the*decision* in Bignell's case [1998] 1 Cr.App.R. 1—the phrase "causing a computer to perform any function" ... refers to the "manipulation" of a computer: paragraph 3.26—it does not justify the language used by Astill J. followed by Kennedy L.J. in the present case. The consideration of the mischief which the Act was designed to meet confirms and does not contradict the clear meaning of section 1 of the Act and the equally clear purpose of section 17(2) (5).

The decision of the Divisional Court in the present case was erroneous and the appeal fell to be allowed. As your Lordships' House has already announced, the case has been remitted to the magistrate for reconsideration. Full reasons having been given for allowing the appeal, it is unnecessary separately to respond to the certified question.

Lord Millett. My Lords, I have had the advantage of reading in draft the speech of my noble and learned friend, Lord Hobhouse of Woodborough. I agree with it, and for the reasons he gives I, too, would allow the appeal.

Appeal allowed.
Cause remitted to magistrate for reconsideration.
No order as to costs.
Solicitors: Crown Prosecution Service, Headquarters; Burton Copeland.

C. T. B.

BACK TO TOP