CO/1004/2006

Neutral Citation Number: [2006] EWHC 1201 (Admin)
IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
DIVISIONAL COURT

Royal Courts of Justice
Strand
London WC2

Thursday, 11th May 2006

B E F O R E:

LORD JUSTICE KEENE
MR JUSTICE JACK

- - - - - - -

DIRECTOR OF PUBLIC PROSECUTIONS

Appellant

-v-

DAVID LENNON

Respondent

- - - - - - -

Computer-Aided Transcript of the Palantype Notes of
Smith Bernal Wordwave Limited
190 Fleet Street London EC4A 2AG
Tel No: 020 7404 1400 Fax No: 020 7831 8838
(Official Shorthand Writers to the Court)

- - - - - - -

MR RICHARD BROWN (instructed by Crown Prosecution Service, Organised Crime Division, 50 Ludgate Hill, London EC4M 7EX) appeared on behalf of the Appellant
MR TOM ALLEN (instructed by Messrs Tuckers Solicitors, Manchester M2 3HZ) appeared on behalf of the Respondent

- - - - - - -

J U D G M E N T
(**As approved by the Court**)

- - - - - - -

LORD JUSTICE KEENE: I shall ask Mr Justice Jack to give the first judgment.

1. MR JUSTICE JACK: On 2nd November 2005 District Judge Kenneth Grant, sitting as a Youth Court in Wimbledon, ruled that there was no case to answer by the defendant, David Lennon, and dismissed the charge brought against him under section 3(1) of the Computer Misuse Act 1990. The Director of Public Prosecutions now appeals against that decision by case stated.

2. David Lennon was charged that, contrary to section 3(1), on a day between 30th January and 5th February 2004 he caused an unauthorised modification to a computer belonging to Domestic and General Group Plc ("D&G") with intent to impair the contents of the computer. The facts which lay behind the charge were the following. Mr Lennon was employed by D&G for three months until he was dismissed in December 2003. He was then 16. On 30th January 2004 Mr Lennon started to send emails to D&G using a "mail-bombing" program called Avalanche V3.6 which he had downloaded from the Internet. The program was set to "mail until stopped". That meant it would continue to send emails until it was manually stopped from doing so. The majority of the emails purported to come from Betty Rhodes, who was D&G's Human Resources Manager. Her email address was purportedly used. Each email contained a list of other employees of D&G to whom it was copied once it reached D&G, thus increasing the email traffic. During the last few hours of the emailing different addresses were used. The purpose of this was to try to defeat attempts to prevent the emails from continuing to arrive. The last message stated "it won't stop" and was addressed to Betty Rhodes. It was estimated that Mr Lennon's use of the program caused approximately 5 million emails to be received by the D&G email servers. When D&G's employees arrived for work on Monday 2nd February, they took steps to stop the emails and eventually this was done. Mr Lennon was arrested and interviewed. He admitted sending the emails purporting to come from Betty Rhodes. He said that his intention was to cause a "bit of a mess up" in the company; that he did not consider what he was doing was criminal; that he did not realise the repercussions of his actions; and it was not his intention to cause the damage to D&G which D&G had in fact sustained. He said also that he could have carried out a PING attack, but had not because that would have only slowed the network for a few hours.

3. The relevant parts of section 3 provide:

> "(1) A person is guilty of an offence if—
>
> (a) he does any act which causes an unauthorised modification of the contents of any computer; and
>
> (b) at the time when he does the act he has the requisite intent and the requisite knowledge.
>
> (2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary."

4. It is also necessary to refer to the interpretation provisions of section 17. Subsections (7) and (8) are relevant. They provide:

"(7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer—

(a) any program or data held in the computer concerned is altered or erased; or

(b) any program or data is added to its contents;

and any act which contributes towards causing such a modification shall be regarded as causing it.

(8) Such a modification is unauthorised if—

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled."

5. The prosecution case was that by his actions in relation to the Avalanche program Mr Lennon caused an unauthorised modification to the contents of D&G's computers by adding data to their contents, that is to say, the half million emails which he caused to be sent, and that when he did so he had the requisite intent and the requisite knowledge. It was alleged that he had the requisite intent as provided for by section 3(2) because he

intended to hinder the operation of the computers by overwhelming them with the emails - section 3(2)(a), and that he intended thereby to prevent or hinder access to their programs and data - section 3(2)(b), and to impair the operation of their programs and the reliability of their data - section 3(2)(c). It was alleged that he had the requisite knowledge as provided for by section 3(4) because he had knowledge that the modifications he intended to cause by adding the emails to the data in the computers were unauthorised. All of this was accepted on behalf of Mr Lennon as sustainable in law, save that it was submitted that on the evidence the modifications could not be shown to be unauthorised. The basis of that submission was that the function of the servers was to receive emails, so D&G clearly consented to receiving emails on them, and so D&G authorised potential senders of emails to modify the contents of the server by sending them.

6. It was submitted before the District Judge on behalf of the prosecution that a computer owner consents only to the receipt of emails from those wanting to make a *bona fide* communication with him. So here D&G did not consent to receiving emails in the number and in the circumstances which Mr Lennon sent them. It was secondly submitted that the emails Mr Lennon sent were unauthorised from the moment that he clicked on the send button. This was to meet an argument made on behalf of Mr Lennon that, if it was the number which were sent that made their sending unauthorised, the first emails were authorised and thereafter it was not possible to draw a line. Thirdly and alternatively, it was submitted that, as the number of emails built up, a point would have been reached when their sending became unauthorised. Fourthly, it was submitted that as all the emails came from a person other than the purported sender they were unauthorised.

7. The District Judge's opinion stated in the case can be summarised as follows:

   (1) section 3 was intended to deal with the sending of malicious material such as viruses, worms and Trojan horses which corrupt or change data, but not the sending of emails;
   (2) as D&G's servers were configured to receive emails, each modification occurring on the receipt of an email sent by Mr Lennon was unauthorised.

8. The issue this court has to consider is whether the addition to the data on D&G's servers arising from the receipt of emails sent by Mr Lennon was unauthorised. Section 17(8) is the relevant provision. Mr Lennon was not the person who was entitled to determine whether the "modification" arising from such receipt should be made. That refers to the person who controls the email address, that is the receiving computer, who will normally be the owner. So section 17(8)(a) is satisfied. The question is then whether Mr Lennon had "consent to the modification from any person who [was] so entitled" - section 17(8)(b).

9. I agree, and it is not in dispute, that the owner of a computer which is able to receive emails is ordinarily to be taken as consenting to the sending of emails to the computer. His consent is to be implied from his conduct in relation to the computer. Some analogy can be drawn with consent by a householder to members of the public to walk up the path to his door when they have a legitimate reason for doing so, and also with

the use of a private letter box. But that implied consent given by a computer owner is not without limit. The point can be illustrated by the same analogies. The householder does not consent to a burglar coming up his path. Nor does he consent to having his letter box choked with rubbish. That second example seems to me to be very much to the point here. I do not think that it is necessary for the decision in this case to try to define the limits of the consent which a computer owner impliedly gives to the sending of emails. It is enough to say that it plainly does not cover emails which are not sent for the purpose of communication with the owner, but are sent for the purpose of interrupting the proper operation and use of his system. That was the plain intent of Mr Lennon in using the Avalanche program. The difference can be demonstrated in this way. If Mr Lennon had telephoned Ms Rhodes and requested consent to send her an email raising a point about the termination of his employment, she would have been puzzled as to why he bothered to ask and said that of course he might. If he had asked if he might send the half million emails he did send, he would have got a quite different answer. In short the purpose of Mr Lennon in sending the half million emails was an unauthorised purpose and the use made of D&G's email facility was an unauthorised use.

10. That is sufficient to answer the question raised by the case stated, namely whether the magistrate was right to find that there was no case to answer. There was a case to answer. But I should deal with some further aspects of the submissions that were addressed to us.

11. The basis of the main submission made by Mr Tom Allen on behalf of Mr Lennon was that the emails sent by Mr Lennon were to be considered on an individual basis, and that there was implied consent to each and so for all. That, I consider, is wrong for the reason I have already given. Further, for the purpose of deciding whether there was implied consent Mr Lennon's conduct is not to be considered on an email by email basis: it is to be considered as a whole. Further again, his purpose was present from the beginning and he initiated the sending of the emails by the single action of starting the Avalanche program. It would run until stopped. Mr Allen submitted that if there was some point at which the sending of emails became unauthorised by reason of their number, then there could be no certainty in the law because that point could not be sufficiently identified. So, he said, the offence offended against Article 7 of the European Convention on Human Rights (no punishment without law). Here the sending of the emails was unauthorised from the start. It should not, however, be thought that I would otherwise have accepted Mr Allen's submission.

12. It was submitted by Mr Richard Brown on behalf of the prosecution that as the emails purported to come from a person who had not sent them or authorised sending them, namely Ms Rhodes, and purported to come from her email address, they were not authorised for the purpose of section 3(4). This was the fourth of the submissions recorded in the case stated as having been made on behalf of the prosecution. It does not, however, feature in the statement in the case of the District Judge's opinion. Mr Brown relied on Zezev and Yarimaka v Governor of HM Prison Brixton and another [2002] 2 Cr App R 33. In that case Wright J in his judgment stated his agreement with that delivered by the Lord Chief Justice Lord Woolf. He then referred to the argument presented on behalf of Mr Zezev and continued:

> "But if an individual, by misusing or bypassing any relevant password, places in the files of the computer a bogus e-mail by pretending that the password holder is the author when he is not, then such an addition to such data is plainly unauthorised, as defined in section 17(8); intent to modify the contents of the computer as defined in section 3(2) is self-evident and, by so doing, the reliability of the data in the computer is impaired within the meaning of section 3(2)(c)."

The basis of the statement that such an email is unauthorised is that it enters the computer by a false pretence and so is bogus, in that it purports to come from somebody other than the actual sender. That conclusion was plainly justified on the facts of that case. I consider that the same analysis is also applicable to the circumstances here because D&G gave no implied consent to the receipt of malicious emails purporting to come from its Human Resources Manager. But I would not necessarily be of the view that in all circumstances an email purporting to come from one person but coming from another is to be treated as unauthorised. For example such an email might be sent as a joke with no malicious intent, and then it could be argued that it was covered by the implied consent of the computer's owner. The answer would depend upon the circumstances, and I express no view upon it.

13. I would answer the question posed in the case stated "no", that is to say the District Judge was not right to find that there was no case to answer, and I would remit it to him to continue with the hearing. Section 3(4) requires that it be established not only that the modifications caused to D&G's computers should be unauthorised, but that Mr Lennon had knowledge that they were unauthorised. That is not an issue which arises on the case stated and it will have to be addressed by the District Judge in due course. One test which the District Judge might consider applying is the answer which Mr Lennon would have expected had he asked D&G whether he might start Avalanche - a point I have referred to in paragraph 9 above. I mention that because it seems to me that it points to the reality of the situation, something which, I consider, has been rather missed in this case thus far.

14. LORD JUSTICE KEENE: I agree. The critical issue is that of "consent" as that word is used in section 17(8) of the Act. I, for my part, see a clear distinction between the receipt of emails which the recipient merely does not want but which do not overwhelm or otherwise harm the server, and the receipt of bulk emails which do overwhelm it. It may be that the recipient is to be taken to have consented to the receipt of the former if he does not configure the server so as to exclude them. But in my judgment he does not consent to receiving emails sent in a quantity and at a speed which are likely to overwhelm the server. Such consent is not to be implied from the fact that the server has an open as opposed to a restricted configuration.

15. I too would allow this appeal and remit the matter to the District Judge to continue the hearing.

16. Yes?

17. MR BROWN: My Lord, I am grateful. There is no application.

18. LORD JUSTICE KEENE: Thank you both very much.
