Neutral Citation Number: [2013] EWCA Crim 1420
No: 201302960 A7
IN THE COURT OF APPEAL
CRIMINAL DIVISION

Royal Courts of Justice
Strand
London, WC2A 2LL

Wednesday 31st July 2013

B e f o r e:

LORD JUSTICE LEVESON

MRS JUSTICE SHARP DBE
MR JUSTICE SPENCER
R E G I N A

v

LEWYS STEPHEN MARTIN

Computer Aided Transcript of the Stenograph Notes of
WordWave International Limited
A Merrill Communications Company
165 Fleet Street London EC4A 2DY
Tel No: 020 7404 1400 Fax No: 020 7404 1424
(Official Shorthand Writers to the Court)

Mr M Griffiths (Solicitor Advocate) appeared on behalf of the **Appellant**
Mr M Yale appeared on behalf of the **Crown**

J U D G M E N T
(As Approved)

1. LORD JUSTICE LEVESON: On 12 April 2013 in the Crown Court at Maidstone the appellant, Lewys Martin, pleaded guilty to various contraventions of the Computer Misuse Act 1990 ("the Act"), for which on 16 May 2013 he was sentenced by His Honour Judge Byers to a total of two years' imprisonment. He now appeals against sentence by leave of the single judge. Having regard to the public significance rightly attached to offending of this nature, we will deal with the facts and principles in some detail.

The offences and sentences

2. The relevant offences and sentences passed on each, all of which were ordered to run concurrently to each other, were as follows:

i) For five offences of unauthorised modification of computer material contrary to section 3(1) of the Act he was sentenced to two years' imprisonment. The maximum sentence for that offence is ten years' imprisonment. These were counts 1, 3, 5, 7 and 8.

ii) For one offence of securing unauthorised access to computer material with intent contrary to section 2(1)(a) of the Act he was sentenced to 12 months' imprisonment. The maximum sentence for that offence is five years' imprisonment. This was count 9.

iii) For one offence of securing unauthorised access to computer material contrary to section1 of the Act he was sentenced to six months' imprisonment. The maximum sentence for that offence is two years' imprisonment. This was count10.

iv) For two offences of making, supplying or obtaining articles for use contrary to section 3(A) and (5) of the Act he was sentenced to four months' imprisonment. The maximum sentence for that offence is also two years' imprisonment. These were counts 12 and 13.

3. A deprivation order was made under section143 of the Powers of Criminal Courts (Sentencing) Act 2000 in relation to various items of computer equipment that were seized. Nine other counts relating to eight other offences under the Act and one offence related to section49 of the Regulation of Investigatory Powers Act 2000 were ordered to lie on the file.

The facts

4. We now turn to the facts and deal with them in chronological order, referring where relevant to the counts to which they related on the indictment.

5. Shortly before 11.40am on 3 March 2011, the appellant launched a Denial of Service ("DOS") attack on the University of Oxford website. DOS attacks involved flooding a website with internet traffic from a single device and internet connection so that the site is not able to respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. One of the system administrators at the website discovered that

there were a large number of requests from a particular Internet Provider (IP) address. The requests from this IP address caused the site to be unresponsive. The administrator blocked the address, and normal service was then resumed. However after the block was put in place, the attack migrated to other sites.

6. On 23 March 2011, the appellant sent to that University an e-mail signed SL1NK which said: "You Just Don't fucking learn". On 2/3 December 2011 he sent it a further e-mail which read:

> "I have owned you once before (DDOS attack about six to seven months ago?) and I am going to do it again along with Cambridge. I have access to your SQL users and password database, they are encrypted as you obviously know but it won't take long and by the time you have read this message I will have sold the two databases and what is needed to have been done will have been done".

7. The IP address for the sender appeared to be based in the United States. DDOS refers to a "Distributed Denial of Service attack. It is similar to a DOS attack, but on a larger scale, using any number of devices and internet connections. It causes greater disruption and is more difficult to detect. SQL means structured query language and can be attacked by a "structured query language injection attack", which takes advantage of insecure codes on a system connected to the internet, to bypass Firewalls and access data not normally available. This was count 1 on the indictment.

8. Count 10 concerned conduct initiated a week after Count1. On 10 March 2011 the appellant made an anonymous telephone call to a Mr David Bradley. He told Mr Bradley that all of his personal and financial information was available on the internet as a result of a Trojan which had been placed on his computer. Mr Bradley asked exactly what sort of information. The appellant said it was details of his loans, credit cards, bank statement, date of birth, address, telephone number, passwords, and his girlfriend's details. The appellant said he felt sorry for him and had changed his internet banking password to stop others from accessing his account. He gave Mr Bradley the new password. Mr Bradley immediately tried to log on to his bank account with his original password. It did not work. He tried the one given by the appellant. It worked. Mr Bradley had to cancel his cards and order replacements.

9. On 3 May 2011 police investigating a burglary searched the appellant's home address in Dover. They seized four USB storage devices and a desktop computer. They found nothing pertaining to the burglary on those items and returned them to the appellant at his home address. However when they were there, one of the officers noticed an envelope with a third party's name on it. The appellant then offered to pay the officer £1,000 to say that he had not seen it. The appellant was re-arrested and interviewed. Further forensic examination was then made of the items that had been seized. It was confirmed that the appellant was then on bail.

10. We move forward to 29 January 2012, when the appellant launched a further DOS attack on the University of Oxford website between 02.21 hours and 15.40 hours. It was detected as the requests forming the attack contained the same data string

contained in the previous attack. The appellant used a program called CyberGhost. This was a program which provides misleading information regarding the location of an IP address, and, as a result, anonymity for its user.

11. During the attack, anyone trying to access the University's website would have either received a very slow response or an error message from their browser. This disrupted the University's business and may have resulted in damage to its reputation. Nearly two weeks' of man hours were expended in dealing with these attacks. This was count 3.

12. As foreshadowed in the earlier e-mail, at 3.50pm on 29January 2012 the appellant launched a DOS attack on the University of Cambridge website, and the system became unresponsive. The attack was traced to a particular IP address and a block placed upon it. Normal service was resumed after about 20 minutes. Ten minutes later a series of connections with the University Server was received via a tool user by network engineers to probe networked computers for information. Just after 5.00pm the University received an e-mail from SL1NK which said: "I have your user and password database sat on my drive and I am also guessing you have noticed your site CAM.AC.UK is under attack" and: "If you ban the IP address I will just switch it again so don't waste your time". Further access attempts and further e-mails from SL1NK were received, one of which read: "You will never find me and you know you won't". These ended on 31January 2012.

13. Similar concerns were expressed by Cambridge University as had been expressed by Oxford University, regarding the damage that such attacks might do. The website was thet University's primary gateway to its undergraduate and postgraduate prospectuses. It was updated daily with news and job vacancies. The DOS attack coincided with the launch of the University Science Week programme and online event booking system, which is one of their major public engagement activities and the largest free science festival in the UK. They also expended nearly two weeks' worth of man hours dealing with the attacks. This was count 5.

14. The facts giving rise to count 7 commenced three days after the attack on Cambridge University. At 9.45am on 1 February 2012 the appellant launched a DOS attack on no less significant a website than that belonging to the Kent Police. It started at one IP address then switched to another, using more and more memory and processing power in the web server. Those IP addresses were blocked. The attack began again from a third IP address, which was also blocked. The attack continued until lunchtime. At one stage, the server had to shut down completely for 30 minutes and disrupted legitimate activity for a matter of a few hours. Once it re-started, it returned to normal operation.

15. At around 10.00am that morning, after the attack had started, the appellant telephoned the BBC South East news desk and informed a journalist that he had hacked into the Kent Police website. He said he was doing it "because I can". He would not give his name but gave the journalist the SL1NK e-mail address. The journalist informed her editor, who then informed the police. The appellant also made a number of telephone calls to his girlfriend during the attack. He discussed the attack and suggested that he might try and attack the Metropolitan Police website instead.

16. The following day, on 2February 2012, the appellant carried out a second DOS attack on the Kent Police website between 12.37pm and 12.51pm. This attack causing the server to run very slowly.

17. The Kent Police public website receives around 6,500 visits a day. That is some 200,000 visits per month. It gives members of the public a wide range of information about Kent Police, crime, advice and news. It is also the primary communication channel for urgent appeals for information, serious crimes and major emergency incidents.

18. On 3 February 2012 police executed a warrant and searched the appellant's home. The appellant said: "The Kent Police website was hacked the other day". He was arrested and told that his computers would be seized. He said they were all encrypted and refused to provide passwords until he had seen his solicitor. The fact of encryption speaks of the sophistication of this operation. It does not appear that the appellant ever accurately provided the encrypted passwords. Information received this morning was to the effect that he had forgotten it; we find that explanation lacking in plausibility. It might have been plausible at the moment that he was initially interviewed, but not thereafter.

19. In addition, a handwritten list headed "Possible Targets" was recovered from his grandparents' address. Next to the heading was written: "False ID, diplomatic immunity, prepaid cards/ccs", presumably a reference to credit cards. The following targets were listed: "Serious and Organised Crime Agency, BBC, Army UK, Oxford Cambridge Uni, Kent Met Police, MI5 6, Fed Reserve, Channel 5 TV, CIA, NSA, FISA, Sony again LOL, major news organisations, HMBC". This was Count 8. Once again the appellant must have been granted bail.

20. Another week was to pass. At 8.34pm on 10February 2012 an internet order for a pizza delivery to the appellant's home address was placed through the website of Domino's Pizza. The pizza cost £15.99. Payment was made using the PayPal account of the complainant in Count 9, Neil Kerin. The appellant had earlier obtained Mr Kerin's computer password while working for him as a self-employed computer repairman. Mr Kerin's partner identified the pizza transaction whilst going through her e-mails on 11February 2012. Mr Kerin went to the delivery address at 8.00pm. A woman at that address denied any knowledge of the transaction, but Mr Kerin recognised the appellant when he came downstairs and he then challenged him. The appellant denied it but said Mr Kerin would be reimbursed.

21. A mobile telephone in the appellant's possession contained personal data belonging to Mr Kerin and his partner including: passwords, e-mail addresses, bank account numbers and credit card numbers. The computer equipment seized from the appellant's home address was analysed and found to contain references to SL1NK, files with titles such as "Bank Hack" containing personal information on Mr Bradley, and personal banking and credit card details for others. This was Count 9. His offending in relation to Mr Kerin was of course a gross breach of trust.

22. Finally, counts 12 and 13 concerned software called Jaindos, which is a program that can be used to instigate DOS attacks and Cyber Ghost, both of which were on the appellant's computer equipment.

23. The SL1NK user name was connected to a group called "Anonymous" which engaged in DOS attacks for political ends. Someone called "Superslink" had posted material relating to computer hacking on YouTube. A link led to a website with a screen-shot of Mr Bradley's online bank account and information on other accounts, credit cards and loans. SL1NK's exploits were referenced on other websites and a hacking forum.

24. The appellant is now 21 years of age. It is worth noting that on 6 August 2008 he was given a police reprimand for obtaining unauthorised access to computer material with intent to commit an offence. In May 2010 Canterbury College, where the appellant was a student, discovered the Firewall to the college computer had been compromised and forbidden websites accessed. This was linked to the appellant, who was subsequently suspended for a week and given a formal warning about computer misuse. The police were not involved, but these two incidents are an indication both of the appellant's determination and of what was to come.

25. The appellant has appeared before the courts on 14 previous occasions between 2010 and 2012. He had been given a range of non-custodial and some custodial sentences for offences including theft, burglary, possessing articles for use in fraud, failing to comply with previous orders and failing to comply with the sex offender notification requirements (to which he was subject following a police caution). On his last appearance on 16 May 2012 he was sentenced to 18 months' imprisonment for burglary and possessing articles for use in fraud. A point advanced on his behalf is that this offending pre-dated the last custodial sentence for unrelated dishonesty.

26. In interview the appellant said that he had used the name SL1NK but it was "just a pseudo name" and that many others used it. He denied carrying out the DOS attacks. That denial is undermined by his admissions.

27. The sentencing judge had before him a number of statements in connection with the appellant's offences. These dealt with the impact of the offending on the particular institutions, organisations and individuals targeted by him. They were from Jonathan Ashton of the University of Oxford; Jon Warbrick and Dr Ruth Charles of the University of Cambridge; PSE Maria Porter and Tim Thomas from the Kent Police; Mr Bradley and Mr Kerin.

28.

29. The two Universities wasted between them 19 working days in dealing with the attacks. Without introducing too much detail into this judgment, Mr Ashton from Oxford spoke of the disruption and the necessary steps taken once there had been a claim to have compromised the security of University data. He referred to the fact that unlike typical incidents, this had targeted Oxford University intended to cause disruption. A similar concern was expressed by Cambridge University.

30. Kent Police said that besides the inconvenience to internal and external users, these were the most serious attacks on their website that they had seen. They wasted 35man hours in dealing with them. 30 per cent of the security team was engaged in dealing with the attacks for nearly a week, and many other important tasks had to be postponed. We refer to what was said by PSEPorter about the potential consequences of a DOS attack on the Kent Police site: she said that should the site become unavailable at the time of a major incident it would have a profound impact on the force's ability quickly to update the public and provide important safety advice.

31. The consequences for the individual victims were, from their perspective, no less significant. Mr Bradley, who runs his own business, has had to set up new credit card and bank accounts, which took him about three weeks to resolve. During this time he was unable to use his accounts for spending or paying bills. He had to change all his passwords and obtain new (secure) e-mail addresses, for which he pays £200 per annum. He now pays for online identity protection, and has closed his Facebook account. He estimated that he had wasted 100 hours, and, as a company director, incurred costs making international calls to resolve the issue. He has reduced his internet use by about one third as a result. Nobody could deny that impact was serious.

32. Mr Kerin had to cancel his bank cards, and change his passwords which took about three weeks to resolve, causing obvious inconvenience. His PayPal account was also closed down, and it took six weeks to obtain a new account. He had to spend money on new antivirus and Firewall software for his computer. He is self-employed, and estimated it took about two days in all to rectify matters.

33. When passing sentence the judge said this was serious crime and absolutely nothing to be proud of. It corrupted the whole integrity of the system. Hacking into major universities and branches of the police caused a lot of extra work for a lot of people, quite apart from the fact that nobody could use the sites which they might have needed to access for good and proper purposes. Much like victims of burglary, individuals invaded in this way very seldom got over the invasion of their privacy. The sentence had to reflect society's distaste for this type of crime, which bordered on identity theft. It had to punish the appellant and send the clearest message to others that such activities would attract custodial sentences. His efforts were persistent, sophisticated, deliberate and planned. Though it did not add to his sentence, the list found at his home address showed that had he not been stopped he would have carried on committing this type of offence. The judge recognised that he pleaded guilty at the earliest opportunity and that he was now in work. He had tried to put his past behind him and turned gamekeeper. That mitigation did not carry sufficient weight to avert an immediate custodial sentence.

34. On behalf of the appellant, it was said by Mr Griffiths, both in writing and orally, that a sentence of two years' imprisonment where full credit was given for the appellant's guilty plea, thus representing a sentence of three years' imprisonment after a trial, was too long for a number of reasons. The appellant's motivation was youthful bravado to a like-minded community. Though it is acknowledged that the offences were planned and persistent, they were not financially motivated. The number of hours expended by the Universities in dealing with what had occurred resulted more from the exaggerated

claims which the appellant had made, rather than the nature of the attacks themselves. It was moreover to be borne in mind that the purpose of DOS attacks was not to cause permanent damage, nor to access or otherwise alter data, but to slow or halt the functionality of the websites for a period. As to the appellant's personal circumstances, the judge gave insufficient weight to the fact that he had served a custodial sentence since the commission of the offences, that he had already been sentenced for other offences arising from the same search and that he had made a positive impression on the Probation Service, as reflected in the Pre-Sentence report. Reference was also made to his good progress whilst on licence.

35. There are no sentencing guidelines relating to offences under the Act; for these offences, as for any other, the court must have regard to the purposes of sentencing set out in section 142(1) of the Criminal Justice Act 2003 (which, in addition to reform and rehabilitation of offenders, includes their punishment, the reduction of crime including by deterrence, the protection of the public and the making of reparation). Also of very great significance is the determination of the seriousness of the offences in accordance with section 143(1) of that Act, which points to the offender's culpability and the harm which the offence caused, was intended to be caused or which might reasonably have been caused.

36. In our judgment, these offences fall into the highest level of culpability: they were carefully planned offences which did and were intended to cause harm both to the individuals and organisations targeted.

37. It is particularly easy to demonstrate that harm in relation to the individuals. Mr Bradley and Mr Kerin sustained financial loss, and disruption to their private and business affairs; the invasive nature of the offences committed against them should not be minimised. Both were deeply affected by these offences, in the short term, and in their approach to computer and internet use in the longer term. We agree with the judge's characterisation of this aspect of the harm caused as akin to burglary or identity theft.

38. We have already mentioned the impact on the organisations concerned and the potential for harm. We should add that the seriousness of the criminality involved cannot necessarily be measured by the length of an attack or directly measurable financial consequences. The disabling of a website for even a short period may have far reaching consequences for the organisations concerned and for those who use the websites, including the general public. It is true that these were DOS attacks rather than DDOS attacks, but given the nature of the organisations concerned, we regard the issue of permanent, as opposed to temporary damage as a factor in mitigation of little consequence, as the evidence of PSE Porter demonstrates. Equally, it is of little moment to the victims of such crimes that the offender may be motivated by bravado within a community of like-minded souls, rather than by financial gain. The capacity for harm is very great either way. Actual damage or financial benefit would substantially aggravate an offence.

39. The wider implications of such crimes for society cannot be ignored. Offences such as these, have the potential to cause great damage to the community at large and the

public, as well as to the individuals more directly affected by them. Further, it is fortuitous and beyond the control of those who perpetrate them, whether they do so or not. This finds reflection in the maximum sentence which may be passed of tenyears' imprisonment for an offence contrary to section3(1) of the Act and of five years' imprisonment for an offence contrary to section 2(1) of the Act. These offences are comparatively easy to commit by those with the relevant expertise, they are increasingly prevalent, and the public is entitled to be protected from them. In our view, it is appropriate for sentences for offences such as these to involve a real element of deterrence. Those who commit them must expect to be punished accordingly.

40. Mr Griffiths places great reliance upon a decision on this court in R v Mangham [2012] EWCA Crim 297, where a sentence of eight months' imprisonment was reduced to one of four months' imprisonment for various "hacking" offences. The circumstances were that over a short period, the applicant, who suffered from a number of conditions including Asperger's Syndrome, hacked into Facebook's computers and stole intellectual property. There were a number of features of personal mitigation, described as extensive (including the fact, as here, of guilty pleas).

41. In the course of his judgment, Cranston J referred to a number of older decisions of this court. In Lindesay [2001] EWCA Crim 1720, [2002] 1 Cr App R(S) 370, a sentence of nine months' imprisonment was upheld upon an offender who, in revenge at his dismissal, gained entry to the computers of his former employers and deleted certain data to cause inconvenience. He pleaded guilty and had strong personal mitigation. In Valor [2003] EWCA Crim 2288, [2004] 1 Cr App R(S) 319, a two year sentence was upheld following guilty pleas for causing disruption on a grand scale by importing a number of viruses into the internet, detected in 42 countries and causing computers to be stopped some 27,000 times. The conduct was considered disruptive but not destructive. Two other viruses caused computers to stop and delete unsaved material: it may have affected 200-300 computers. Mr Griffiths makes the point that the circumstances of that case were far more serious than in the present appeal. Finally, in Baker [2011] EWCA Crim 928, a four month term was upheld on a person of good character, again a disgruntled ex-employee, who, on 20occasions, had gained unauthorised access to the Welsh Assembly computer system, reading sensitive e-mails.

42. At paragraph 19 in Mangham, the court identified a number of aggravating factors which may be relevant to sentence in cases of this nature. These included matters which are common to other offences: whether the offence is planned, whether the offending is persistent; the nature of the damage; the wider public interest; the effect on individual privacy; the effect on public confidence; the effect on commerciality and confidence; whether or not the information obtained is sold to others and the value of the intellectual property involved. Cranston J observed that the psychological profile of the offender deserved close attention.

43. Without seeking to undermine the mitigating features or the sentence in Mangham, in our judgment, it should not be considered a benchmark for such cases, which, in the ordinary course, are now likely to attract sentences that are very considerably longer: for offending of this scale, sentences will be measured in years rather than months. The

prevalence of computer crime, its potential to cause enormous damage, both to the credibility of IT systems and the way in which our society now operates, and the apparent ease with which hackers, from the confines of their own homes, can damage important public institutions, not to say individuals, cannot be understated. The fact that organisations are compelled to spend substantial sums combating this type of crime, whether committed for gain or out of bravado, and the potential impact on individuals such as those affected in this case only underlines the need for a deterrent sentence.

44. A number of aggravating features were present in this case.

i) There was a significant degree of sophisticated planning. The appellant attacked targets on more than one occasion and sent e-mails making claims about what he had done and threats about what he would do. He installed software on his computer for the purpose of orchestrating a DOS attack, namely Jaindos (count 12) and Cyber Ghost (count 13): these are programmes, as we have said, which provide misleading information about the IP address of the user and a cloak of anonymity for illegal acts. The list of possible targets found, three of which had already been attacked, provided further evidence of substantial and wide-ranging planning. He had encrypted his computer, thereby making full investigation more difficult.

ii) The appellant's conduct was persistent. The period covered by the offences spanned a period of nearly a year: from March 2011 to February 2012; it involved five different victims, two of whom were targeted twice. It involved offences committed whilst on bail.

iii) We have already dealt with the damage caused to those targeted by the appellant. The suggestion that the fullest weight should not be given to the time the organisations had to spend in dealing with the attacks perpetrated by the appellant because this resulted more from the content of his e-mails, rather than from the offences themselves, is in our judgment entirely misconceived. The content of those e-mails connoted a deliberate desire to maximise the damage and disruption which the appellant's offending would cause; and we regard the fact that they were sent as a seriously aggravating feature.

iv) As for the public interest, the websites of the Universities of Oxford and Cambridge and the Kent Police were attacked rendering them unusable. This had serious potential consequences for those organisations. The nature of the organisations the appellant selected really speaks for itself with regard to the potential for harm.

v) The invasion of the individual privacy of two of the victims itself cannot be underestimated. The appellant accessed the personal bank account of Mr Bradley and his personal and banking details were found on the appellant's computer. Mr Kerin's PayPal account was compromised; and used by the appellant for his own purposes. Mr Kerin's password had been obtained when the appellant held himself out as a computer repair man, and purported to repair his computer, thereby demonstrating a gross breach of trust. His password and personal details, as well as those of his girlfriend, were found on a mobile phone belonging to the appellant.

45. There were of course a number of mitigating features, which the judge evidently considered. These included the fact that, with the exception of the pizza, none had been commmitted for profit. We underline that had the attacks been motivated by benefit, longer sentences would have been inevitable. Furthermore, the appellant had served a sentence for other crime subsequent to the commission of these offences. On the other hand, there were substantial aggravating factors, including the appellant's poor criminal record.

46. In our view, these sentences were amply justified for the reasons given by the judge. This appeal against sentence is accordingly dismissed.