Neutral Citation Number: [2012] EWCA Crim 973

Case No: 201201041/A3

IN THE COURT OF APPEAL
CRIMINAL DIVISION

Royal Courts of Justice
Strand
London, WC2A 2LL

Date: Wednesday, 4th April 2012

B e f o r e:
LORD JUSTICE HOOPER
MR JUSTICE CRANSTON
HIS HONOUR JUDGE ROOK QC
(Sitting as a Judge of the CACD)

- -

R E G I N A

v

GLEN STEVEN MANGHAM

- -

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 7831 8838
(Official Shorthand Writers to the Court)

- -

Mr T Ventham appeared on behalf of the **Applicant**

Mr S Patel appeared on behalf of the **Crown**

- -

J U D G M E N T

1. MR JUSTICE CRANSTON: The Registrar has referred this application for leave to appeal against sentence directly to the court. It came before a different constitution of the court on 15th March, when the matter was adjourned so that the transcripts from the sentencing hearing could be obtained .

2. The applicant is 26 years old. On 13th December 2011, in the Crown Court at Southwark, he pleaded guilty to four counts on the indictment: counts 1 to 3, securing unauthorised access to computer material with intent, contrary to the Computer Misuse Act 1990, section 1; and count 4, the unauthorised modification of computer material, contrary to section 3 of that Act. He was sentenced by His Honour Judge McCreath on 17th February this year to 8 months' imprisonment concurrent on each count. A separate count, count 5, making and supplying or obtaining articles for use, an offence under section 1 or 3 of the 1990 Act, was left on the file in the usual terms.

3. In addition to these sentences the judge imposed a serious crime prevention order under the Serious Crime Act 2007. The duration of that order is 5 years, beginning with the date of release from either prison or sentencing. Unfortunately that means that the start date is unclear. Pursuant to the order the applicant can own and use only one personal computer with Internet access. He also has to give notification to the authorities about the use of a computer in the course of employment and is forbidden from using encryption software and from using data wiping software on his personal computer. He is also prevented from deleting any log or history of use and is not permitted to allow another person to use his personal computer. In addition, there is a restriction on the email accounts which he is able to employ: he can have only have two email accounts and they have to be with UK based service providers. There are certain notification obligations under the order. The application in relation to the order comes to us pursuant to the Serious Crime Act 2007 (Appeals under Section 24 Order 2008, 2008 SI 1863.

4. The background is this. Between April and May 2011 the applicant hacked into Facebook's computers. He was able to infiltrate a Facebook employee's email account and then stole intellectual property which he stored on a portable hard drive . In outline the method he used was as follows. He first accessed Facebook's protected systems including a server known as the Puzzle server. Puzzles are placed there by Facebook as a series of tests for prospective employees. The applicant exploited vulnerabilities within the Puzzle server and then infiltrated the private side of the server to download a number of programmes which modified their functionality. That enabled a continued breach of security by providing ongoing access. He then used that to gain unauthorised access to the Mailman server, which handles Facebook's internal and external emails. That contained email archives, a selection of which he copied. The next step was that he created a programme which utilised the compromised electronic identity of a Facebook employee to gain access to the Phabricator server. The upshot was that he was able to access the Facebook source code. That is the unique software which gives Facebook its functionality. As we have said he copied part of that onto his hard drive.

5. In a statement before the judge, Facebook estimated that they had incurred direct costs of some $200,000 in responding to the incident. That included the time dedicated by

Facebook professionals to investigate, access and remediate the damage done and also included the professional fees of outside experts. The statement by Facebook continued:

> "The unauthorised access to Facebook's computer system resulted in the compromise of sensitive and confidential corporate information and intellectual property. No personal use of data or corporate financial data was compromised as a result of the applicant's actions. Facebook appreciates the outstanding efforts made by the Metropolitan Police which led to the swift recovery and return of all compromised material to Facebook without any direct financial loss."

6. The judge was also given a letter form the Department of Justice, which explained that it would forgo prosecution of the applicant in favour of prosecution by the authorities here. The letter said that the FBI and the United States' Department of Justice had expended extraordinary resources to identify the applicant. Three special agents had worked full-time on the case for about three weeks. The FBI had incurred further expense by sending two agents to this country.

7. At the sentencing hearing the judge heard submissions from both Mr Ventham, representing the applicant, and Mr Patel, for the Crown. The judge was told that the applicant had on a previous occasion exposed vulnerabilities at Yahoo. As a result of that Yahoo had contacted him to learn about the defects in their system and had, in fact, paid him a small amount to assist. In addition, the judge was told that following this incident Facebook had paid some $40,000 over a 3-week period to hackers to help it to identify flaws in its system, under a so-called "bug bounty" initiative.

8. The judge heard evidence from the applicant. In the course of that the applicant was asked about his motivation, on this occasion, as compared with what he did when he exposed the vulnerabilities in Yahoo. It was put to him that whereas he had relatively quickly notified Yahoo of the vulnerabilities he had exposed, he had not done that with Facebook. Not until he had suspected that Facebook had identified him as a hacker that he had then began to cover his tracks. It was put to him that he was not the ethical hacker he had presented himself to be.

9. Before the judge were two reports. One was a report from a chartered psychologist. It stated that the applicant probably suffered from a number of conditions including Asperger's syndrome, personality disorder, social phobia and possibly major depression. The psychologist concluded that he would benefit from therapy to help him to minimise the impact of his problems on his every day life. The psychologist recorded that the applicant had said to him that he had set himself the goal to prove that he could do what he did.

10. As well there was a pre-sentence report. In the course of that report the probation officer recorded that the applicant had told him that his sole intention had been to try to seek out a weakness in the Facebook system and that he intended to notify that to Facebook. The applicant offered no excuses to the probation officer, who assessed him as being honest and open about what he had done. The applicant regarded what

he had done as an intellectual challenge. The probation officer concluded that the likelihood of reconviction was low and that there was a low risk of harm to others in the future.

11. In sentencing the applicant the judge said that he would take into account that the applicant was of good character, that he was relatively young in years but possibly emotionally younger, and that he had a psychological and a personal make up which had led to the behaviour. The judge acknowledged that the applicant had never intended to pass any information that he had obtained to anyone else and in fact never did so. The judge also recognised that the applicant had never intended to make any financial gain for himself. In terms of the impact of the offending, the judge explained that in his view this was not harmless experimentation, that the applicant had accessed the very heart of an international business of a massive size, had acquired fundamental knowledge of its internal systems and had put the entire operation of that business at potential risk. The applicant had created immense difficulties for Facebook and for those who investigated what he had done. There was the cost, the $200,000 to investigate and remedy what the applicant had done. The judge characterised the behaviour as persistent and sophisticated.

12. As to motive, the judge said that having heard the applicant's evidence he was satisfied that the applicant had not offended in order to inform Facebook what he had discovered, as earlier with Yahoo. He was not an ethical hacker. Rather that was a justification after the event for what the applicant had done. The judge underlined the potential effect, as he saw it, of the offending. In particular, he referred to the concern on the part of Facebook as to what might have happened.

13. In relation to the serious crime prevention order, the judge concluded that this was a serious crime and that there was a risk of the applicant's continuing to commit offences.

14. Before us today Mr Ventham contends that while a custodial sentence could be justified the sentence was manifestly excessive when taking account of the whole range of factors, including the lengthy interview with the police. There he had told what one officer said was the complete and utter truth. In addition, Mr Ventham emphasised the extensive personal mitigation of the applicant. There were also the fact that he has had to abandon an Open University course.

15. As to the serious crime prevention order, Mr Ventham's contention is that there is a low risk of the applicant re-offending. He is now *persona non grata* on the Internet which made future behaviour of this character even less likely.

16. In his very helpful written submissions, Mr Patel for the Crown has drawn attention to a number of authorities regarding offences under the Computer Misuse Act 1990. The first is R v Lindesay [2001] EWCA Crim 1720, [2002] 1 Cr App R(S) 370, where this court upheld a sentence of 9 months' imprisonment: that was imposed on an offender who had, in revenge for his dismissal, gained unauthorised entry into three websites and deleted certain data to cause inconvenience. There was no damage to the software or direct revenue loss. The appellant had pleaded guilty and had strong personal mitigation. This court regarded the use of confidential passwords, the inconvenience

to the company and its clients, the appellant's motive and the breach of trust as justifying the sentence the judge imposed.

17. In R v Vallor [2003] EWCA Crim 2288, [2004] 1 Cr App R(S) 319, the appellant unsuccessfully appealed a sentence of 2 years' imprisonment. He had imported a number of viruses into the Internet. The first was detected in 42 different countries and apparently led to computers stopping some 27,000 times. The court regarded that behaviour as disruptive, albeit not destructive. The second and third viruses were worms in email messages, which caused computers to stop and delete unsaved material. The damage was unknown but may have affected material on 200 to 300 computers. This court said the offending was planned and calculated to cause disruption on a grand scale.

18. In the third case, R v Baker [2011] EWCA Crim 928, the sentence of 4 months' imprisonment on a person of good character was upheld. On 20 occasions, over a week in June, the appellant had used a remote dial-up connection from his home computer to gain unauthorised access to the Welsh Assembly computer system. The appellant had read a number of sensitive emails up to the restricted level. He had been dismissed and said he was searching for material relevant to that.

19. From these authorities we would identify a number of aggravating factors which will bear on sentence in this type of case: firstly, whether the offence is planned and persistent and then the nature of the damage caused to the system itself and to the wider public interest such as national security, individual privacy, public confidence and commercial confidentiality. The other side of the coin to the damage caused will be the cost of remediation, although we do not regard that as a determining factor. Next, motive and benefit are also relevant. Revenge, which was a feature in Lindesay and Baker, is a serious aggravating factor. Further, the courts are likely to take a very dim view where a hacker attempts to reap financial benefit by the sale of information which has been accessed. Whether or not the information is passed onto others is another factor to be taken into account. The value of the intellectual property involved may also be relevant to sentencing. Among the mitigating factors the psychological profile of an offender will deserve close attention.

20. As to the imposition of a serious crime prevention order, the offence must be a serious offence, either specified in the schedule to the Serious Crime Act of 2007, or as section 2(2)(b) provides, one which "in the particular circumstances of the case, the court considers to be sufficiently serious to be treated for the purposes of the application or matter as if it were so specified." The leading authorities are R v Batcherlor [2010] EWCA Crim 1025 and R v Hancox [2010] EWCA Crim 102.

21. In Hancox the court said that there must be reasonable grounds for believing that an order will protect the public by preventing, restricting, or disrupting involvement by the defendant in serious crimes, as required by section 19(2) of the Act. That means that there has to be reasonable grounds to believe that there is a real or significant risk, not a bare possibility, that the offender will commit further serious offences. In addition, the court underlined the importance of proportionality and referred to Article 8 of the European Convention on Human Rights. The court said that an order should not be

imposed because it was thought that a defendant deserved it; an order was not designed to punish but rather was preventive in character.

22. In our view, the judge faced a difficult sentencing exercise. He took into account all the aggravating and mitigating factors we have mentioned. He rightly highlighted the persistence, sophistication and deliberateness with which the applicant mounted his attack. Having heard the applicant give evidence, the judge was entitled to conclude that his motive was not to inform Facebook of the defects in their system, by contrast with what he had done with Yahoo, but more to prove that he could beat the Facebook system**.** The judge also alluded to the strong personal mitigation which the applicant had.

23. Standing back, however, we have concluded that the balance of the aggravating and mitigating factors is such that the more appropriate sentence would have been 6 months' imprisonment, reduced to 4 months in the light of the applicant's plea and personal mitigation.in particular, we underline the points which the judge made at the very outset of his sentencing remarks, that the information hacked had not been passed on to anyone and that there was no financial gain involved. The judge was correct, in our view, to identify the damage to Facebook, but it may be that he gave too much emphasis to the potential damage. It will be recalled that Facebook acknowledged that although the applicant's activity resulted in the compromise of sensitive and confidential corporate information all the compromised material was swiftly recovered and Facebook did not suffer any financial loss, apart from the costs of investigation.

24. Moreover, in our view the serious crime prevention order cannot stand. The judge assessed the applicant as posing a future risk, contrary to the assessment of the probation officer. He was entitled to do that. But we are not persuaded that the proportionality of the order was properly assessed in all the circumstances of the applicant's case.

25. That being the case, we give leave, allow the appeal, and substitute 4 months for the 8 months on each of the counts. The sentences will run concurrently in each case. We quash the serious crime prevention order.