Neutral Citation Number: [2019] EWCA Crim 95

2018/04878/A2

IN THE COURT OF APPEAL

CRIMINAL DIVISION

Royal Courts of Justice

The Strand

London

WC2A 2LL

Wednesday 30th January 2019

B e f o r e:

LORD JUSTICE FLAUX

MR JUSTICE SWEENEY

and

MR JUSTICE SOOLE

R E G I N A

- v -

CONNOR DOUGLAS ALLSOPP

Computer Aided Transcript of Epiq Europe Ltd, 165 Fleet Street, London EC4A 2DY

Tel No: 020 7404 1400; Email: rcj@epiqglobal.co.uk (Official Shorthand Writers to the Court)

Mr A Bell appeared on behalf of the Appellant

Mr P Ratliffappeared on behalf of the Crown

J U D G M E N T

(Approved)

Wednesday 30th January 2019

LORD JUSTICE FLAUX:

1. This case concerns the hacking in October 2015 of the computer systems of the mobile phone company, TalkTalk.

2. On 30th March 2017, at the Central Criminal Court before His Honour Judge Topolski QC, the appellant, who was born on 4th March 1997 and who is therefore just short of 22 years of age, pleaded guilty on re-arraignment to count 6 (supplying

an article for use in fraud, contrary to section 7(1) of the Fraud Act 2006), and to count 8 (supplying articles for use in an offence under sections 1, 3 or 3ZA of the Computer Misuse Act 1990).

3. His co-accused, Matthew Hanley, also pleaded guilty on re-arraignment to count 3 (causing a computer to perform a function to secure or to enable unauthorised access to a program or data, contrary to section 1(1) of the 1990 Act); count 4 (supplying articles for use in an offence under sections 1, 3 or 3ZA of the 1990 Act); count 5 (supplying an article for use in fraud); and count 9 (obtaining articles for use in an offence under sections 1, 3 or 3ZA of the 1990 Act).

4. It was decided by the court that the two defendants should not be sentenced straightaway but that sentence should await the outcome of the forthcoming trial of another man, Daniel Kelly, who was charged with a number of offences relating to the TalkTalk hacking attack, including blackmail. In the event, the trial of Kelly having been adjourned on a number of occasions, the court proceeded to sentence the appellant and Hanley.

5. On 19th November 2018, they were sentenced at the Central Criminal Court by Her Honour Judge Dhir QC. The appellant was sentenced to eight months' imprisonment on count 6 and to a concurrent term of seven months' imprisonment on count 8. Hanley received an overall sentence of twelve months' imprisonment.

6. The appellant now appeals against sentence with the leave of the single judge.

7. The relevant background to computer hacking and the specific hacking attack on TalkTalk is as follows. Computer hackers have skills in coding or programming computer tools in order to exploit vulnerabilities in a specific target's device or network in order to access secured information. Once access is gained, hackers often alter the system or security features of the device or network. In a practice called "doxing", a hacker may take data and publish it or blackmail the legitimate owner with the threat of publication of the data. Hackers may also "exfiltrate" the data to find other potential "doxing" targets, or may "dump" (i.e. duplicate and take) the accessed database.

8. On 21st October 2015, TalkTalk became aware of potential latency issues on its website from a cyber attack which had led to its data being unlawfully accessed. Holding pages were placed on the website and the email exchange. BAE Systems

were employed to investigate the attack.

9. The Chief Executive Officer of TalkTalk at the time, Dido Harding, was subjected to repeated attempts to blackmail her by demands for payment of Bitcoins in return for the stolen data. The police and the National Crime Agency were informed of the attack. It was not suggested by the prosecution that either the appellant or Hanley was involved in the blackmail, although the latter is far from an unusual example of what often follows hacking activity.

10. At the time of the offending, the appellant was aged 18 and Hanley was aged 20. They both lived in Tamworth and knew each other. Hanley was a dedicated computer hacker. On 24th October 2015, no doubt concerned that the police were investigating, he wiped his computer so that the police were unable to reconstruct its contents, but they were able to piece together his involvement from a large number of Skype conversations that he had had. His plea of guilty to count 3 involved an admission that he was involved in hacking the TalkTalk database between 18th and 22nd October 2015 and in obtaining stolen data. Count 4 related to his supply of the database scheme for the website to a man named Liam Fields, whom he knew was involved in computer misuse.

11. Count 5 related to Hanley's supply to the appellant on 23rd October 2015 of a computer file containing the personal and financial details of TalkTalk customers. In his police interview, the appellant admitted that he had asked Hanley for the TalkTalk database. In a Skype conversation, Hanley told the appellant to move to an off-the-record platform to continue the discussion about what he had done. There was evidently then a conversation about the hacking of the data and a file exchange since, in another Skype conversation 90 minutes later, Hanley told the appellant "Be careful with that dump. Don't sell unless £1,000 plus and you didn't get it from me". The "dump" or computer file given to the appellant was the personal and financial details of 8,000 TalkTalk customers.

12. On the same day, 23rd October 2015, the appellant supplied that computer file to an online user called "Reign", knowing that it was for use in connection with fraud. It is clear that the appellant knew that he had obtained the file illegally from Hanley and that Hanley and "Reign" were concerned with fraud and hacking. This offending was count 6, to which the appellant pleaded guilty. It appears that, in exchange for the TalkTalk data, "Reign" originally agreed to provide a list of credit cards, but in fact supplied a series of computer files with personal data and website details and passwords, including for NASA, which could be used in further hacking, but which

ultimately proved next to worthless.

13. In a Skype conversation on 28th October 2015, Hanley asked the appellant for credit cards, thinking that this was what the appellant had obtained in exchange for the TalkTalk data. In fact, between 23rd and 29th October 2015, the appellant supplied to Hanley the computer files that he had obtained from "Reign". As the judge said in her sentencing remarks, those files included a file which contained 77 websites, with additional syntax information at the end of each address and a text file containing 492,000 odd unique email addresses, with passwords in plain text and a hash diary for the passwords. This offending was count 8, to which the appellant pleaded guilty.

14. Count 9 is the obverse of count 8 that is the offending by Hanley in obtaining those computer files from the appellant, together with other files that Hanley obtained from other computer hackers.

15. Hanley was arrested at his home address on 1st November 2015 and the appellant was arrested some time later, on 20th April 2016. On arrest, he claimed that his computer had been destroyed in a house fire. As with Hanley, the police were able to piece together his involvement from Skype conversations. He also made significant admissions in his interviews with the police.

16. The appellant had no previous convictions, but had a caution from 2013 for the possession of an offensive weapon in a public place. Hanley had no previous convictions, but a caution from 2016 for possession of cannabis.

17. The judge had the benefit of pre-sentence reports for both the appellant and Hanley. The appellant gave a full account to the author of the report in his interview. At the time, he acted without any regard for the impact of his behaviour on the victims of the hacking. The author took the view that, although the appellant now regretted his involvement, he did not grasp the "enormous negative reputation and significant financial impact" on TalkTalk. He was assessed as a low risk of re-offending and a low risk of harm. The author concluded that he was impressionable and immature, in awe of Hanley's computer hacking skills and wanted to emulate him.

18. The report in relation to Hanley noted that he accepted his involvement, as set out in his basis of plea. He denied that his offending was financially motivated and said that any comments about demanding money were to impress his friends. He

presented as socially isolated and had a long history of anxiety and low self-esteem. He was able to recognise the distress and inconvenience caused to TalkTalk customers. He was assessed as having a 39 per cent likelihood of re-offending within a two year period. He was also assessed as a low risk of harm to others. Given his history of anxiety and depression, self-harm and suicidal ideation, the probation officer took the view that he would be vulnerable within a custodial environment.

19. There was also a psychologist's report in relation to Hanley, dated December 2016, which recommended that he be viewed as meeting the criteria for a social anxiety disorder. It concluded that a custodial environment was likely significantly to exacerbate his anxiety and it was recommended that Hanley be considered for a non-custodial sentence.

20. In her sentencing remarks, the judge noted that both defendants were involved in a significant, sophisticated, planned attack on the computer systems used by TalkTalk. They had not exposed the vulnerabilities in the company's systems. Others had started the attack, but at different times they both joined in. The attack led the two, along with others, to gain access to TalkTalk's confidential client information. The estimated loss to TalkTalk was £77 million. Confidential information was stolen and passed to others, causing misery and distress to thousands of customers.

21. The judge then set out the facts of the offending in considerable detail, which it is not necessary to repeat. She said that there are no sentencing guidelines for offences under the 1990 Act. She had been referred to two authorities: *R v Martin [2013] EWCA Crim 1420* and *R v Mudd [2017] EWCA Crim 1395* . The judge noted that in *Martin* , Leveson LJ said that these offences fell into the highest level of culpability. This was because of the financial loss and destruction to private and business affairs. She quoted what Leveson LJ had said at paragraphs 38 and 39 as follows:

> "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 …"

22. The judge noted that *Mudd* involved more serious offending. The appellant in that case, who was aged 20, had no serious convictions and was diagnosed with Asperger's syndrome. The offending had occurred when he was aged 16 and there was substantial mitigation. The court had reduced the sentenced from six years for an adult to 24 months. The Court of Appeal further reduced it to 21 months, but concluded that immediate custody was appropriate and said that it was important that the courts sent the clear message that cyber crime on this scale was not a game but would be taken very seriously by the courts and punished accordingly.

23. In relation to counts 5 and 6, there were sentencing guidelines for offences under section 7 of the Fraud Act in the Fraud, Bribery and Money Laundering guideline, to which the judge was referred. The judge considered that in the case of both defendants, the offending fell towards the lower end of medium culpability, and it was accepted that it was in the category of greater harm. The starting point was two years six months' custody, and the range eighteen months to five years. The court took a starting point for Hanley of two years six months. Then, taking account of his age at the time, his lack of previous convictions, the relatively short period over which the offending occurred, the reports about him and his basis of plea, together with the absence of further offending, reduced that starting point to fifteen months. The court then gave him credit for his guilty plea of 20 per cent and on count 5 passed a sentence of twelve months' immediate custody, with concurrent shorter sentences of nine months on the other counts.

24. In relation to the appellant, the judge said that his involvement was less than that of Hanley. The court took account of everything said on his behalf and the pre-sentence report. He had been 18 years old at the time and immature. He had no previous convictions. The considerable period of time between the offending and sentence was not the appellant's fault. The mitigating factors reduced the starting point from 20 months to twelve months. The judge gave the appellant a full one-third credit due to his considerable admissions in police interviews. On count 6, the sentence was eight months' imprisonment, and on count 8, seven months' imprisonment concurrent. The judge concluded that she could not suspend the sentence in

view of the seriousness of the offending.

25. On behalf of the appellant, Mr Bell raises three grounds of appeal. First, he submits that the judge overstated the appellant's involvement in the hacking of the TalkTalk database and therefore took too high a starting point, which should have been between twelve and eighteen months, not twenty months. He submitted that the judge had mistakenly assumed that the appellant had taken part in the original attack.

26. We agree that if the judge's statement at the outset of her sentencing remarks that the appellant was involved in a "significant, sophisticated, systematic, planned attack" were taken in isolation, it might suggest that she had proceeded on the assumption that the appellant was involved to a greater extent than he was. However, when the judge's careful consideration of the facts is taken into account, it is quite clear that there is no question of her having misunderstood the extent of the appellant's involvement.

27. The second ground is closely related to the first. It is said that the judge did not distinguish sufficiently between the culpability of the two co-defendants. Hanley was a dedicated hacker, who had early access to the TalkTalk "dump", whereas the appellant was only given access to part of it. While Hanley suggested that it was worth in excess of £1,000, the appellant had failed to achieve that, but only something of minimal value which he did not use himself. It was submitted that his culpability was less than that of Hanley and that the one-third less starting point of 20 months, rather than 30 months in the case of Hanley, did not reflect their respective culpability.

28. Attractively though these submissions were advanced, we cannot agree with them. The judge was right to put the appellant's offending towards the bottom end of the medium culpability category in the guideline and her starting point of 20 months (slightly above the bottom of the sentencing range) faithfully reflected that. Furthermore, contrary to the views expressed by the single judge, the judge took full account of the appellant's youth and immaturity and of the delay in sentencing. In reducing the starting point from 20 months to twelve months, then in giving the appellant a full one-third credit when he had not pleaded guilty until four months after the plea and case management hearing and four months before trial, the judge might be thought to have been somewhat generous. We do not consider that the sentence passed can be said to be excessive, or that the appellant has any legitimate complaint about alleged disparity of sentence between himself and Hanley.

29. The final ground of appeal is that the judge erred in not suspending the sentence. Particular emphasis has been placed by Mr Bell in his submissions to the court this morning on two matters: first, the considerable period of delay between the plea of guilty and sentence, during the course of which the prospect of a custodial sentence was hanging over the appellant and his family; and secondly, that since he was sentenced the appellant has been incarcerated in Belmarsh Prison for 20 weeks, which Mr Bell submits is a sufficient sentence to reflect the seriousness of the offending.

30. Attractively though these submissions were advanced, we cannot agree with them. The judge took account of the delay in reducing the amount of the starting point and the issue in relation to whether or not she should have suspended the sentence is not one which is related to the delay, but is related to the seriousness of the offending. Although the appellant may not have initiated the cyber attack, he took advantage of it. It was accepted on his behalf that this was a case of greater harm within the guideline, since the offending facilitated fraudulent acts which could have affected a large number of victims. We consider that, applying the analysis of this court in both *Martin* and *Mudd* , which the judge helpfully referred to in her sentencing remarks, only an immediate custodial sentence was appropriate.

31. The only amendment we would make to the sentences passed is that they should have been sentences of detention in a young offender institution, rather than imprisonment, because at the date of his conviction on 30th March 2017 the appellant was under 21.

33. Apart from that technical defect in the sentencing, which we correct, this appeal is dismissed.
