APPEAL COURT, HIGH COURT OF JUSTICIARY

[2023] HCJAC 51
HCA/2023/350/XC

Lady Paton
Lord Doherty
Lord Matthews

OPINION OF THE COURT

delivered by LORD DOHERTY

in

the Appeal under Section 74(1) of the Criminal Procedure (Scotland) Act 1995

by

AARON CAMPBELL LIND

Appellant

against

HIS MAJESTY'S ADVOCATE

Respondent

Appellant: Gravelle (sol adv); Beltrami & Co, Solicitors
Respondent: Campbell AD; Crown Agent

23 October 2023

Introduction

[1] The appellant is now aged 20. He was prosecuted on indictment in the Sheriff Court at Glasgow, charged with having possession of indecent photographs or pseudo-photographs of children contrary to section 52A(1) of the Civic Government (Scotland) Act 1982, and with taking or permitting to be taken or making such photographs

contrary to section 52(1)(a) of that Act. He lodged a preliminary issue minute objecting to the admissibility of indecent photographs of children which the police had recovered from a cloud storage account. Following an evidential hearing the sheriff repelled the minute. The appellant now appeals in terms of section 74(1) of the 1995 Act against that decision.

The evidential hearing and the sheriff's decision

[2] On 11 February 2021 the Procurator Fiscal, Glasgow presented a petition seeking a search warrant. The petition was in the following terms:

> "From information received by the Petitioner it appears that there are reasonable grounds for suspecting that offences contrary to Sections 52 and 52A of the Civic Government (Scotland) Act 1982 have been committed and are being committed at the premises at [the appellant's home address]. That the Petitioner is under necessity of investigating said offences and that there are reasonable grounds for believing that evidence material to the investigation of said offences is present in the said premises.
>
> The Petitioner therefore craves the Court to grant Warrant to any Officers of the Police Service of Scotland … to enter said premises at [the address]… and to search said premises, and ground pertaining thereto, any outbuildings relative thereto and to secure and take possession of mobile phones, tablets, computers, laptops, central processing units, external and internal drives, external storage equipment or media, terminals or video display units together with peripheral equipment such as keyboards, printers, modems or scanners, any computer or data processing software or data including but not limited to hard disks, floppy disks, video cassette tapes, other permanent or transient storage devices and other data storage devices, and other relevant documentation and any other articles which such officers have reason to believe are evidence material to the investigation of said crime and to examine any aforesaid devices or any other things whatsoever found in said premises which they have reasonable cause to believe may produce evidence material to said investigation and any card, document or other material which there is reasonable cause to believe may provide evidence material to said investigation and for that purpose to make patent all shut and lockfast places in said premises …"

On the same day Sheriff Considine granted the warrant as craved.

[3] On 5 March 2021 police officers attended the premises to conduct a search in terms of the search warrant. Among the items seized were a laptop and an iPhone. The appellant gave the officers the password to the iPhone.

[4] Thereafter, police cybercrime officers examined the items seized. 100 still images of child sexual exploitation and abuse were recovered from deleted space on the laptop, of which 11 were Category A, 9 were Category B, and 80 were Category C. Log in credentials - a user name and a password - for an account with the website Mega.NZ were stored in the settings on the iPhone.

[5] Mega.NZ is a website which provides a cloud storage and file hosting service offered by Mega Ltd (an Auckland-based company). Cloud storage involves making data storage space available to users on a remote server. One of the advantages is that users do not require to use up data storage capacity on the hard drive of their phones or other devices. Where a user has an account with Mega.NZ they may access the account by using a web browser and logging in using their log in credentials. That can be done from any device capable of accessing the internet. Another means of access is available to the user where they have installed the Mega.NZ application ("the app") on their smart phone. In that case the app is a portal to the data stored by the user in their account. Access via the app is direct. It does not require the use of a web browser and log in credentials. The app is installed on the phone, but the data in the account is in cloud storage on a remote server.

[6] When the cybercrime officers examined the iPhone the app was not installed on it. One of the officers sought advice from a superior as to whether the search warrant authorised him to use a web browser to access Mega.NZ using the log in credentials found on the iPhone. He was advised that it did. The officer accessed the Mega.NZ website using a web browser on a police device. He logged in using the recovered log in credentials. That

took him to an account named "Aaron Lind". Within the account images of the appellant were stored in a folder named "camera uploads". Another folder contained 123 images of child sexual exploitation and abuse, 4 of which were still and 119 of which were moving. 53 of the images were Category A, 38 were Category B, and 32 were Category C. The images could be accessed from any device capable of accessing the internet by using the log in credentials. Although those credentials had been stored automatically on the iPhone, it was not possible to say whether the iPhone had been used to access the account.

The submissions to the sheriff and his decision

[7] The evidential hearing took place before Sheriff McCormick. The Crown submitted that the recovery of the iPhone and its interrogation had been authorised by the search warrant. The log in credentials for the Mega.NZ account had been lawfully recovered from the iPhone and they had been used to obtain access to the data stored in the folders in the "Aaron Lind" account. The search of that data had been authorised by the search warrant. Alternatively, if the search of the folders in the "Aaron Lind" account had been irregular, the irregularity should be excused. The officer had acted in good faith, believing that the warrant authorised the search. He had obtained advice to that effect from a superior. The evidence recovered was important evidence of serious criminal offending.

[8] The defence submitted that the recovery of the images had not been authorised by the warrant. They had not been at the premises or on any device found at the premises. Moreover, the app had not been installed on the iPhone. Search warrants should be strictly construed (Renton & Brown, *Criminal Procedure*, 5.09). Reference was also made to *JL & EL* v *HM Advocate* [2014] HCJAC 35, in particular to paras [10] to [12]. Having found the name of the website and the log in credentials stored on the iPhone, the police ought to have sought

a further warrant if they wished to use the credentials to log in to and search the account on Mega.NZ to which they related. The irregularity of the search ought not to be excused; cf *McAvoy* v *Jessop* 1988 SCCR 172.

[9] The sheriff held that the search of the Mega.NZ account had not been irregular. In his opinion it had been authorised by the terms of the search warrant, which authorised officers to:

> "take possession of mobile phones, tablets, computers, laptops, central processing units, external and internal drives, external storage equipment or media terminals…"
>
> and
>
> "data processing software or data including but not limited to hard discs, floppy discs, video cassette tapes or other permanent or transient storage devices and other storage devices…"
>
> (the sheriff's emphasis), and to
>
> "examine any aforesaid devices or any other things whatsoever found in said premises which they have reasonable cause to believe may produce evidence material to said investigation and any card, document or other material which there is reasonable cause to believe may provide evidence material to said investigation…".

The sheriff noted that while the app was not installed on the iPhone, the iPhone had stored within it the name of the website and the account log in credentials. Using that information the appellant could access the data in the folders by using a web browser installed on his iPhone, or indeed by using a web browser on any device. In his report the sheriff explained:

> "[51] I therefore concluded that standing the wording of the warrant the limit (reach or extent) of the warrant had not been breached. The search was lawful and included the premises, the phone and the information within it."

He reasoned that although neither the images objected to nor the app were on the iPhone, the means of accessing them were. He continued:

> "[55] The solicitor for the appellant had referred to a situation where a key might be found on premises searched but the key itself was for a safety deposit box at a

> bank or a safe located elsewhere. The finding of the key would not entitle police officers to go to the bank and open the safe. A further warrant would be needed.
>
> [56] I did not find that analogy particularly helpful. I say this because, to continue the analogy, the appellant would not need to take the key to the bank. He could access his account information via his phone. In the same way, the court must recognise advances in technology whereby an appellant with the site details, the user name and the password stored on his phone (capable of browsing the internet) could use that phone to access the images uploaded and stored elsewhere. The warrant was widely framed."

The sheriff did not go on to consider whether the irregularity should be excused if he was wrong about the scope of the warrant. He granted leave to appeal.

Submissions for the appellant

[10] Mr Gravelle submitted that the appeal should be allowed. The search warrant authorised the search of the premises and the seizure of items on the premises. It did not authorise the search of the data in the Mega.NZ account or the seizure of the images. The Mega.NZ account provided access to a cloud storage and file hosting service. The relevant data was not stored or in use on the iPhone. It was not situated on the premises or on any item within the premises. The use of the account credentials to access an account that was neither present nor in use on the iPhone exceeded the limits of the search warrant. Here, the warrant authorised the seizing of the iPhone and data or data processing software found on it. The log in credentials and the reference to the Mega.NZ website were data on the iPhone. A Mega.NZ app might be data processing software, but there was no such app on the iPhone. More importantly the data in the folders in the account was not on the iPhone or anywhere else at the premises. Accordingly the search of the account and the seizure of the images were unlawful. The irregularity should not be excused. It was not reasonably open to the searching officer to take the view that the search of the account and the seizure of the

images were authorised by the warrant (*McAvoy* v *Jessop* 1988 SCCR 172). The fact that it was thought appropriate to check with a superior officer was indicative of the fact that the cybercrime officer had some doubt whether the warrant authorised accessing and searching the account. There had been no urgency justifying dispensing with the obtaining of an appropriate warrant (*Lawrie* v *Muir* 1950 JC 19).

Submissions for the respondent

[11] The appeal should be refused. It was accepted that the police required authority to search the appellant's account and seize the stored images. However, the scope of the search warrant was wide. It allowed the searching officers to secure and take possession of "data processing software or data". That authorised what had been done here.

[12] Mega.NZ provide a cloud storage and file hosting service. It is a mode of remote data storage in which data is stored in a remote server. It is an electronic repository for data. Such remote storage had been rightly described as "practically ubiquitous" by 2017 (see the uncontentious expert evidence referred to in *R* v *Parsons* [2018] 1 WLR 2409, at paragraphs 20 to 23). In 2023 cloud storage was even more widely used. The law had to adapt to advances in technology and the resultant changes in the way people stored data. Drawing analogies with physical repositories elsewhere was not helpful. The crucial distinction here was that the remote data could be accessed instantaneously using any web browser and the log in credentials stored on the iPhone. That could be done using the iPhone. It would obstruct the investigation of crime if the investigating authority were required to obtain a further warrant to use log in credentials to search remote data storage. Such a warrant might be difficult to obtain. Where, as here, the remote server was situated abroad, issues of whether the court had jurisdiction to grant the further warrant might arise.

There was also a risk that in the intervening period between finding the log in credentials and obtaining a further warrant the data on the remote server might be deleted.

[13] If the search of the "Aaron Lind" account had not been authorised by the warrant, the irregularity should be excused. The officer had acted in good faith. He had clarified with a senior officer that he was indeed authorised to conduct the search. The terms of the warrant were wide and it had not been unreasonable for the officer to conclude that the search was within its scope. The search carried out had been a specific one. The offences being investigated were extremely serious and the data recovered was very important evidence.

Decision and reasons

[14] We begin by observing that the passage in Renton & Brown at paragraph 5.09 does not vouch the appellant's proposition that search warrants require to be "strictly" construed. That proposition is not an accurate statement of the law. A search warrant does not fall to be construed either strictly or liberally. Rather, generally, the proper approach is to give the words used in the warrant their ordinary and natural meaning.

[15] Of course, a wide or indefinite warrant would be illegal (C N Stoddart, *Criminal Warrants*, (2nd ed.), paragraph 1.19); and warrants for the search of premises must specify the articles to which the search is directed and the places to be searched (Stoddart, *supra*, paragraph 3.11). However, in the present case no such issues arise. There was no challenge to the warrant's *validity* on those or any other grounds.

[16] We agree with the sheriff that the law requires to have regard to advances in information and electronic communications technology and to changes in the ways that data is commonly stored by the users of such technology. We also agree with him that the court

should be cautious about drawing analogies with physical items or data stored in premises not specified in a search warrant.

[17] It was common ground that authority was required for the police to use the log in credentials to search the account to which they related. That appears to us to be correct in the present case, because the data in the account was private data which was password protected. However, in some circumstances data stored with a cloud provider may be "open source" rather than private. One example of open source data is where a person has created a profile on Facebook which anyone may view. That is public content which police officers may examine without the need for the person's permission or a warrant. The position is different where data is accessible only with the use of a password. With such private data permission or a warrant is necessary in order to access it lawfully.

[18] The search warrant authorised a search of the appellant's home and the taking possession of mobile phones, tablets, computers, laptops, computer hardware, with peripheral equipment such as *inter alia*:

> "any computer or data processing software or data…other permanent and transient storage devices and other data storage devices…and any other articles which the officers have reason to believe are relevant to the investigation of the said crime and to examine any aforesaid devices or any other things whatsoever found in said premises which they have reasonable cause to believe may produce evidence material to said investigation".

It is clear that the recovery of the iPhone and its further examination were authorised, as was the recovery of the Mega.NZ log in credentials from the iPhone. The primary question for the court is whether the search of the "Aaron Lind" account was authorised by the warrant. That turns on a proper construction of the warrant's terms. Giving those terms their natural and ordinary meaning, we are satisfied that they did not authorise the police to use the log in credentials to log in to Mega.NZ or to search the account to which the

credentials gave access. The Mega.UK website was not peripheral equipment such as "data" or a "data storage device" on the premises, nor was it "other articles" or "other things whatsoever" found in the premises which the police had authority to examine. It follows that we disagree with the sheriff as to the warrant's scope.

[19] We are not convinced that our conclusion need present investigating or prosecuting authorities with insuperable difficulties. Drafters of search warrants ought to be alert to the possibility that log in credentials may be discovered on devices in premises; that examining the related cloud storage account or accounts may be necessary; and that authority to do that may need to be craved. Provided the usual rules concerning the validity of search warrants are complied with, we see no reason why such authority ought not to be granted. In cases where search warrants do not include such a crave the investigating authorities have two options if log in credentials are discovered on devices during the course of a search. They may obtain permission from the person concerned to use the credentials to log in to the account and to search it. If such permission is not given they may seek a further warrant. We foresee no real difficulty in obtaining such a warrant (especially where, as here, material evidence has already been found during the search). In cases where neither permission nor a further warrant has been obtained and the search has proceeded it will be up to the prosecuting authority to satisfy the court that there are good grounds for the irregularity being excused.

[20] In the present case the Mega.NZ app was not installed on the iPhone. It is unnecessary for us to opine whether, if it had been, access to, and search of, the "Aaron Lind" account via the app would have been authorised by the warrant. We confine ourselves to these observations. Clearer and more specific drafting could have put the matter beyond doubt. If there is uncertainty whether such a search is covered by the

terms of an existing warrant the matter may be resolved by obtaining the permission of the user or by seeking a further warrant. Once again, if a search proceeds without either of those courses having been followed, and it transpires that the search was irregular, it will be open to the prosecutor to seek to persuade the court that the irregularity should be excused.

[21] We have determined that the use of the log in credentials to access and search the "Aaron Lind" account went beyond the scope of the warrant and was irregular. The question which remains is whether that irregularity ought to be excused. In the whole circumstances we have no difficulty in concluding that it should. The search carried out was a very specific one. The offences being investigated were extremely serious and the data recovered was very important evidence. The cybercrime officer acted in good faith. He clarified with a senior officer that he was indeed authorised to conduct the search. The officer's belief that the search was within its scope was not an unreasonably held one having regard to the apparent width of the powers of search in the warrant and the advice given to him. We are reinforced in that conclusion by the fact that the sheriff formed the same view.

[22] The appeal is refused.