IN WESTMINSTER MAGISTRATES' COURT

LAURI LOVE

V

THE NATIONAL CRIME AGENCY

DECISION AND REASONS OF DISTRICT JUDGE M. COLEMAN

BACKGROUND AND PROPERTY IN DISPUTE

The court is dealing with an application by Mr. Lauri Love made under section 1 of the Police Property Act of 1897. He is seeking the return to him of items of computer hardware which remain in the possession of the National Crime Agency (NCA) following a search of his home address on 25th October 2013. During that search approximately 30 items of computer equipment were removed of which 24 have been returned.

The items the court is concerned with are as follows:

1. a Fujitsu Siemens laptop computer containing, amongst other information, private and confidential data exfiltrated ("hacked") from the "Police Oracle" website
2. Compaq computer tower containing, amongst other information, pirated versions of copyrighted films
3. Samsung laptop computer which was found with attachments, comprising 3 physically detachable parts (itemised below as 4-6) upon which data is stored:
4. an SD card containing, amongst other information, encrypted files x and q
5. a Western Digital external hard drive containing, amongst other information, encrypted file "truecrypt2"

6. a hard drive fitted within the laptop containing, amongst other information, encrypted data (a file "truecrypt1") which includes the following information:
    - hacked data from the United States Department of Energy and Senate
    - details of complainants and respondents to discrimination and harassment claims within the US military
    - copies of passports both UK and foreign with no apparent legitimate connection to Mr. Love
    - email addresses and associated passwords (the passwords in "hashed" format but which can in certain cases be unhashed)
    - details of names and home addresses and contact details of 258 court staff and judges in California
    - folders beginning "lolcc" details of over 232,000 individuals with their names, billing address, email address, telephone number, credit card number, expiry date and CVV number together with details of transactions, many of which appear to be donations to charities having no apparent connection with Mr. Love.
    - Private data, including photographs of vulnerable children, from an autism charity and treehouse school.

In February 2014 Mr. Love was given notice that a disclosure requirement had been imposed on him under section 49 of Part III of the Regulation of Investigatory Powers Act 2000 (RIPA) The Central Criminal Court ordered him to provide the encryption key or password for the encrypted items of hardware which are the subject of this application. To date he has not done so.

Application was first made by Mr. Love to the Bury Saint Edmunds Magistrates Court on 3 February 2015. That Court made a direction that he provide the decrypted information. He failed to do so and he withdrew the application on 1st July 2015, five days before the hearing date.

The application to this court was made on 1 October 2015 but had been adjourned pending the extradition proceedings which followed from a request by the Government of the United States of America for Mr. Love to stand trial in three

separate States on computer hacking charges. The applicant was discharged in February 2018 following an appeal to the High Court.

I note that in these proceedings the Court directed Mr. Love to submit a witness statement giving particulars of the contents of the files. He has not done so.

The matter came before me for hearing on 11 February 2019. On that date the applicant represented himself, with not inconsiderable ability, assisted by a McKenzie friend. The NCA was represented by Mr. Bird.

I am grateful to both the applicant and Mr. Bird for their skeleton arguments. They have made my task more straightforward by addressing the issues.

OPEN OR CLOSED HEARING?

These proceedings are regulated by the Criminal Procedure Rules. Rule 47 (37) states that the hearing should be in private *unless the judge directs otherwise*.

There is a significant interest in this case as evidenced by the large number of journalists and members of the public who attended court for the hearing. The BBC had reported the day before the hearing that it was due to take place and where it was to take place. Mr. Love enthusiastically engaged with reporters outside the courthouse on arrival at court as evidenced by photographs and he unequivocally waived his right to have the hearing in private.

Whilst I am a strong proponent of open justice I was also mindful that there may well be a prosecution of the applicant in due course. The Lord Chief Justice and Mr. Justice Ousley stated in their judgement in relation to the extradition proceedings that the applicant should face prosecution in this country. The Lord Chief Justice stated as follows:

"We emphasise however that it would not be oppressive to prosecute Mr. Love in England for the offences alleged against him. For from it. If the forum bar is to operate as intended, where it prevents extradition, the other side of the coin is that prosecution in this country rather than impunity should then follow. Much of Mr. Love's argument was based on the contention that

this indeed where it should be prosecuted. The CPS must now bend its endeavours to his prosecution with the assistance to be expected from the authorities in the United States, recognising the gravity of the allegations in this case and the harm done to victims….. these are serious offences indeed"

I therefore permitted the press and the public to be present during the hearing but imposed reporting restrictions. The only matters I permitted to be reported were the fact the application was being made, what the application related to and the date to which judgement would be reserved. I was informed that the applicant had uploaded his skeleton argument onto social media prior to the hearing. The journalists all had it. I asked Mr. Love to remove the document, which he said he would do straight away. I gave the press permission to report certain paragraphs contained within it whilst prohibiting other paragraphs. I told the members of the press that a written decision would be given to them on the date judgement is handed down. My intention is to ensure that no information would go into the public domain which might prejudice or compromise the integrity of a fair trial in due course.

THE LEGAL FRAMEWORK

CIVIL PROCEEDINGS

As these are civil proceedings the burden of proof rests on the applicant and the standard of proof is on the balance of probabilities. In other words, is a fact more likely than not.

POLICE POWERS OF SIEZURE AND RETENTION.

The applicants home address was searched under the authority of a search warrant and the items which form the subject of these proceedings were seized under section 8(2) of the Police and Criminal Evidence Act 1984.

Section 20 of the same statute it titles police officers to require computer you will be produced in the form which was visible and legible and available to take away. This they achieved by using the HARVEST exercise, which allows data to be seen and preserved. Unfortunately, before that process could be finished an encryption process cut in to the devices themselves.

Section 22(1) of PACE gives authority to police to retain any property which has been ***seized "so long as it is necessary in all the circumstances"***

S22(2) anything seized for the purposes of a criminal investigation may be retained for use as evidence at a trial for forensic examination or for investigation in connection with an offence….

S22(4) nothing may be retained for either of those purposes ……if a photograph or copy would be sufficient for that purpose.

THE POLICE PROPERTY ACT 1897.

Where any property has come into the possession of the police in connection with their investigation of a suspected offence, a court of summary jurisdiction may on application either by an officer of police or by claimant of the property, make an order for the delivery of the property to the person appearing to the magistrate or court to be the owner thereof…….

What immediately comes to mind is that there is more than one type of "property" which is the subject of this application. The six items of computer hardware form the first category of "property" and the data therein forms the second category.

There is no dispute that the computer items themselves belong to the applicant. It seems clear to me that the second category of property does not belong to the applicant, and indeed is "property" which ought not to be in his possession.

THE EVIDENCE

EVIDENCE OF THE APPLICANT.

The applicant was sworn and he adopted his statement as his evidence in these proceedings.

He also told me in oral evidence there was personal information contained on the computers which was of "*inestimable sentimental value*" He said some 5½ years had gone by since he was arrested and the Crown Prosecution Service had still not received a case file from the police. He also queried what had happened in the year since the determination of his extradition appeal. He said to me the police/CPS should "*do one's business or get off the pot*"

He said the NCA had effectively banned him from leaving this country because the USA would seek his extradition afresh from another country.

The cross- examination of the applicant by Mr. Bird related to the data/information which is contained in the computers. I do not intend to summarise this as it is information which ought not to go into the public domain for the reason stated above.

What I will say is that Mr. Love was unwilling to answer questions about the contents of the computers, neither about the content nor about how that content may have got onto his computers.

EVIDENCE OF THE NCA

This is contained within:

- the statements of two officers working with the NCA (Mr. Brown and Mr. Donnington-Smith)
- the founder of www. Policeoracle.com (Mr. Geoffrey Hyams)
- Adam Rutherford, offers the NCA cyber-crime unit. He has a Bachelor of Science degree in forensic computing and security.
- Joe Davies, he took a statement from the following witness.
- Steve Maughan. He is head of IT at a charitable organisation helping vulnerable children. He manages the desktop IT infrastructure for the organisation. He has confirmed that private information was contained on the applicant's computer. He says the information held by the applicant is significant. It contains personal details of users including significant personal and private information he says there is no reason for him to hold it and the organisation does not wish the applicant to have this data returned to the applicant under any circumstances.

As with Mr. Love's evidence and the evidence of his cross-examination, I am not going to set out the evidence of the NCA in full. It is similarly evidence which ought not to be in the public domain and which might compromise a criminal prosecution in due course.

I will summarise it as follows:

The identity that Mr Love uses for himself online suggests he has gained unauthorised access to highly confidential US and UK servers and has obtained massive amounts of compromised data. This unauthorised activity by Mr Love discloses offences under the law in the UK, contrary to the Computer Misuse Act 1990 and consequently the NCA commenced an investigation. That investigation was effectively put aside whilst the Government of the USA sought the extradition of Mr. Love. Since the determination of those proceedings 12 months ago the NCA's investigation was recommenced and is ongoing.

It is a massive task. The information on the devices is encrypted. At the time the computers were seized they were switched on and the NCA officers were able to harvest some of the data prior to the encryption software taking effect. The information on the computers although currently inaccessible to police is timeless and may be decrypted in the future. What material was obtained before the encryption process gives a snapshot of what data is there and none of it is anything that should be in the possession of the applicant.

The value of the hardware itself was estimated by the NCA officer, Mr Brown, at about £600. Mr Love suggested it was about half of that value.

The HARVEST drive is an image copy of what was taken from the applicant's laptop computer. There is about 124 gigabytes of data. That is about 67 million pages of A4.

Before the investigation by the NCA can complete, all of that must be gone through.

Additionally, the three files from the USA must be gone through, and only one has so far been received. The legal process for the transfer of the evidence needs to be gone through, from three separate States involving Letters of Request and Mutual Legal Assistance. It is a massive undertaking and clearly takes time.

FINDINGS ON THE EVIDENCE

I found Mr. Love to be evasive. He repeatedly tried to avoid answering questions by posing another in return to Mr. Bird or by saying that the NCA had not proved certain facts and would say nothing until full disclosure had been made to him and his legal team within a criminal prosecution. The applicant has the right not to self-incriminate but his refusal to answer questions about the content of the computers has made it impossible for him to discharge the burden of establishing that the data on his computers belongs to him and ought to be returned to him. He did concede he should not have the private details of individuals. He asked me to accept an undertaking from him that if the computer hardware is returned to him he would not decrypt or even attempt to decrypt any of the data. That is not a course I am willing to take.

I find as a fact that the information/data on the computers is NOT data to which the applicant is entitled and I find as a fact that the information on the HARVEST drive is data taken from Mr Love's computer eqipment. This is not a situation where the computers have been used as a repository by others, as Mr. Love suggested may have been the case.

ANALYSIS

Although the hardware is the property of the applicant it is of little financial value and what is of real significance is the data that is stored within each device.

Although I have not summarised the nature or content of that data within this judgement I am satisfied to the necessary standard that it is data which appears to have been "hacked."

I can see no legitimate purpose for the applicant being in possession of this data and it would clearly not be in the public interest for him to have any of it. Indeed, Mr. Love is a risk of the commission of further offences if he were to regain possession of this data. The information would be of considerable use to those engaged in organised crime.

I am also satisfied that the NCA needs to retain the items of computer equipment for its continuing criminal investigation and for any subsequent trial. I accept the

assertion by the officers of the NCA that copies or images would not suffice for the purposes of a trial.

The continued retention of the items is permitted under section 22 of PACE.

I have been referred by both the applicant and the respondent to a number of decisions, as follows, and I have read them. The relevant parts have been set out in the skeleton arguments of both parties.

a) Gough v Chief Constable of West Midlands Police [2004]EWCA Civ 206
b) Holding v Chief Constable of Essex [2005] EWHC 3091 (QB)
c) Scopelight v Chief Constable of Northumbria Police [2009] EWHC Civ 1156
d) Chief Constable of Merseyside v Owens [2012] EWHC 1515 (Admin)

I have been referred to the "public interest" defence and the relevance of article 1 of Protocol 1 to the European Convention on Human Rights.

Article 1 states that *every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.*

The word "*except*" demonstrates that this is not an absolute right. I assume those individuals from whom personal information appears to have been taken, would also wish not to be deprived of their possessions, in this case their private and personal information/data.

DECISION

I am satisfied that neither any of the computing items nor the data contained on any or all of them, should be returned to the applicant.

The computers and the data cannot be separated. The applicant is unwilling to assist in that regard.

Whilst I am satisfied that the computers belong to him I am satisfied that the NCA has both the power to retain the computers under section 22 of PACE and the need to retain them, to complete its criminal investigation and mount a criminal prosecution.

As noted in the extradition proceedings, there is substantial inconvenience in making all of the US evidence available to a trial court in this jurisdiction.

These computers are evidence in an ongoing enquiry and cannot be returned.

Turning to the data I am satisfied that it does not belong to Mr. Love. It belongs to others. It cannot be given back to him.

If a decision is taken not to prosecute Mr. Love in this jurisdiction, I will at that point authorise a second version of this decision, the closed version, to be handed down. It will contain a summary of the evidence that was given in court during these proceedings, which I have not allowed to be disclosed.

If there is a trial, the "closed version" of this decision will no longer be necessary as all the evidence will come out during that trial.

District Judge (Magistrates' Courts) Margot Coleman.

19th February 2019.