IN THE CITY OF WESTMINSTER MAGISTRATES' COURT
No. 011503187270

FOR MENTION ON 12 APRIL 2016 AND FOR FINAL HEARING ON 28 JULY 2016

DISTRICT JUDGE TEMPIA

IN THE MATTER OF AN APPLICATION UNDER SECTION 1 OF THE POLICE PROPERTY ACT 1897

LAURI LOVE

Claimant

-v-

NATIONAL CRIME AGENCY

Respondent

SKELETON ARGUMENT OF THE CLAIMANT
FOR MENTION ON 12 APRIL 2016

INTRODUCTION

1. The issue to be decided at the hearing on 12 April 2016 is whether or not the Court should direct the Claimant to provide the encryption keys or passwords for files stored on three items of computer hardware which the Respondent seized from the Claimant in October 2013 ("**the Direction**"). The Respondent has applied for the Direction to be given under the Court's general case management powers set out in Rule 3A of the Magistrates' Court Rules 1981 SI 552 ("**the Case Management Powers**"). The Claimant opposes the Respondent's application and submits that no direction should be given at this hearing.

2. The encrypted items to which the Respondent's application relates ("**The Encrypted Files**") are:

    a. The file truecrypt1 on the internal Hard Drive (exhibit AH/01/HD1/25/10/13) of the Claimant's Samsung Laptop (exhibit AH/01/25/10/13);

b. Files x and q on the Claimant's SD Card (exhibit AH/01/SD1/25/10/13);

c. The file truecrypt2 on the Claimant's Western Digital Hard Drive (exhibit AH/02/25/10/13).

3. The Respondent's application is made in the context of an application by the Claimant for the return of five items of computer hardware from the Respondent, of which three store the Encrypted Files. The Claimant's application is made under section 1 of the Police (Property) Act 1897 ("**PPA**"). The application will be determined at a final hearing on 28 July 2016.

4. The Claimant submits that the Court should not accede to the Respondent's application to direct the Claimant provide the encryption keys or passwords for the following reasons:

a. The Respondent is seeking to bypass the proper statutory mechanism by which to seek encryption keys or passwords, namely section 49 of the Regulation of Investigatory Powers Act 2000 ("**RIPA**"), and hence to bypass the statutory safeguards which Parliament intended should protect Mr Love;

b. Such a direction would infringe Mr Love's rights under Article 8, Article 18 and Article 1 Protocol 1 of the Human Rights Act 1998 ("**HRA**"). The Court's Case Management Powers and section 1 PPA must be read so as to be Convention rights compliant, pursuant to section 3 HRA.

FACTUAL BACKGROUND

5. Lauri Love is 31 years old (DOB 14.12.84) and has lived with his parents, the Reverend and Mrs Love, at 2 Ash Walk, Stradishall, Newmarket, Suffolk CB8 9YE since 2012, following a period of depression and mental ill-health in his late twenties.

6. On 24 October 2013, the Respondent National Crime Agency ("**NCA**") was granted a search warrant in relation to the Love family property. The search warrant relied upon

to seize the computers cited section 1(1) and (3) of the Computer Misuse Act 1990 (causing a computer to perform a function to secure unauthorised access to a program / data) as the offence under investigation.

7. The warrant was exercised on 25 October 2013 in a manner which prompted Reverend Love, Lauri Love's father, to make a complaint to the NCA's Professional Standards Unit for investigation on 5 January 2014. Complaints included:

    a. NCA officers entered the property by deception, with the first officer purporting to be a courier;
    b. An excessive number of officers (14) attended the residence;
    c. Reverend Love was prevented from going into his garden during the search, despite not being a suspect;
    d. The possibility that NCA officers had released information about the search to the press, as the Love's property was subsequently 'flooded' with journalists.

8. During the exercise of the search warrant on 25 October 2013, computer equipment and digital storage devices belonging to all three members of the family were seized.

9. During the search, Lauri Love was arrested. He was then released on pre-charge conditional bail. Mr Love was never charged and ceased to be on bail in July 2014. Mr Love states at [48] of his personal statement that in October 2014 he was shown a letter sent by CPS in reply to a letter from his MP, Matthew Hancock, stating that it had no intention of prosecuting him at that time. Mr Love has requested a No Further Action letter but the CPS has not provided one.

10. The return of these items has been an ongoing issue for the 2 ½ years following the seizure. In summary:

    a. The Loves were informed by an NCA officer at the time that these items would be required for two to three weeks for examination to determine their relevance to the NCA's investigation, after which time irrelevant items would be returned.

b. Reverend and Mrs Love's computer equipment was not returned until 29 January 2014, over 14 weeks after their seizure and after the NCA was prompted by Reverend Love's letter of complaint.

c. Of approximately 29 seized items, 24 have been returned to date. Mr Love's s1 PPA application relates to the outstanding five items.

d. In November 2014 the NCA offered to return the outstanding property on the condition that they "forensically wipe" the data contained on all the devices.[1] Mr Love refused as the devices contain everything he owned digitally including photographs, writing and other creative pieces of work.

11. In February 2014, Mr Love was given notice that a disclosure requirement had been imposed upon him pursuant to section 49 RIPA. He was thereby required to decrypt the Encrypted Files within 28 days. Mr Love did not comply. The section 49 process was not continued by NCA. Mr Love was not arrested or charged but rather in July 2014 was released from bail.

12. In early 2015, Mr Love made his first application under s1 PPA for the return of his property. Bury St Edmunds Magistrates' Court gave case management directions that he provide decryption information. Mr Love objected, and when this objection was unsuccessful, withdrew his application.

RELEVANT LAW

13. Part III of the Regulation of Investigatory Powers Act 2000 provides, in relevant part:

Section 49 - Power to require disclosure

(1) This section applies where any protected information –
(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;

…

(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds –

(a) that a key to the protected information is in the possession of any person,

[1] Lauri Love Personal Statement at [49]

(b) that the imposition of a disclosure requirement in respect of the protected information is
   i. Necessary on grounds falling within subsection (3), or
   ii. Necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,
(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and
(d) That is is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section,

the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security;
(b) for the purpose of preventing or detecting crime; or
(c) in the interests of the economic well-being of the United Kingdom.

(4) A notice under this section imposing a disclosure requirement in respect of any protected information—
(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;
(b) must describe the protected information to which the notice relates;
(c) must specify the matters falling within subsection (2)(b)(i) or (ii) by reference to which the notice is given;
(d) must specify the office, rank or position held by the person giving it;
(e) must specify the office, rank or position of the person who for the purposes of Schedule 2 granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;
(f) must specify the time by which the notice is to be complied with; and
(g) must set out the disclosure that is required by the notice and the form and manner in which it is to be made;
and the time specified for the purposes of paragraph (f) must allow a period for compliance which is reasonable in all the circumstances.

…

Section 50 – Effect of notice imposing disclosure requirement

(1) Subject to the following provisions of this section, the effect of a section 49 notice imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that he—

(a) shall be entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form; and
(b) shall be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form.

(2) A person subject to a requirement under subsection (1)(b) to make a disclosure of any information in an intelligible form shall be taken to have complied with that requirement if—

(a) he makes, instead, a disclosure of any key to the protected information that is in his possession; and
(b) that disclosure is made, in accordance with the notice imposing the requirement, to the person to whom, and by the time by which, he was required to provide the information in that form.

(3) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a section 49 notice—
(a) that person is not in possession of the information,
(b) that person is incapable, without the use of a key that is not in his possession, of obtaining access to the information and of disclosing it in an intelligible form, or
(c) the notice states, in pursuance of a direction under section 51, that it can be complied with only by the disclosure of a key to the information,
the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the notice imposing the requirement, to make a disclosure of any key to the protected information that is in his possession at a relevant time.

…

(8) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a section 49 notice—
(a) that person has been in possession of the key to that information but is no longer in possession of it,
(b) if he had continued to have the key in his possession, he would have been required by virtue of the giving of the notice to disclose it, and
(c) he is in possession, at a relevant time, of information to which subsection (9) applies,
the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the notice imposing the requirement, to disclose all such information to which subsection (9) applies as is in his possession and as he may be required, in accordance with that notice, to disclose by the person to whom he would have been required to disclose the key.

(9) This subsection applies to any information that would facilitate the obtaining or discovery of the key or the putting of the protected information into an intelligible form.

…

Section 53 – Failure to comply with a notice

(1) A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice.

(2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.

(3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if—
(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and
(b) the contrary is not proved beyond a reasonable doubt.

(4) In proceedings against any person for an offence under this section it shall be a defence for that person to show—

(a) that it was not reasonably practicable for him to make the disclosure required by virtue of the giving of the section 49 notice before the time by which he was required, in accordance with that notice, to make it; but
(b) that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.

(5) A person guilty of an offence under this section shall be liable—

(a) on conviction on indictment, to imprisonment for a term not exceeding the appropriate maximum term or to a fine, or to both;
(b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

Safeguards
Section 55 – General Duties of specified authorities

(1) This section applies to—

(a)the Secretary of State and every other Minister of the Crown in charge of a government department;

(b)every chief officer of police;

(ba)the Director General of the Serious Organised Crime Agency;

(bb)the Director General of the Scottish Crime and Drug Enforcement Agency;

(c)the Commissioners for Her Majesty's Revenue and Customs;

(d) every person whose officers or employees include persons with duties that involve the giving of section 49 notices.

(2) It shall be the duty of each of the persons to whom this section applies to ensure that such arrangements are in force, in relation to persons under his control who by virtue of this Part obtain possession of keys to protected information, as he considers necessary for securing—

(a) that a key disclosed in pursuance of a section 49 notice is used for obtaining access to, or putting into an intelligible form, only protected information in relation to which power to give such a notice was exercised or could have been exercised if the key had not already been disclosed;

(b) that the uses to which a key so disclosed is put are reasonable having regard both to the uses to which the person using the key is entitled to put any protected information to which it relates and to the other circumstances of the case;

(c) that, having regard to those matters, the use and any retention of the key are proportionate to what is sought to be achieved by its use or retention;

(d) that the requirements of subsection (3) are satisfied in relation to any key disclosed in pursuance of a section 49 notice;

(e) that, for the purpose of ensuring that those requirements are satisfied, any key so disclosed is stored, for so long as it is retained, in a secure manner;

(f) that all records of a key so disclosed (if not destroyed earlier) are destroyed as soon as the key is no longer needed for the purpose of enabling protected information to be put into an intelligible form.

(3) The requirements of this subsection are satisfied in relation to any key disclosed in pursuance of a section 49 notice if—

(a) the number of persons to whom the key is disclosed or otherwise made available, and

(b) the number of copies made of the key,

are each limited to the minimum that is necessary for the purpose of enabling protected information to be put into an intelligible form.

14. Section 3 of the Human Rights Act 1998 provides:

Interpretation of Legislation

(1) So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights.

…

15. Article 8 of the Human Rights Act 1998 provides:

Right to respect for private and family life

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society

in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

16. Article 18 of the Human Rights Act 1998 provides:

Limitation on use of restrictions on rights

The restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed.

17. Article 1 of Protocol 1 of the Human Rights Act 1998 provides:

Protection of property

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 preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.

18. Rule 3A of the Magistrates' Court Rules 1981 SI 552 as amended provides:

(1) The court must actively manage the case. That includes—
(a) the early identification of the real issues;
(b) the early identification of the needs of witnesses;
(c) achieving certainty as to what must be done, by whom and when, in particular by the early setting of a timetable for the progress of the case;
(d) monitoring the progress of the case and compliance with directions;
(e) ensuring that evidence, whether disputed or not, is presented in the shortest and clearest way;
(f) discouraging delay, dealing with as many aspects of the case as possible on the same occasion and avoiding unnecessary hearings;
(g) encouraging the participants to co-operate in the progression of the case; and
(h) making use of technology.

(2) The court must actively manage the case by giving any direction appropriate to the needs of that case as early as possible.

(3) Each party must—
(a) actively assist the court in managing the case without, or if necessary with, a direction; and

(b) apply for a direction if needed to assist with the management of the case.

…

(7) In fulfilling its duty under paragraph (2) actively to manage the case the court may give any direction and take any step unless that direction or step would be inconsistent with legislation, including these Rules.

…

SUBSTANTIVE ARGUMENT: WHY THE DIRECTION SHOULD NOT BE GIVEN

19. The Claimant submits that the direction sought by the NCA circumvents RIPA, is an improper use of the Court's Case Management Powers and breaches Mr Love's Article 8, Article 18 and A1P1 rights under HRA. Each argument is considered in turn below.

CIRCUMVENTING SECTION 49 RIPA

20. The NCA seeks the encryption keys and passwords pursuant to the Court's general Case Management Powers. In doing so the NCA is circumventing the proper statutory mechanism for the investigation of encrypted data. This is found in Part III of RIPA, from sections 49 to 56, which is entitled "*Investigation of electronic data protection by encryption".* In Part III RIPA, Parliament has enacted a single, unified scheme setting out the process which the police, the NCA and others must follow in order to require encrypted data to be disclosed.

21. One situation which triggers the power in Part III RIPA is when encrypted information is seized under a warrant. The Part III process begins by giving a written notice requiring disclosure to the person reasonably believed to possess the encryption key. That person is then required to disclose the key within a specified time. If it is no longer in their possession they must disclose all information in their possession to facilitate obtaining the key. If they do not make the required disclosure in the specified time, they have committed an offence and criminal proceedings may be brought. During those proceedings the defendant may establish that they were not in possession of the key. They are required only to adduce sufficient evidence to raise this defence and it is then for the prosecution to prove the contrary beyond reasonable doubt. The defendant may

also raise the defence that it was not reasonably practicable to make the disclosure within the required time.

22. The RIPA scheme has multiple inbuilt safeguards. These were considered so important by Parliament that section 55 RIPA, in which some of them are found, is devoted entirely to safeguards. The Part III protections include:

    a. The imposition of the disclosure requirement must be necessary for one of four specified purposes;
    b. The disclosure requirement must be proportionate to that purpose;
    c. The disclosure requirement must be the only reasonably practicable means of obtaining the encrypted information;
    d. The person imposing the notice must have appropriate permission;
    e. A duty to ensure access is only gained by means of the requirement to information to which the notice gave entitlement;
    f. A duty to ensure the use to which the key is put is reasonable ;
    g. A duty to ensure the use and retention of the key is proportionate to the aims for which it was necessary;
    h. A duty to ensure the key is stored securely;
    i. A duty to ensure that records of the key are destroyed as soon as no longer needed.

23. Additionally, Parliament was under an obligation when enacting RIPA to ensure the quality of the law was such that it was compatible with Convention rights. Section 19 HRA requires a minister with the conduct of any Bill, before its second reading, to make and publish a "statement of compatibility".

24. The NCA began the Part III RIPA process in February 2014 but then elected to take no further action to continue it. In now seeking the key to encrypted data under the Case Management Powers they seek wholly to bypass the proper statutory scheme. In doing so they deprive Mr Love of all the statutory safeguards in that scheme set out above.

25. Rule 3A of the Magistrates' Court Rules 1981, at subsection 7, provides that "*in fulfilling its duty […] actively to manage the case, the court may give any direction and taken any step unless that direction or step would be inconsistent with legislation, including these Rules".* The Respondent acknowledges at [4] of its supplementary skeleton argument that disclosure ought to permit a level playing field "*so far as it does not infringe other legislation".* A direction to provide encryption keys and passwords under general Case Management Powers infringes the RIPA legislation, and would not be permissible under the Magistrates' Court Rules 1981 pursuant to subsection 7. It also infringes s.6 of the Human Rights Act for reasons which are developed below.

IMPROPER USE OF CASE MANAGEMENT POWERS

26. Even without the circumvention of Part II RIPA, the Respondent's application constitutes an unusual and improper use of the Court's Case Management Powers.

27. The Claimant has brought a civil action for the return of his property under s1 PPA. The NCA states that it has made this application for access to the Encrypted Files because the data will be needed in order for the Claimant to establish ownership at the final hearing. However, whether its opponent will need certain evidence or not in order to succeed at that final hearing cannot be of concern to the Respondent. The Claimant has brought the claim, and it is for the Claimant to prove his case to the civil standard of proof, under the doctrine that "*he who asserts must prove".* The judge at the final hearing will determine whether or not to grant the Claimant's application based on the arguments and evidence which both parties in fact offer. The key to the correct approach lies in the burden of proof. If the Claimant, on the arguments he chooses to run, satisfies the court to the civil standard, his application will succeed. Otherwise, it will fail. In the absence of an appropriate application by the Respondent under the proper statutory scheme (RIPA), it is for Mr Love to decide whether he is able to and whether he elects to adduce the decrypted data.

28. It is not for the Respondent to take steps or make case management applications on the Claimant's behalf or to tell the Claimant what or how to argue at his final hearing. Neither is it for the Respondent to decide what evidence will assist the Claimant's chosen arguments. It is certainly not for the Respondent, having second guessed what

the Claimant will do to win, to attempt to force the Claimant to do it at an earlier stage of proceedings.

HUMAN RIGHTS ACT 1998

29. The Claimant submits that the NCA's application violates his rights under Article 8, Article 18 and A1P1 of HRA. Section 6 HRA makes it unlawful in most circumstances for a public authority to act in a way which is incompatible with a Convention right[2]. Section 6(3)(a) makes courts and tribunals public authorities. In the instant case both the NCA and the Court are therefore subject a duty to act in such a way as to give effect to the Convention.

Article 8

30. Article 8 HRA protects "*rights of central importance to the individual's identity, self-determination, physical and moral integrity, maintenance of relationships with others and a settled and secure place in the community"*: *Connors v UK* (2005) 40 EHRR 9 at [82]. In the instant case, it is the state's negative duty to abstain from interference in a citizen's private life which is engaged.

31. Article 8 is a qualified right. In order to be justified, however, an interference by the state with a person's Article 8 rights must fall within one of the exceptions in Article 8(2) and must meet the general requirements of justification (it must be in accordance with law and necessary in a democratic society). It is for the citizen who enjoys the right to establish interference. It is for the public body interfering with the right to justify its interference: *R (Wood) v Metropolitan Police Commissioner* [2009] All E R 951. Nonetheless, the Claimant submits that the interference in the instant case is unjustified.

32. The Court of Appeal in *AG (Eritrea) v SSHD* [2007] EWCA Civ 801 at [19] used five questions by which it can be determined whether there is a breach of Article 8:

[2] The only exception is where the public authority is required to do so by primary or secondary legislation which cannot be interpreted compatibly with the Convention.

a. Will there be an interference with the right to respect for private or family life?
b. If so, is the interference of such gravity to engage Article 8?
c. If so, is such an interference in accordance with the law?
d. If so, is it necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others?
e. If so, is such interference proportionate to the legitimate public end sought?

33. To answer each question in turn:

a. The NCA's application for the encryption keys and passwords constitutes an interference with Mr Love's right to respect for private life, right to respect for correspondence and his right to privacy. This is clear from it being an application to be given access to Mr Love's private information stored in the Encrypted Files.

b. The interference is of such gravity to engage Article 8. Mr Love explains at [14] of his personal statement that the seized items of computer hardware and digital storage devices contain his entire digital life, including "the collected creative works of my life, ongoing projects, cherished correspondence, photographs, writings and memories of inestimable personal and sentimental value". Like the European Court of Human Rights ("**ECtHR**"), the domestic courts' threshold for engaging Article 8(1) is generally low: *LB Harrow v Quazi* [2003] UKHL 43, [2004] 1 AC 983 at [8] – [10]. This interference clearly far exceeds the low threshold[3].

c. It is for the NCA to justify its interference with Mr Love's Article 8 rights, and thus to answer questions (c) to (e), and not for Mr Love to prove that the interference is unjustified. Nonetheless, the Claimant submits that in this case

[3] This interference also exceeds the interference in other cases in which Article 8 was not only engaged but also breached. In *Halford v UK* (1997) 24 EHRR 523 the interception of phone calls was found to breach Article 8. In *Khan v UK* (2001) 31 EHRR 45 the same was found for a listening device in a person's home. In *R (Wood) v Metropolitan Police Commissioner* [2009] EWCA Civ 414, [2009] All ER 951 the retention by the police of a photograph of a protester in the street violated Article 8. In *PG v UK* [2001] ECHR 44787/98 it was found that recording a suspect in a police cell interfered with Article 8.

justification is not possible. The first element of justification is whether the interference is in accordance with the law. As explained above, gaining the encryption keys and passwords through the use of the Court's Case Management Powers would not be in accordance with the law because it circumvents the s49 RIPA statutory scheme for the investigation of encrypted data.

d. The NCA's stated aim in making its application is to ensure the court will be able to dispose of Mr Love's civil claim. There are two reasons why this does not satisfy the necessity requirement:

    i. This purpose does not fit within one of the legitimate aims permitted by Article 8(2). It is not for public bodies to act as legislator by creating their own 'legitimate' aims.
    ii. Even if the stated aim had been legitimate, the direction sought is not actually necessary for the NCA's purpose. As explained above, the judge will determine whether Mr Love has succeeded in his application on the balance of probabilities on the basis of the arguments and evidence offered. As the NCA itself admits at [15] of its skeleton argument, in the absence of a Court inspection of the Encrypted Files, the best approach is "*for (1) Mr Love as Claimant and (2) the NCA as Respondent to give evidence of what data is on the media*".

e. Even if disclosing the encryption keys were necessary to achieve a legitimate aim, it would be a disproportionate interference with Mr Love's Article 8 rights to direct that he give the police access to all the Encrypted Files. The degree of scrutiny appropriate when deciding proportionality depends on the nature of the right at stake. In cases concerning 'the most intimate aspects of private life' the Court adopts a tough standard of review: *Dudgeon v UK* (1981) 4 EHRR 149. It is possible for there to be a disposal of Mr Love's claim without any of his rights being infringed. Without this direction, Mr Love has a choice of whether to offer access to the Encrypted Files or risk the non-return of his property. It would be disproportionate for the Court to infringe Mr Love's Article 8 rights

in order to furnish him with an additional argument for use in his own civil proceedings, against his wishes.

Article 18

34. The legitimate aims set out in Article 8(2) should be read with Article 18 of the Convention. Article 18 provides that the restrictions to the qualified rights shall not be applied for any purpose other than those for which they have been prescribed. This is in effect a good faith provision.

35. Even if the reason given by the NCA for the interference had been one of the legitimate aims listed in Article 8(2) (which it is not), Article 18 obliges the NCA to be interfering in reality for the reason given. The NCA must not be interfering for an ulterior reason.

36. The unusual and irregular nature of this application (see above) suggests an ulterior reason. The NCA has had the Encrypted Files in its possession since October 2013. It has been unable to decrypt them in those 2 ½ years. It has made various unsuccessful attempts to obtain the encryption keys or passwords, including unfulfilled requests and the aborted use of the section 49 RIPA procedure. The NCA has demonstrated through its behaviour that it wants access to the Encrypted Files. It now presents an argument that the very access it had been seeking since 2013 is needed for case management purposes. This strongly suggests the Article 18 good faith requirement is not met.

Article 1 Protocol 1

37. A direction to provide the encryption keys and passwords would breach Mr Love's rights under Article 1 Protocol 1 ("**A1P1**"). In *Sporrong and Lonnroth v Sweden* (1982) 5 EHRR 35 at [61] the ECtHR interpreted A1P1 as containing "three distinct rules". There will be prima facie interference with the right to property if:

    a. The peaceful enjoyment of the applicant's possessions has been interfered with by the state (rule 1);

    b. The applicant has been deprived of possessions by the state (rule 2);

c. The applicant's possessions have been subjected to control by the state (rule 3).

38. The fact that Mr Love has been deprived of the computer hardware and data (a breach of rule 2) is an issue for the final hearing. However, a direction to provide encryption keys and passwords would constitute a breach of rules 1 and 3. The provision of the encryption keys and passwords would lead to direct interference by the NCA in which the state takes actual control of Mr Love's computer hardware and data in a manner which prevents peaceful enjoyment. This state control would, inter alia, effectively set aside Mr Love's A1P1 rights to practice data security as regards his possessions as he sees fit as their owner. Controls on the use of property can include requirements that property owners take positive action: *Denev v Sweden* (1989) 59 DR 127. Here the requirement that Mr Love provide the encryption keys and passwords would constitute control by the state.

39. A1P1 is a qualified right. Interference will not violate A1P1 if it is justified, meaning if it is done in the public interest or to enforce such laws as the state deems necessary to control the use of property in the public interest. As with Article 8, the interference must be lawful and achieve a fair balance between the public interest and the fundamental rights of individuals. The same test for justification applies to controls on use of property as to deprivations of possessions: *Pye v UK* (2008) 46 EHRR 34.

a.

Section 3

40. Section 3 HRA requires primary and secondary legislation to be read and given effect in a way which is compatible with Convention rights, so far as it is possible to do so. This is the case whether or not the legislation was enacted after HRA. Section 3 is a general requirement applicable to any reader, not just judges. It therefore applies to NCA as well as the Court. It is a strong interpretive obligation, imposing a duty to interpret statutory provisions compatibly with Convention rights wherever possible regardless of other, perhaps more literal, interpretations, or precedents to the contrary.

41. Section 1 PPA and the Court's Case Management Powers both fall under s3 HRA to be interpreted and given effect in a way which is compatible with Mr Love's Convention rights. Case Management Powers cannot permit the Court to give directions in violation of Articles 8 and A1P1 (further reinforcing the s7 Magistrates' Court Act prohibition on Case Management Powers infringing other statute). Likewise the requirements which s1 PPA places on Mr Love as an applicant cannot be such as to infringe his Article 8 and A1P1 rights.

RESPONSE TO NCA'S SUPPLEMENTARY SKELETON ARGUMENT

42. The NCA has submitted a supplementary skeleton argument dated 5 April 2016 which relies on section 4 subsection 47.37 (3)(a) of the Criminal Procedure (Amendment) Rules 2016 SI 120 ("**Section 3(a) CPR**"). Section 3(a) CPR requires that an application for an order under section 1 PPA must, inter alia, "*explain the applicant's interest in the property (either as a person who claims to be its owner or as an officer into whose possession the property has come)".* The NCA asserts without further argument that this section "*lends some support to its submission that Mr Love should in this case be required to provide the encryption key or password as only thus will the Court be able to adjudicate fairly upon the complete contents of the devices*".

43. The Claimant's position is that this section adds nothing to the NCA's submission. Section 3(a) is a procedural requirement. It is found in a list of necessary contents of a Claimant's written application for the return of seized property under s1 PPA. It was already established in PPA itself before this new statutory instrument came into force that s1 PPA is for use by owners of property which has been seized.

44. Section 3 HRA requires primary and subordinate legislation to be read and given effect in a way which is compatible with Convention rights, so far as it is possible to do so. This strong interpretive obligation on the NCA and the Court means that Section 3(a) (in addition the Court's Case Management Powers and PPA, see above) must be understood in a way which does not infringe Mr Love's Convention rights, in particular Article 8 and A1P1. The requirement that an applicant under s1 PPA be an owner cannot mean that Section 3(a) or the Court's Case Management Powers entitle the NCA or the

court to breach Mr Love's property rights and his right to respect for his private life. The NCA's reading of Section 3(a) is precluded by section 3 HRA.

45. In relation to [4] and [5] of the Respondent's supplementary skeleton, the Claimant submits that each of his arguments opposing the Respondent's application for the encryption keys and passwords would apply equally whether that application was made under Civil or Criminal Procedure Rules. It is the attempted use of case management powers *per se* in order to gain access to seized encrypted data to which the Claimant objects. It is therefore not necessary for the Court to determine which set of rules apply to applications under section 1 PPA in order fairly to dispose of this application.

CONCLUSION

46. For the reasons stated above, the Court is invited to decline making the direction sought by the Respondent.

STEPHEN CRAGG QC

Monckton Chambers

BEN COOPER

Doughty Street Chambers

9 April 2016