The Law Society
of British Columbia

Report of the Mirror Imaging Working Group: *Forensic Copying of Computer Records by the Law Society*

For: The Benchers

Date: October 14, 2009

Gavin Hume, Q.C. (Chair)
Robert Brun, Q.C.
Bruce LeRose, Q.C.
Glen Ridgway, Q.C.
Kenneth Walker

Purpose of Report: **Discussion and Decision**

Prepared on behalf of: **The Mirror Imaging Working Group**

Policy and Legal Services Department
Doug Munro 604-605-5313

1. EXECUTIVE SUMMARY

This report contains a series of recommendations designed to modernize the Law Society's regulatory function in order to keep pace with changes in computer technology, as well as suggesting processes to better protect personal information contained in digital records the Society can copy and access. The main focus of the report is on the Rule 4-43 discipline investigation, but the report also contains recommendations regarding custodianships and some general recommendations.

Rule 4-43 of the Law Society Rules establishes a process by which a designated category of Bencher can order an investigation into a lawyer's records in circumstances where the lawyer may have committed a discipline violation. This process requires the lawyer who is subject to the order to immediately permit the copying of all records. A "record" now includes electronic storage devices, such as a computer hard drive and the information contained therein. Although courts have likened computer hard drives to filing cabinets, digital information is stored in a qualitatively different manner than non-digital information, and the analogy becomes strained in application.

The copying of a hard drive, often called "mirror imaging", creates a range of challenges because it captures all of the information stored on the hard drive. In this report the Working Group has used the term "forensic copying" because it is more descriptive of the purpose for which the Law Society would seek to copy digital records. [1] This report contains the analysis and recommendations of the Working Group regarding how the Law Society can carry out its regulatory function, while at the same time preserving a reasonable expectation of privacy of its members in the personal information stored on digital records.

This issue was brought to the attention of the Executive Committee in June 2008. The Executive Committee struck a working group consisting of Gavin Hume, Q.C. (Chair), Bruce LeRose, Q.C. and Glen Ridgway, Q.C., to explore the practical and policy issues involved in the Law Society making a copy of a lawyer's hard drive. The Working Group met on four occasions, and reported to the Benchers on February 27, 2009. At that meeting several Benchers expressed concern about the topic, and the Benchers resolved to appoint the three Benchers with the greatest concerns to the Working Group, and tasked the reconstituted group with revisiting the issue. With the additions of Robert Brun, Q.C., Robert Punnett, Q.C. (as he then was), and Kenneth Walker, the Working Group met three more times. In June 2009 the Working Group lost the services of The Honourable Mr. Justice Punnett, due to his appointment to the Supreme Court of British Columbia. The Working Group met an additional time in July 2009, and this report was drafted subsequent to that meeting. While Mr. Justice Punnett did not

[1] Reference to "digital records" is intended to support the broad, modern concept of what constitutes a record as defined in the *Interpretation Act*, R.S.B.C. 1996, c. 238, and should not be read as limited to a computer hard drive.

participate in the drafting of this report, as a Bencher participant he provided a valuable perspective to the topic.

The Working Group engaged in detailed analysis and debate, and while consensus was achieved in many areas, it was not achieved in all. Mr. Walker holds a different view than the majority regarding the best process for the Law Society to engage in the copying of digital records. Rather than create two reports, the Working Group has set out Mr. Walker's concerns in this report. In addition, one of the recommendations is presented as two options: that of the majority and that of Mr. Walker. The reason for taking this approach is that the analysis of the Working Group was a collaborative effort, and while Mr. Walker expressed a preferred approach, he also contributed to the development of the majority approach.

The Working Group received staff support from the Audit and Investigation Department, the Professional Conduct Department, and the Policy and Legal Services Department, and external assistance regarding the technical aspects of making a forensic copy of computer records.

2. THE ISSUE

The Law Society has a variety of powers to deal with lawyers' records, including investigations under Rule 4-43, Audits, Custodianships, Practice Standards, etc. These powers were conceived in a non-digital paradigm, where the authority to copy records was less problematic because many non-digital records can be pre-filtered by sight, thereby reducing the risk that irrelevant records are being copied. Digital records are stored in packets of information that can be scattered in various locations on a storage device. They are stored in the form of code, and use a combination of hardware and software to become comprehensible to people accessing them.

The sort of pre-filtering that is capable with non-digital records is not an option with digital records. The act of making a forensic copy of a hard drive takes a snapshot of all the information on the hard drive at a point in time. Some of the information captured in the forensic copy will be critical to a Law Society investigation, but other information will not. Of the latter, some of the information will be personal information for which the lawyer or a third party rightly expects a degree of protection. The core issue the Working Group considered was how the Law Society can carry out its investigative function to protect the public interest pursuant to s. 3 of the *Legal Profession Act*, while respecting a reasonable expectation of privacy a member under investigation has in personal information stored on digital records.

3. THE WORKING GROUP'S ANALYSIS

(a) The Scope of Rule 4-43

The Working Group analyzed whether Rule 4-43, as presently drafted, is broad enough to contemplate making a forensic copy of a computer hard drive or other storage device. Rule 4-43 states:

> 4-43 (1) If the chair, vice chair or another Bencher member of the Discipline Committee believes that a lawyer or former lawyer may have committed a discipline violation, that Bencher may order that an investigation be made of the books, records and accounts of the lawyer or former lawyer.
>
> (2) When an order is made under subrule (1),
>
> > (a) the Executive Director must designate one or more persons to conduct the investigation, and
> >
> > (b) the lawyer or former lawyer concerned must immediately produce and permit the copying of all files, vouchers, records, accounts, books and any other evidence and must provide any explanations that the persons designated by the Executive Director under paragraph (a) require for the purpose of the investigation

While "record" is not defined in the *Legal Profession Act* or the Law Society Rules, the *Interpretation Act*, R.S.B.C. 1996, Chapter 238, s. 29 defines "record" as including:

> books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise.

It is well established by case law that computer hard drives and similar storage devices are records (see, for example, *Prism Hospital Software Inc. v. Hospital Medical Records Institute* (1991), 62 B.C.L.R. (2d) 393 (S.C.), where the court observed that the only difference between records and programs that are stored on paper versus magnetic media are the techniques required to access the information (para. 6), and *Baldwin Janzen Insurance Services (2004) Ltd. v. Janzen,* 2006 BCSC 554 where the court held: "[t]here is no dispute that data and information in electronic form are documents" (para. 28)). The dispute in most cases centers around access to information stored on the record, or the scope of disclosure required. While these cases are informative, most of them deal with disputes between civil litigants or between the state and the accused in a criminal matter; they do not deal with the authority of a regulatory body to copy and access records of one of its members.

The “thing” on which information is stored is the hard drive, and therefore a hard drive is a record. The hard drive is a record, and it contains records and documents. Rule 4-43 requires the lawyer to immediately permit the copying of all records. There are no words of limitation contained in Rule 4-43.

The Law Society Rules state a “"discipline violation" means any of the following:

> (a) professional misconduct;
>
> (b) conduct unbecoming a lawyer;
>
> (c) a breach of the Act or these Rules;
>
> (d) incompetent performance of duties undertaken by a lawyer in the capacity of a lawyer;
>
> (e) conduct that would constitute professional misconduct, conduct unbecoming a lawyer or a contravention of the Act or these Rules if done by a lawyer.”

A discipline violation can cover a wide variety of matters, but even if one were to construe it narrowly, there can be many types of records stored on a hard drive that are relevant (e.g. accounting records, email, notes to file, etc.). Reading the rule in its ordinary meaning and context and with regard to its purpose in the Act and Rules led the majority of the Working Group to conclude that a 4-43 order contemplates the ability to copy all records in order to examine a wide variety of matters for which lawyers are subject to regulation.

This was an area where there was a divergence of opinion. The majority view was that the power to copy records includes the power to copy a hard drive. The forensic copy is critical to preserve evidence at the point of request. The 4-43 process is in some ways similar to an *Anton Piller* order, in that it proceeds *ex parte* and carries with it an element of surprise.[2] In *Celanese Canada Inc. v. Murray Demolition Corp.,* [2006] 2 S.C.R. 189, Binnie J. observed at paragraph 32:

> Experience has shown that despite their draconian nature, there is a proper role for *Anton Piller* orders to ensure that unscrupulous defendants are not able to circumvent the court's processes by, on being forewarned, making relevant evidence disappear. Their usefulness is especially important in the modern era of heavy dependence on computer technology, where documents are easily deleted, moved or

[2] Rule 4-43 differs from the *Anton Piller* order in several important respects, including that it is an investigative step of a public authority whereas the *Anton Piller* order is an extraordinary process available to private litigants who stand in a qualitatively different relationship to each other than a lawyer does with the Law Society. Rule 4-43 does not require a strong *prima facie* case to be met for the order to issue, whereas an *Anton Piller* order does.

> destroyed. The utility of this equitable tool in the correct circumstances should not be diminished.

The observations regarding the utility and importance of a process to preserve records are equally applicable in the context of Rule 4-43.

Rule 4-43 orders are not common,[3] but they are an essential tool in the Society's investigative repertoire. The view of the majority was that preserving evidence of a discipline violation was essential, and that a process is required after copying to cull information that the Law Society should not be accessing. The Working Group recognized that current technology does not allow for forensic copying to occur in a manner that captures only records of the sort that may reveal a discipline violation. Part of the challenge is that often it takes weeks or months for the investigators to identify which information may be relevant. To have the investigator take over the lawyer's office and sift through computer records for weeks or months would be harmful to the lawyer's practice, and could open the door to the argument that the investigator altered the computer record through using the computer. Copying the record and letting the lawyer get on with his or her practice is less disruptive, and allows the lawyer under investigation to continue meeting the needs of his or her clients while the investigation is ongoing.

Some lawyers will conduct all their practice electronically, others will use a mix of computer and print records, and very few (if any) will eschew using computer technology altogether. Because there is not a uniform method of managing records, it is possible for some records to never be printed, some digital records will be well organized, and others not. In addition, a digital record can contain relevant information that is absent in the paper copy. The Working Group realized it was insufficient to simply view printed records as descriptive of the life of a file. In the past, some lawyers have backdated bills to cover improper taking from Trust. A print copy of the falsified bill or letter to the client will not reveal the misdeed, whereas the computer can contain information such as metadata that can reveal the breach of the Rules. Email is a critical part of an investigation, and often it will not be printed (or the print record will be incomplete). Sometimes the review of files in one complaint will lead the investigator to discover wrongdoing in other files. An overly restrictive reading of "record" can lead the investigator to miss critical information and would put the public at risk. The majority of the Working Group favoured the Benchers being able to modify the 4-43 process to make it clear forensic copying is permitted, and to establish a process to resolve disputes regarding access to information on the copied record. Sections 11 and 36 of the *Legal Profession Act* provide the Benchers with sufficient rule-making authority to deal with digital records.

The majority view was that when the threshold has been met for a 4-43 order to issue, it is critical to preserve the records at the point of request in order to protect the public. The majority recognized that this would likely involve copying personal information in

[3] From 2004-2008 there were a total of 46. Over that same period the Law Society received 7163 complaints about members (note: this does not include complaints against students).

circumstances where computer records are copied, but felt that spoke to the need for process safeguards to prevent improper access and use of such information, rather than speaking to the lack of authority to copy records necessary to prove a discipline violation has occurred.

Mr. Walker's preference was for the culling to occur before copying. Mr. Walker contended that Rule 4-43 allows for the copying of a limited category of records, but not the copying of records outside that category. Mr. Walker recognized the horns of the dilemma, however, and that a lawyer should not be able to prevent the Law Society from copying the sort of records he felt was contemplated by Rule 4-43. To resolve this dilemma, Mr. Walker favours an application to the court to authorize forensic copying and to establish the terms of accessing the record.

(b) Balancing rights under Rule 4-43

The Working Group spent a considerable amount of time testing assumptions and analysis to arrive at a fair approach to an intractable problem. On the one hand the Law Society has the statutory mandate to uphold and protect the public interest in the administration of justice and to regulate the practice of law. Sections 11 and 36 of the *Legal Profession Act* empower the Benchers to make a broad range of rules to fulfill the Society's mandate. The investigative function is a core aspect of a regulatory body, and the powers need to be robust to ensure the public is not at risk. On the other hand, lawyers are entitled to a reasonable expectation of privacy and the Society needs to establish processes that are not over-reaching. The Working Group strove to find the balance between protecting the public interest and preserving a reasonable privacy interest of lawyers. In doing so the Working Group was cognizant of the importance that the Act and Rules be read, to the extent possible, in a technology-neutral manner.

The Working Group assessed whether the copying power under Rule 4-43 would violate s. 8 of the *Charter.* In *British Columbia Securities Commission v. Branch*, [1995] 2 S.C.R. 3, 1995 the Court considered whether the investigative powers of the British Columbia Securities Commission violated ss. 7 and 8 of the *Charter*. In concluding the provisions did not offend the *Charter,* the Court made a series of observations that are relevant to the application of Rule 4-43 and the authority to make a forensic copy.

> In our opinion, persons involved in the business of trading securities do not have a high expectation of privacy with respect to regulatory needs that have been generally expressed in securities legislation. It is widely known and accepted that the industry is well regulated. Similarly, it is well known why the industry is so regulated. The appellants in this case were well aware of the dictates of the *Securities Act*. [at para. 58]
>
> Hence, the *Securities Act* is essentially a scheme of economic regulation which is designed to discourage detrimental forms of commercial

> behaviour. The provisions provided by the legislature are pragmatic sanctions designed to induce compliance with the Act. After all, the Act is really aimed at regulating certain facets of the economy and business. This has obvious implications for the nation's material prosperity: *Thomson Newspapers.* As such, the effective implementation of securities legislation depends on the willingness of those who choose to engage in the securities trade to comply with the defined standards of conduct. In this respect, we fully agree with Wilson J.'s comments that "[a]t some point the individual's interest in privacy must give way to the broader state interest in having the information or document disclosed": *Thomson Newspapers*, at p. 495. [at para. 59]

Similarly, the Law Society regulates lawyers to protect the public interest in the administration of justice. Lawyers know their records may be subject to inspection by the Society, and cannot frustrate the authority of the Society to investigate their records by a mere assertion that their computer contains personal information.

Although *Branch* provides a strong precedent in support of the investigative powers of the Society, the Working Group was cognizant of the fact that the Court did not appear to consider that computer records commingle business and personal records.[4] The Working Group tried to assess how the issue would be reconciled today, including whether a lawyer's subjective expectation of privacy would remain objectively reasonable when the lawyer stored personal information on a record he or she knew could be subject to inspection by the Society. The Working Group concluded that a lawyer makes a choice to use a computer for both business and personal purposes, and that choice cannot prevent the Society from copying the records it requires to discharge its statutory duty. The Working Group believes, however, that there is a distinction between copying a record and access to the record, and that a process is necessary to ensure the Society is not improperly accessing information over which a lawyer rightly asserts a privacy interest. The Working Group believes this represents the middle ground between the Society accessing everything and accessing nothing.

(c) Process safeguards

The Working Group considered a number of process safeguards to prevent the Law Society from accessing personal information that is not relevant to an investigation.

Section 88 of the *Legal Profession Act* sets out safeguards regarding confidential and privileged information:

[4] The Court in *Branch* noted a distinction between business and personal records (para. 62).

> 88 (1) A lawyer who, in accordance with this Act and the rules, provides the society with any information, files or records that are confidential, or subject to a solicitor client privilege, is deemed conclusively not to have breached any duty or obligation that would otherwise have been owed to the society or the client not to disclose the information, files or records.
>
> (2) Despite section 14 of the Freedom of Information and Protection of Privacy Act, a person who, in the course of carrying out duties under this Act, acquires information, files or records that are confidential or are subject to solicitor client privilege has the same obligation respecting the disclosure of that information as the person from whom the information, files or records were obtained.
>
> (3) A person who, during the course of an investigation, audit, inquiry or hearing under this Act, acquires information or records that are confidential or subject to solicitor client privilege must not disclose that information or those records to any person except for a purpose contemplated by this Act or the rules.

These provisions afford a level of protection regarding confidential and privileged information.

The Working Group considered that there are technological safeguards associated with making a forensic copy. Forensic copying makes a bit-stream image of a hard drive, resulting in a perfect copy of the record. The copy is incomprehensible until it is reconstructed using special programs. Although not a perfect analogy it would be similar to copying all the paper in an office, but the copied paper becomes covered in incomprehensible symbols until it is run through a second machine that reconstructs the information into a comprehensible form. What this suggested to the Working Group was that as long as the Law Society does not possess the forensic copy and the hardware and software necessary to reconstruct the information, there is a technological firewall between the information the lawyer may seek to protect and Law Society access.

The concept of a firewall is borne out in similar processes where forensic copying occurs in court cases. The best examples are found in *Anton Piller* orders. In *Anton Piller* cases where forensic copying occurs, the copied records will be in the possession of a forensic expert, and then in the hands of an independent supervising solicitor. This process creates a firewall between the record and the person seeking access to the information stored on the record. The Working Group considered that, failing being able to arrive at an agreement with the lawyer as to the scope of access to the record, using an independent supervising solicitor would provide a mechanism where the Law Society could indicate to the lawyer under investigation, and to his or her counsel, the search parameters the Society intended to use (which in most cases will include all practice

records), and any objections could be worked out between counsel and through the independent supervising solicitor. The Society would then be provided copies of the information it was permitted to access, while not accessing that information the independent solicitor deems inappropriate. In this context inappropriate material would include personal information that is not relevant to the alleged discipline violation, and also legal advice given to the lawyer regarding a Law Society investigation over which solicitor-client privilege is claimed. General matters of solicitor-client privilege and confidentiality will be protected by s. 88 of the *Legal Profession Act.*

The Working Group also considered how to improve the fairness of the process of using a supervising solicitor. The Working Group felt it was important to construct a process where decisions of the supervising solicitor regarding access could be reviewed. For such a process to be functional, it is important that it be an expedited process and not one that creates delay through a series of appeals. At first the Working Group considered whether a chambers Bencher could be appointed to review decisions of the supervising solicitor. While this would have met the requirements of an expedited process, the Working Group had concerns that the supervising solicitor must be independent and appear to be independent, and having a Bencher review decisions of the supervising solicitor could compromise the appearance of independence. The Working Group also felt that the review should include the ability to review the decision of the supervising solicitor on the merits. While a reviewing Bencher could make determinations on the merits, the Working Group was concerned that judicial review of that decision would be limited. In order to test their concerns, and determine what process would best meet the needs of an independent, expedited review on the merits the Working Group sought the opinion of outside counsel.

The opinion of outside counsel confirmed the view that a Bencher review process would compromise the appearance of independence of the independent supervising solicitor. Outside counsel suggested concerns about independence would be addressed by appointing a retired judge as a Review Commissioner to hear these reviews on the rare occasion they arise. The opinion noted that this would be analogous to s. 60.1 of the *Police Act,* RSBC 1998, c. 367:

> 60.1(2) If the police complaint commissioner arranges a public hearing under section 60 or orders a public hearing under section 64 (7),
>
> > (a) the police complaint commissioner must appoint a retired judge of the Provincial Court, the Supreme Court or the Court of Appeal to preside as an adjudicator at the public hearing

Under the proposed system, the retired judge could make a determination on the merits. If the Benchers wish for a right of appeal to the court from the decision of the retired judge, the *Legal Profession Act* would have to be amended. Failing amending the

Act, only judicial review would be possible, and both sides have the right to judicial review. The Working Group believes an amendment of the Act to allow for an appeal to the court of the retired judge's decision is not required. The proposed method allows for considerable input by the member and his or her counsel along the way, and carries the safeguard of a determination by an independent supervising solicitor and a right to review on the merits by a retired judge. Based on the opinion, and their own consideration of the issue, the Working Group believes this adequately meets the needs of procedural fairness and is a practical solution to the need to balance the investigative authority of the society with the reasonable expectation of privacy of a member who is subject to a 4-43 order.

(d) Establishing a positive duty to preserve records in circumstances where a lawyer refuses to comply with a 4-43 order.

The Working Group believes there is merit in creating a Rule that requires a lawyer who refuses to comply with a 4-43 order to be under a positive obligation to preserve records. The recently revised *Nova Scotia Civil Procedure Rules* provide in Rule 16.02:

> (2)A party who becomes aware that a proceeding is to be defended or contested, must take measures to preserve relevant electronic information that is of one of the following kinds:
>
> > (a) it is readily identifiable in a computer, or on a storage medium, the party actually possesses;
> > (b) it is accessible by the party to the exclusion of another party, such as information in a database the party accesses by password on a computer the party does not actually possess.

Rule 16.02(2) reflects an effort to modernize court rules to deal with the risks attendant in computer records and digital storage media. Creating a similar obligation in the Law Society Rules would reduce the risk of necessary records being destroyed, and provide a further safeguard to the public.

Although the Law Society could draw a negative inference from the destruction of records that takes place subsequent to the lawyer being provided the 4-43 order, a positive duty to preserve the records better protects the public. The Working Group believes the absence of such a rule presents a troubling gap that should be closed. Unlike the Nova Scotia rule, however, the Working Group believes the duty should apply to both digital and non-digital records. The Working Group recommends that the Benchers either direct the Act and Rules Subcommittee to create such a rule, or if the Benchers believe further policy analysis is required prior to creating such a rule, to refer the matter to the Discipline Committee or another group for further policy development.

(e) Should there be two Rule 4-43 processes?

In an effort to arrive at a process that is fair and transparent, the Working Group considered a number of options, including whether there should be a single 4-43 process that deals with all records, or two 4-43 processes: one that contemplates all records being copied, and one that only contemplates non-digital records being copied. The Working Group tried to balance the importance of the issuing Bencher considering the potential for forensic copying to occur with the fact that the Bencher should be deciding to issue the order on the basis of whether the threshold for a 4-43 order has been met, not based on whether the records being copied are non-digital or digital. The Working Group rejected the idea of staff seeking a general order and then, if circumstances suggest a need to copy computer records, seeking a digital order. The Working Group concluded that the application for a 4-43 order should be a single process, but one that includes in it the step of alerting the issuing Bencher that forensic copying will likely occur, thereby requiring the Bencher to turn his or her mind to the possibility (perhaps by ticking a check box). The order should indicate that staff may make forensic copies.

(f) The majority process for Rule 4-43

The majority of the Working Group recommends that rules and policies be created to give effect to the following process for 4-43 orders. It is important to note that the decision to make a forensic copy is an investigative decision, and not the basis on which a 4-43 order should be granted or refused. The purpose for providing the issuing Bencher a copy of the process is to allow the Bencher to better understand the safeguards in the investigative process, not to affect whether or not a 4-43 order should issue.

1. When staff apply for a 4-43 order they should indicate forensic copying is likely to occur, and the issuing Bencher should acknowledge in the order that forensic copying may occur.

2. In order to minimize the chance of the Law Society accessing personal information that is not relevant to a 4-43 investigation, the Law Society should not be the custodian of the forensic copies. For greater clarity, this does not limit the ability of the Society to retain and access records that have been culled from the forensic copies.

3. The investigators present the 4-43 order and covering letter to the lawyer. This information establishes that the lawyer must allow copying of records at the point of request, including making a forensic copy. The lawyer is provided a document setting out the process for how forensic copies are dealt with.

4. The lawyer is encouraged to instruct counsel.

5. If the lawyer refuses to comply with the 4-43 order:

    a. The lawyer is informed of his or her obligation to preserve records [**note:** this is predicated on such a rule being created];

    b. Staff determine whether to apply to court pursuant to s. 37 of the Act for an order to seize records.

6. If the lawyer complies with the 4-43 order the following process ensues:

    a. Two forensic copies are made. One copy is to be preserved as a best evidence copy and the other copy is the working copy from which information is abstracted.

    b. It is contemplated that the forensic expert may have to hold on to the forensic copies until agreement can be reached for a third party to hold on to the copies, or until the independent supervising solicitor is appointed.

    c. Staff will attempt to reach an agreement with the member regarding retention and the terms of access to the forensic copies, and if staff and the member cannot agree to the terms of access:

        i. The member will be provided a list of Law Society approved independent supervising solicitors to choose from to resolve the disputes as to access. If the member does not agree to anyone on the list, the President may appoint an independent supervising solicitor.

    d. In circumstances where staff and the member agree to access parameters, the forensic copies will be held by the person agreed upon (e.g. the forensic expert, counsel for the member, etc.).

    e. In circumstances where an independent supervising solicitor has been appointed, the forensic copies will be held by the supervising solicitor.

    f. If an independent supervising solicitor is appointed, the solicitor will perform a function similar to such a solicitor in *Anton Piller* applications. In circumstances where the lawyer and the Law Society cannot agree as to the scope of access to the computer record, the independent supervising solicitor will determine the scope of access. The process should require that:

        i. The lawyer and his or her counsel are advised in writing of the search parameters, which in most cases will include all practice records, prior to the LSBC obtaining copies of the information

abstracted from the forensic copies. The lawyer is provided a reasonable period of time to object in writing to the scope of the search. The independent supervising solicitor will consider the objection prior to disclosing the information to the Law Society, and after the period of time allowed for a review will provide the information to the Law Society.

ii. If there is a dispute as to the decision of the independent supervising solicitor regarding access to the forensic copy, either the member or the Society may seek a review on the merits of the decision of the independent supervising solicitor.

iii. The Law Society will appoint a retired judge to conduct reviews of the decision of the independent supervising solicitor as contemplated in 6(f)(ii). The retired judge may review the decision of the independent supervising solicitor as to jurisdiction and on the merits, and may affirm or alter decisions as to the scope of access to the forensic copies in order to balance the investigative authority of the Society with a member's reasonable expectation of privacy in information contained in the forensic copy.

iv. Following the passage of the time allowed for objecting to the search parameters, the information from the search is provided to the investigators.

g. If the investigators later require additional search parameters the process is repeated.

h. Records retention issues should be dealt with as follows:

i. If the investigation results in a disposition by the Benchers the member has 60 days from the day on which the final appeal period from disposition expires to make a request in writing to the Society for the return of the forensic copies. In circumstances where the member fails to make the application in time the Society may destroy the forensic copies or return them to the member as it sees fit;

ii. If the investigation is closed the member has 60 days from the date of notice from the Society that the investigation is closed to make a request in writing to the Society for the return of the forensic copies. In circumstances where the member fails to make the application in time the Society may destroy the forensic copies or return them to the member as it sees fit;

iii. If the member voluntarily resigns, retires, ceases practice, or goes on non-practising status prior to conclusion of the investigation or disposition of any proceeding resulting from the investigation, the Society will advise the member that the Society will maintain the forensic copies as the Society may require them in the event the member reapplies for admission; and

iv. The Working Group recommends that the Law Society ensure that:

1. its records retention policy establish a process for dealing with records that are culled from the forensic copies and that have been provided to the Society; and

2. its records retention policy establishes a process for dealing with forensic copies it retains in circumstances identified in 6(h)(iii) above.

(g) The minority process for Rule 4-43

The process suggested by Mr. Walker differs from that of the majority in the following respect. Mr. Walker believes the process should be resolved through an application to the Court pursuant to s. 37 of the Act, but where the judge makes determinations regarding copying records and the scope of access, rather than seizure. Mr. Walker's preference would be for the Act and Rules Subcommittee to determine whether s. 37 needs to be modified to accommodate this approach. Mr. Walker believes, due to the privacy rights implicated by the copying of digital records, the court is the better body to authorize the copying of such records and the terms of access.

During its discussion of this approach, the majority of the Working Group expressed concern that abdicating to the court an authority they believe lies with the Benchers could have a negative impact on the independence and self-governance of the profession. In the event the Benchers endorse the minority process, the majority of the Working Group believes that the Act and Rules Subcommittee should consider this issue as part of such a review.

(h) Custodians

The language for the custodian powers illustrates the interpretive challenges involved in making a forensic copy. The custodian is allowed to deal with records that are "reasonably necessary" to carrying out the custodianship. A hard drive is a record that will be reasonably necessary, and it will contain records that are reasonably necessary, yet it will also contain records that are not reasonably necessary. The Working Group

considered that the custodian stands in a unique position in that the custodian can take possession of the lawyer's property to manage the practice, but can also investigate the practice. These broad powers, coupled with the originating authority of the custodian as an appointee of the court, favour the ability of the custodian to make a forensic copy of the hard drive.

The Working Group believes any ambiguity is best dealt with by making it a standard procedure to have the court order appointing the custodian clearly state that the custodian has the power to deal with and copy digital records. While the Law Society is well positioned to argue it already has this authority, setting it out in the court order provides clarity.

Because a custodian can have the dual roles of managing the lawyer's practice and investigating the lawyer's practice, the Law Society should require forensic copying to take place at the beginning of the custodianship. The reason for this is that if the custodian uses the lawyer's computer to manage the practice, the lawyer might argue that the forensic integrity of the hard drive has been compromised since the lawyer last used it. If the hard drive were to be relied on as a piece of evidence, this might cause unanticipated problems. Making a forensic copy at the commencement of the custodianship protects against this risk by preserving a record of the hard drive. As with the 4-43 process, the Working Group believes two forensic copies should be made in order that one can be used as a working copy if an investigation is required, and the other preserved as evidence of the computer records on the date the custodial order issued.

The Working Group also noted that s. 52 of the *Legal Profession Act* predates the in-house custodian program, and recommend that Mr. Hoskins and Mr. Keirstead consider the application of that section to the in-house program, as well as whether there may be circumstances where the original property is required and not merely a copy.

(i) Third party contractors

The *Freedom of Information and Protection of Privacy Act,* R.S.B.C. 1996, c. 165 ("FIPPA") governs the Law Society's collection, use and disclosure of personal information. When the Law Society retains third parties to provide services and those parties obtain custody of personal information as an incident of providing those services, it is necessary for the third parties in dealing with that personal information to adhere to the standards of protection expected of the Law Society and required by privacy legislation. The Law Society uses a forensic expert to make forensic copy of hard drives. That expert will have custody over hard drives that contain personal information. In light of this, the Working Group recommended to the Executive Committee that the Law Society retain counsel with experience in this area to draft a schedule to contracts the Law Society has with its forensic expert, and other service providers, to ensure those service providers adhere to the standards required by FIPPA.

The Audit and Investigation department has put the schedule in place with its external forensic expert and auditors.

(j) Encryption

Encryption technology creates a loophole in the Law Society Rules. It is possible to make a forensic copy of an encrypted hard drive, but the forensic copy will also be encrypted. The encrypted data is a record, and allowing for its copying would amount to technical compliance with the Rules. However, commercially available encryption technology is powerful enough that the Law Society would not be able to decrypt the record. In other words, a literal application of the rule has the potential to frustrate the spirit of the rule because of how computer technology works.

It is possible a lawyer would allow for the encrypted hard drive to be copied, but refuse to provide the password or decryption key, and argue that he or she has complied with the rules (Rule 4-43 requires the lawyer to provide explanations, whereas the custodian rules require the lawyer to cooperate). The Working Group is unable to forecast the likelihood of this risk occurring, but note that if it did occur it presents a litigation risk and carries the attendant risks associated with the Law Society not being able to access the required data in a comprehensible form. The Law Society encourages the use of encryption technology to safeguard client information, yet that technology can frustrate the ability of the Law Society to carry out its regulatory function. The Working Group concluded that this loophole creates an unnecessary risk (however remote) and that the Law Society Rules should be amended to require lawyers to provide the necessary information, including decryption keys and passwords, to allow the Law Society to access records in a comprehensible form. Section 36(d) of the *Legal Profession Act* empowers the Benchers to make rules to "require a lawyer to cooperate with an investigation or examination under paragraph (b) or (c), including producing records and other evidence and providing explanations on request." This section provides the authority for creating such a rule.

(k) Special Cases

When the Executive Committee discussed the topic of forensic copying, and decided to strike a working group to explore the policy issues arising from it, the question arose as to what happens when the investigator uncovers material on the hard drive that doesn't relate to the investigation, but might be evidence of a crime or wrongdoing. The answer to this depends on the nature of the information that is uncovered, and the reasonable apprehension of the investigator as to whether the information may constitute a discipline violation, or a matter that needs to be reported to another authority.

The Law Society Rules, Rule 3-4 states:

> (2) Information received from any source that indicates that a lawyer's conduct may constitute a discipline violation must be treated as a complaint under these Rules.

As previously noted a "discipline violation" is defined in the Law Society Rules. "Conduct unbecoming a lawyer" includes any matter, conduct or thing considered by the Benchers or a panel:

> (a) to be contrary to the best interest of the public or the legal profession, or
> (b) to harm the standing of the legal profession.

The foregoing suggests the nature of the material will dictate how it is to be treated. The Working Group considered the following examples as guidelines for how this issue would likely be dealt with if it arose.

> **Scenario 1:** Lawyer A and Lawyer B are partners. While investigating a complaint against Lawyer A, the Law Society uncovers material on the law firm's computers that suggest Lawyer B is engaged in real estate fraud. In this scenario, the Law Society has uncovered information that may constitute a discipline violation, and it must be treated as a complaint. The circumstances of how it was uncovered don't protect Lawyer B.

> **Scenario 2:** While reviewing the content of Lawyer C's computer, the Law Society investigator notes that there are approximately 1,200 songs stored in Lawyer C's "my music" folder. While the songs may have been copied in violation of copyright law, it is unlikely that a threshold test has been met to argue that a discipline violation may have occurred, or that a crime has been committed. While violating the law is clearly not in the best interest of the public or the legal profession, the mere presence of the songs do not provide compelling evidence that the lawyer is uploading copies of the songs online, or making them available for file sharing.

> **Scenario 3:** While reviewing the content of Lawyer D's computer the Law Society investigator uncovers several hundred images of child pornography. In this situation the investigator has uncovered material that is illegal on its face, and clearly constitutes a discipline violation. The material will also trigger obligations under various laws such as the *Child, Family and Community Service Act,* RSBC 1996, Chapter 46, ss. 13&14. Scenario 3 triggers an obligation to treat the content as a complaint, and

an obligation to report the matter to an external authority. The Law Society would be able to determine the few instances in which s. 14(2)(a) applied to prohibit the Law Society from providing the information to an external authority. Arguably, it would be extremely rare for child pornography stored on a lawyer's computer to be information to which solicitor client privilege attaches.

(l) Education & Communication

Throughout its discussions the Working Group considered the importance of proper education and communication about computer technology. In particular, the Working Group believes that articled students and lawyers need to be reminded that the Law Society has the responsibility to govern the profession in order to protect the public interest, and that mandate empowers the Society to investigate and copy records relating to a lawyer's practice, including digital records.

Articling students and lawyers need to be reminded as part of PLTC, continuing legal education, legal technology conferences, practice standards checklists, notices to the profession and educational resources such as the Small Firm Practice Course, that the Law Society may access a lawyer's computer and copy the hard drive. These education and communication pieces provide an opportunity to remind lawyers about their obligations to safeguard the confidentiality of client information and practical steps, such as partitioning hard drives on computers that are used for both work and personal purposes, securing access to the work-related content through passwords and encryption, etc. Lawyers and articling students should be advised that the mere use of a computer for both work and personal purposes does not prevent the Law Society from copying the content of the computer's hard drive.

The education and communication pieces should recommend that lawyers use, to the extent *reasonably* possible, a separate computer for personal and work purposes, and in circumstances where another person has access to the lawyer's computer that the lawyer has a professional obligation to partition and password protect confidential and privileged information so that other user cannot access it.

(m) Ethical considerations

The Working Group discussed whether the issue of forensic copying was one that might best be dealt with through amendments to the *Professional Conduct Handbook.* The Working Group concluded that the authority to copy records is not a matter of ethics, and is best dealt through the Act and Rules. However, the Working Group recognized that any policies or education pieces that are created might appropriately contain observations relating to a lawyer's ethical obligations and as such the Benchers may wish to refer such documents to the Ethics Committee for input.

(n) Matters for future consideration

In the course of its analysis the Working Group identified several issues that fall into the category of matters for future consideration. Some of these matters relate to the potential requirement to amend the *Legal Profession Act.* While the Working Group is of the view that the issues relating to computer technology and interpretation of the Act will become more prevalent as more practices move to a paperless office, it believes the recommendations in this report relating to rule reform and policy development are adequate measures until proper consideration can be given to whether the Act needs to be amended. As such, the Working Group recommends that Mr. Hoskins consider as part of the next revision of the *Legal Profession Act* what changes should be made to better accommodate the application of the Act in light of computer technology.

When the Working Group first reported to the Benchers that the *Legal Profession Act* and Law Society Rules should be reviewed periodically to ensure they remain current with technology, they did so on the basis forensic copying identified a need for such review. At the Benchers meeting David Zacks, Q.C. asked whether forensic copying would be a short-lived problem because of cloud computing and similar evolutions in technology could mean lawyers were storing their data remote servers. Cloud computing highlights the need for the sort of review the Working Group proposed.

Law Society Rules, Rule 3-68 reads:

> 3-68 (0.1) In this Rule, "records" means the records referred to in Rules 3-60 to 3-62.
>
> (1) A lawyer must keep his or her records for as long as the records apply to money held in trust and, in any case, for at least 10 years.
>
> (2) A lawyer must keep his or her records at his or her chief place of practice in British Columbia for as long as the records apply to money held in trust and, in any case, for at least 3 years.
>
> (3) A lawyer must protect his or her records and the information contained in them by making reasonable security arrangements against all risks of loss, destruction and unauthorized access, use or disclosure.
>
> (4) A lawyer who loses custody or control of his or her records for any reasons must immediately notify the Executive Director in writing of all the relevant circumstances.

Lawyers who use cloud computing will be in breach of Rules 3-68(2) and (3) because the servers storing their data will not be at the lawyers' chief place of practice in British Columbia (the servers may be outside the jurisdictional reach of the Society, which creates additional problems), and the lawyers may be unable to take reasonable

security arrangements against all the identified risks. Beyond cloud computing, however, Rule 3-68 demonstrates the sort of unintended consequence of defining records to include computer records, as many lawyers may be storing these records on servers outside their chief place of practice in British Columbia. With respect to computer records the more critical question may be that the records are accessible on request, stored within the jurisdictional reach of the Society, and subject to verifiable security safeguards. This is an issue the Benchers may wish to refer to the Act and Rules Subcommittee for consideration.

4. CONCLUSION

Computer technology pervades our personal and professional lives. The early efforts by legislators to address this technology involved changing the legislative definition of "records" to include electronic storage devices such as hard drives. This has led to a considerable amount of litigation, in part because a computer record is qualitatively different than a paper record. The technology works in a manner that creates unintended consequences and complicates the task of interpreting the law. Not surprisingly, the areas of intellectual property and privacy are at the forefront of disputes because of the unprecedented capacity of the technology to copy and disseminate information.

Because the Law Society governs the profession in order to protect the public interest, it is important to ensure the Society's regulatory mechanisms are current. The Working Group's review of the Act and Rules reveal that the Law Society should take steps to modernize its Rules in order to account for computer technology. While processes that have been developed in other contexts are informative, it is appropriate for the Law Society to develop a customized approach in the regulatory context.

While it is essential that the regulatory capacity of the Law Society not be hindered by evolutions in technology, it is also important for the Society to identify unintended consequences that arise from the use of such technology. In the case of making a forensic copy of a hard drive, an unintended consequence is that the act of copying the hard drive will, of necessity, include the copying of records the Law Society does not need to access in order to fulfill its regulatory function. At present there are insufficient rules and policies to make it clear the Law Society can copy a lawyer's digital records, while providing a mechanism for the lawyer to have personal information appropriately protected. The Working Group believes the following recommendations achieve the object of ensuring the Law Society's regulatory function remains robust, while providing mechanisms to protect a reasonable expectation of privacy of its members.

5. RECOMMENDATIONS

Recommendation 1:

Note: In Recommendation 1 the Benchers are asked to choose between Option A (the majority option) and Option B (the minority option).

Option A:

Rules and policies should be created that facilitate the Society's ability to inspect and copy digital records, while maintaining a reasonable expectation of privacy its members have in personal information contained in such records. Staff, working with the Act and Rules Subcommittee will identify which of the steps below are best set out in a new Rule 4-43, and which are best set out in a 4-43 policy and procedure document. In most cases the investigative search parameters will include all practice records. The new Rule 4-43 and attendant policies and procedure should reflect the following:

1. When staff apply for a 4-43 order they should indicate forensic copying is likely to occur, and the issuing Bencher should acknowledge in the order that forensic copying may occur.

2. In order to minimize the chance of the Law Society accessing personal information that is not relevant to a 4-43 investigation, the Law Society should not be the custodian of the forensic copies. For greater clarity, this does not limit the ability of the Society to retain and access records that have been culled from the forensic copies.

3. The investigators present the 4-43 order and covering letter to the lawyer. This information establishes that the lawyer must allow copying of records at the point of request, including making a forensic copy. The lawyer is provided a document setting out the process for how forensic copies are dealt with.

4. The lawyer is encouraged to instruct counsel.

5. If the lawyer refuses to comply with the 4-43 order:

    a. The lawyer is informed of his or her obligation to preserve records [**note:** this is predicated on such a rule being created];

    b. Staff determine whether to apply to court pursuant to s. 37 of the Act for an order to seize records.

6. If the lawyer complies with the 4-43 order the following process ensues:

a. Two forensic copies are made. One copy is to be preserved as a best evidence copy and the other copy is the working copy from which information is abstracted.

b. It is contemplated that the forensic expert may have to hold on to the forensic copies until agreement can be reached for a third party to hold on to the copies, or until the independent supervising solicitor is appointed.

c. Staff will attempt to reach an agreement with the member regarding retention and the terms of access to the forensic copies, and if staff and the member cannot agree to the terms of access:

    i. The member will be provided a list of Law Society approved independent supervising solicitors to choose from to resolve the disputes as to access. If the member does not agree to anyone on the list, the President may appoint an independent supervising solicitor.

d. In circumstances where staff and the member agree to access parameters, the forensic copies will be held by the person agreed upon (e.g. the forensic expert, counsel for the member, etc.).

e. In circumstances where an independent supervising solicitor has been appointed, the forensic copies will be held by the supervising solicitor.

f. If an independent supervising solicitor is appointed, the solicitor will perform a function similar to such a solicitor in *Anton Piller* applications. In circumstances where the lawyer and the Law Society cannot agree as to the scope of access to the computer record, the independent supervising solicitor will determine the scope of access. The process should require that:

    i. The lawyer and his or her counsel are advised in writing of the search parameters, which in most cases will include all practice records, prior to the LSBC obtaining copies of the information abstracted from the forensic copies. The lawyer is provided a reasonable period of time to object in writing to the scope of the search. The independent supervising solicitor will consider the objection prior to disclosing the information to the Law Society, and after the period of time allowed for a review will provide the information to the Law Society.

    ii. If there is a dispute as to the decision of the independent supervising solicitor regarding access to the forensic copy, either the member or the Society may seek a review on the merits of the decision of the independent supervising solicitor.

iii. The Law Society will appoint a retired judge to conduct reviews of the decision of the independent supervising solicitor as contemplated in 6(f)(ii). The retired judge may review the decision of the independent supervising solicitor as to jurisdiction and on the merits, and may affirm or alter decisions as to the scope of access to the forensic copies in order to balance the investigative authority of the Society with a member's reasonable expectation of privacy in information contained in the forensic copy.

iv. Following the passage of the time allowed for objecting to the search parameters, the information from the search is provided to the investigators.

g. If the investigators later require additional search parameters the process is repeated.

h. Records retention issues should be dealt with as follows:

i. If the investigation results in a disposition by the Benchers the member has 60 days from the day on which the final appeal period from disposition expires to make a request in writing to the Society for the return of the forensic copies. In circumstances where the member fails to make the application in time the Society may destroy the forensic copies or return them to the member as it sees fit;

ii. If the investigation is closed the member has 60 days from the date of notice from the Society that the investigation is closed to make a request in writing to the Society for the return of the forensic copies. In circumstances where the member fails to make the application in time the Society may destroy the forensic copies or return them to the member as it sees fit;

iii. If the member voluntarily resigns, retires, ceases practice, or goes on non-practising status prior to conclusion of the investigation or disposition of any proceeding resulting from the investigation, the Society will advise the member that the Society will maintain the forensic copies as the Society may require them in the event the member reapplies for admission; and

iv. The Working Group recommends that the Law Society ensure that:

1. its records retention policy establish a process for dealing with records that are culled from the forensic copies and that have been provided to the Society; and

2. its records retention policy establishes a process for dealing with forensic copies it retains in circumstances identified in 6(h)(iii) above.

Option B:

Because of the privacy concerns implicated in forensic copying, the authority of the Society to make forensic copies should be determined by the Court pursuant to s. 37 of the *Legal Profession Act.* The Act and Rules Subcommittee should determine whether s. 37 allows for forensic copying, or if the section should be amended to give the Court the authority to set out the terms on which the Society may copy and access computer records. As part of this review the Act and Rules Subcommittee should consider whether this has any implications for the independent, self-governing status of the profession.

Recommendation 2:

When a member refuses to immediately allow copying of records under a 4-43 order, it places those records at risk of destruction. In light of this the Benchers should either:

1. Direct the Act and Rules Subcommittee to create a rule that requires a lawyer who refuses to comply with a 4-43 order to preserve records as they existed at the time the order was presented to the member; or
2. Instruct the Discipline Committee, or another group, to engage in further analysis of this issue prior to determining whether to create such a rule.

Recommendation 3:

When seeking an order appointing a custodian, the Law Society should as a matter of practice request that the order contain language that identifies the Law Society's authority to make a copy of any storage devices in the lawyer's possession or control that the Law Society has reason to believe contains information related to the lawyer's practice.

Recommendation 4:

The Law Society should ensure that two forensic copies are made at the commencement of a custodianship in order to preserve the forensic integrity of the records in the event the custodian needs to investigate the lawyer's practice.

Recommendation 5:

Because s. 52 of the *Legal Profession Act* pre-dates the in-house custodian program, staff should consider how the section relates to that program. Consideration should also be given, as part of any amendments to the Act, whether there may be circumstances in which it is desirable to have access to the original property and not merely a copy of it.

Recommendation 6:

The Law Society Rules should be amended to require a lawyer to provide the Law Society with the necessary information, including passwords and encryption keys, for the Law Society to access, in a comprehensible form, records in the lawyer's possession or control that the Law Society has reason to believe contain information related to the lawyer's practice.

Recommendation 7:

Lawyers and articling students should be reminded through Law Society communications, practice standards checklists, the Small Firm Practice Course, PLTC, CLE and legal technology conferences, that the Law Society has the authority to inspect and copy computer records, and that articling students and lawyers should take precautions to segregate the storage of work records from personal records, by methods such as partitioning hard drives. These education and communication tools should also be used to remind articling students and lawyers of their obligation to safeguard confidential client information, including preventing unauthorized access to their client's records.

Recommendation 8:

The Act and Rules Subcommittee, as part of any future revision to the *Legal Profession Act*, and as a regular review of the Law Society Rules, should consider whether any amendments are required to avoid mischief caused by technology (e.g. the storage of accounting records on servers that fall outside the scope of Rule 3-68).

Recommendation 9:

The Society should liaise with the Office of the Information and Privacy Commissioner to see if they have any concerns with the policies and procedures being created to copy and access digital records. Staff should inform the Executive Committee of the results of these communications.