Technology and Confidentiality

Technology plays a significant role in the legal profession. Because technology has become a part of the everyday practice for attorneys, it is impossible to escape the need to know the issues and benefits surrounding technology.\(^1\) It is a difficult task for attorneys to keep informed about the issues and benefits of technology when technology is constantly changing. The ABA Commission on Ethics 20/20 sought to address the issues regarding technology and confidentiality, among others, in their recent proposal to the ABA Model Rules of Professional Conduct.

The mission of the ABA Commission on Ethics 20/20 (Commission) was to research the “impact of technology and globalization on the legal profession” and to determine what, if any, changes the legal profession needed to make in order to respond to this increasing globalization and use of technology.\(^2\) The Commission spoke with lawyers, clients, and consumer groups and businesses related to the profession in order to compile their recommendations to the ABA Model Rules of Professional Conduct.\(^3\) Relevant to this paper’s topic of technology and confidentiality, the Commission determined that legal advice and communication are often accomplished

---


\(^2\) Letter from Jamie S. Gorelick and Michael Traynor, Co-Chairs ABA Comm’n on Ethics 20/20, to ABA Entities, Courts, Bar Assoc. (state, local, specialty and international), Law Schools, and Individuals (Dec. 28, 2011) (on file with author).

\(^3\) *Id.*
through technology. Additionally, the Commission determined that confidential client information is often kept on technological devices such as laptops and phones.

Following its thorough research, the Commission recommends amending language in Comment nine of Rule 1.0, Terminology, regarding the term “Screened.” Under the recommended rule, “materials” would to be changed to “information, including information in electronic form.” The effect of this amendment is to make it clearer that the screened lawyer is not to have any contact with any information, including electronic information, related to the screened matter or client. The rationale behind this recommendation is the increasingly easy access a lawyer within the firm has to documents and other case related information through the firm’s computer system.

This recommendation addresses concerns regarding lawyers within the firm who must be screened from a particular matter or client. However, clients may also have concerns regarding lawyers within the firm who do not need to be screened from the client’s case, but who nevertheless have no need to access the client’s confidential case information. This issue most commonly arises in the context of large firms with multiple departments. For example, a lawyer in the intellectual property department of the firm does not need to have access to all of the cases handled by the insurance

---

4 Id.
5 Id.
6 ABA Comm’n on Ethics 20/20, Revised Draft Resolutions for Comment—Tech. and Confidentiality (Feb. 21, 2012).
8 See Id.
9 Ann Ostrander, Safeguarding Confidentiality: Ensuring Your Technology, Policies and Practices Protect Sensitive Client and Firm Information, http://www.cnapro.com/pdf/SafeguardingConfidentiality(Ann%20Ostrander%20Kirkland%20Ellis%20LLP).pdf (last visited Apr. 10, 2012) (“Increasingly, clients want to restrict who within the firm is able to access their sensitive business information. Examples might include IP matters, strategic or financial matters of significant import or implication, or high-profile entities or individuals with sensitivities about the potential for public disclosure.”).
department of the firm. Additionally, the same rationale behind the proposed rule on screening, that lawyers within the firm have easy access to documents and case information through the firm’s computer system, applies to the internal situation of a large firm as well. Therefore, the model rules and or comments should offer some guidance on limiting access to client information within a firm in order to increase the security of client confidentiality. Some suggested practical solutions for the firm to limit internal access to client information include “defined matter team only’ access and other tracking and reporting obligations.”\textsuperscript{10} The Commission should have addressed this issue in their recommendations.

The Commission also recommends a change to Comment six of Rule 1.1, Competence, mandating a lawyer’s duty to maintain competence. The current rule states that “[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of the changes in the law and its practice” and engage in continuing education.\textsuperscript{11} The Commission recommends inserting “including the benefits and risks associated with technology.”\textsuperscript{12} As examples, the Commission lists knowing how to use e-mail and how to create and edit an electronic document as being necessary skills in order to provide competent representation.\textsuperscript{13}

This amendment is important because it clarifies lawyers’ duties to remain competent with respect to technology. However, the examples provided by the Commission are extremely basic and are of general common knowledge at this point in

\textsuperscript{10} \textit{Id.}

\textsuperscript{11} \textsc{Model Rules of Prof’l Conduct R. 1.1} (2006).

\textsuperscript{12} ABA Comm’n on Ethics 20/20, Revised Draft Resolutions for Comment—Tech. and Confidentiality (Feb. 21, 2012).

\textsuperscript{13} ABA Comm’n on Ethics 20/20, Revised Draft Report for Comment—Tech. and Confidentiality (Feb. 21, 2012).
time. E-mail and electronic documents have long been discussed within the legal community. It would have been beneficial for the Commission to set forth a technology that lawyers might actually need to learn about the benefits and risks. Addressing specific technology may be something the Commission plans to include on the proposed website discussed below—at least it should be.

Under the Committee’s recommendations, Comment four to Rule 1.4 would instruct lawyers to “promptly respond to or acknowledge client communications” instead of only “client telephone calls.” Although this is a listed amendment under Technology and Confidentiality, this recommendation does not directly deal with confidentiality issues and therefore it is only briefly mentioned in this paper.

The most significant proposal by the Commission is to rule Rule 1.6, Confidentiality of Information. The Commission’s recommendation adds a subsection c which would state, “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” The rationale for recommending the addition of subsection c is to emphasize the importance of preventing a disclosure of confidential information by making it black letter law. Currently, the duty to prevent disclosure is discussed only in the comments to Rule 1.6.

Specifically, there are three areas lawyers need to take precautions in protecting client confidentiality: (1) inadvertent disclosures; (2) unauthorized disclosures; and (3)

\[14\] ABA Comm’n on Ethics 20/20, Revised Draft Resolutions for Comment—Tech. and Confidentiality (Feb. 21, 2012).

\[15\] Id.

\[16\] ABA Comm’n on Ethics 20/20, Revised Draft Report for Comment—Tech. and Confidentiality (Feb. 21, 2012).

\[17\] See Model Rules of Prof’l Conduct R. 1.6 cmt. 16; cmt. 17 (2006).
Unauthorized access.\textsuperscript{18} Inadvertent disclosure is when confidential client information is accidentally disclosed, such as mistakenly sending an e-mail to the wrong recipient.\textsuperscript{19} Unauthorized disclosure is the intentional disclosure of confidential client information without the required permission to do so.\textsuperscript{20} Unauthorized access addresses situations such as being hacked by a third party.\textsuperscript{21} These are three distinct areas requiring unique precautions by lawyers. Therefore, it was necessary for the Committee to include each.

Reasonable efforts are required by attorneys to prevent disclosure of confidential client information.\textsuperscript{22} The comments provide five factors to assist attorneys in determining reasonableness: (1) sensitivity of the information; (2) likelihood of disclosure if additional safeguards are not employed; (3) cost of employing additional safeguards; (4) difficulty of implementing the safeguards; and (5) the extent to which the safeguards adversely affect the lawyer's ability to represent clients.\textsuperscript{23} These factors are broad and leave much of the determination up to the judgment of the individual lawyer.\textsuperscript{24} However, this is an appropriate approach considering the constantly changing nature of technology. Because technology is constantly changing, the rules are unable to provide specific steps attorneys must take in order to protect client confidentiality. The implementation of factors to guide the attorney in deciding what measures to take is

\textsuperscript{18} Letter from Jamie S. Gorelick and Michael Traynor, Co-Chairs ABA Comm'n on Ethics 20/20, to ABA Entities, Courts, Bar Assoc. (state, local, specialty and international), Law Schools, and Individuals (Feb. 21, 2012) (on file with author); ABA Comm'n on Ethics 20/20, Revised Draft Resolutions for Comment—Tech. and Confidentiality (Feb. 21, 2012).
\textsuperscript{19} Id.
\textsuperscript{20} Id.
\textsuperscript{21} Id.
\textsuperscript{22} ABA Comm'n on Ethics 20/20, Revised Draft Resolutions for Comment—Tech. and Confidentiality (Feb. 21, 2012). For a recent discussion on the ABA’s view of what constitutes reasonable efforts under the current ABA model rules with respect to a lawyers duty to protect confidentiality of clients when using e-mail see ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 11-459 (2011).
\textsuperscript{23} ABA Comm'n on Ethics 20/20, Revised Draft Resolutions for Comment—Tech. and Confidentiality (Feb. 21, 2012).
helpful, while at the same time it allows the opportunity to change with future advances of technology. Additionally, the website which is proposed by the Commission and discussed below would hopefully help attorneys stay informed on what is a “reasonable effort.”

If the lawyer takes reasonable steps to prevent disclosure but confidential client information is still disclosed, the lawyer has not committed a violation of Rule 1.6.\textsuperscript{25} However, the comments provide that “a client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule.”\textsuperscript{26} The commission included this comment because it is currently found in Comment seventeen to Rule 1.6 regarding measures a lawyer must take when sending confidential information. Therefore, the Commission felt the comment should also apply to the storage of confidential information.\textsuperscript{27} This comment suggests that lawyers should speak to clients about the risks associated with using technology and should obtain clients consent to the use of technology at the outset of the representation.\textsuperscript{28} That way, if after taking reasonable measures, confidential information is still disclosed, the client was aware of risk beforehand and the attorney is protected.\textsuperscript{29}

Finally, the recommended comment to Rule 1.6 would add a provision reminding lawyers of their obligations of other laws regarding the duty of confidentiality towards

\textsuperscript{25}ABA Comm’n on Ethics 20/20, Revised Draft Resolutions for Comment—Tech. and Confidentiality (Feb. 21, 2012).
\textsuperscript{26}Id.
\textsuperscript{27}ABA Comm’n on Ethics 20/20, Revised Draft Report for Comment—Tech. and Confidentiality (Feb. 21, 2012).
\textsuperscript{28}Kimbro, supra note 24.
\textsuperscript{29}Id.
clients.\textsuperscript{30} This recommendation is a useful reminder to lawyers to consider other aspects
of the laws in addition to the ethics rules, especially in light of the constantly changing
laws regarding the transfer of information through technology.

The final recommended change by the Committee regarding technology and
confidentiality is to Rule 4.4, Respect for rights of Third Persons. The recommendation
is to change the word “document” to the more specific language of “electronically stored
information” with respect to a lawyer’s duty, upon receipt of information inadvertently
sent, to notify the sender.\textsuperscript{31} The comment to this rule provides examples such as when
an e-mail or electronically stored information, including metadata, is inadvertently sent.\textsuperscript{32}

Notably, the Committee also recommends the addition of a website to assist
lawyers in remaining up to date on changing technology and on how to protect client
confidentiality.\textsuperscript{33} The website would contain easy to understand information on
technology and ways for lawyers to ensure confidentiality on behalf of their clients.\textsuperscript{34}
Because the rules must provide long term guidelines, the website would provide specific
and up to date information on issues surrounding technology. This website would be an
invaluable resource for attorneys to receive technological information they may not
otherwise understand or would need to hire an expert to assist them with.

One concept the Commission did not specifically address is a lawyer’s
responsibility toward protecting confidential client information when disposing of
technological equipment. This is a popular topic of discussion among practitioners in

\textsuperscript{30} ABA Comm’n on Ethics 20/20, Revised Draft Resolutions for Comment—Tech. and Confidentiality
(Feb. 21, 2012).
\textsuperscript{31} Id.
\textsuperscript{32} Id.
\textsuperscript{33} ABA Comm’n on Ethics 20/20, Revised Draft Report for Comment—Tech. and Confidentiality (Feb. 21,
2012).
\textsuperscript{34} Id.
legal journals and also in bar journals.\textsuperscript{35} Therefore, the disposing of technological devices is seemingly a topic warranting discussion by the Commission.

Devices such as copy machines, cell phones, flash drives, fax machines, and of course laptops all store confidential data.\textsuperscript{36} As a result, lawyers must be careful in how they dispose of these types of devices in order to ensure that their client’s confidential information remains protected. A recent Florida Bar Opinion contains a useful summary on this topic. It states that a lawyer should know enough about the technology he or she is using to know whether it needs to be “sanitized, or cleaned of all confidential information, before disposal.”\textsuperscript{37} The Florida Opinion also directs attorneys to ensure the devices have in fact been sanitized before disposal.\textsuperscript{38} This requires attorneys to supervise the business cleaning the equipment and to confirm the equipment has in fact been cleaned of all confidential information before disposing of it.

Arguably, the issue of properly disposing technological devices so as to ensure the protection of clients’ confidential information is contained within the proposal to Rule 1.6 and Rule 1.1. Rule 1.1 requires an attorney to remain competent on the issues and risks surrounding technology and the disposal of technological devices falls within this category. However, the Committee could have been more clear by including disposal as an example along with e-mail and electronic documents. Similarly, the disposal of


\textsuperscript{37} \textit{Id.}

\textsuperscript{38} \textit{Id.}
technological equipment is arguably covered under Rule 1.6’s duty to take reasonable steps to prevent disclosure of client confidentiality. Again, it would have been beneficial for the Committee to explicitly state that this duty covers the storage, use, and disposal of technology.

The Commission proposes several changes to the ABA Model Rules of Professional Conduct. All of the recommendations are beneficial with respect to clarifying attorneys’ duty to protect clients’ confidential information with respect the technology. However, the Committee should have addressed internal restrictions on access to client information and the disposal of equipment which contains confidential information.