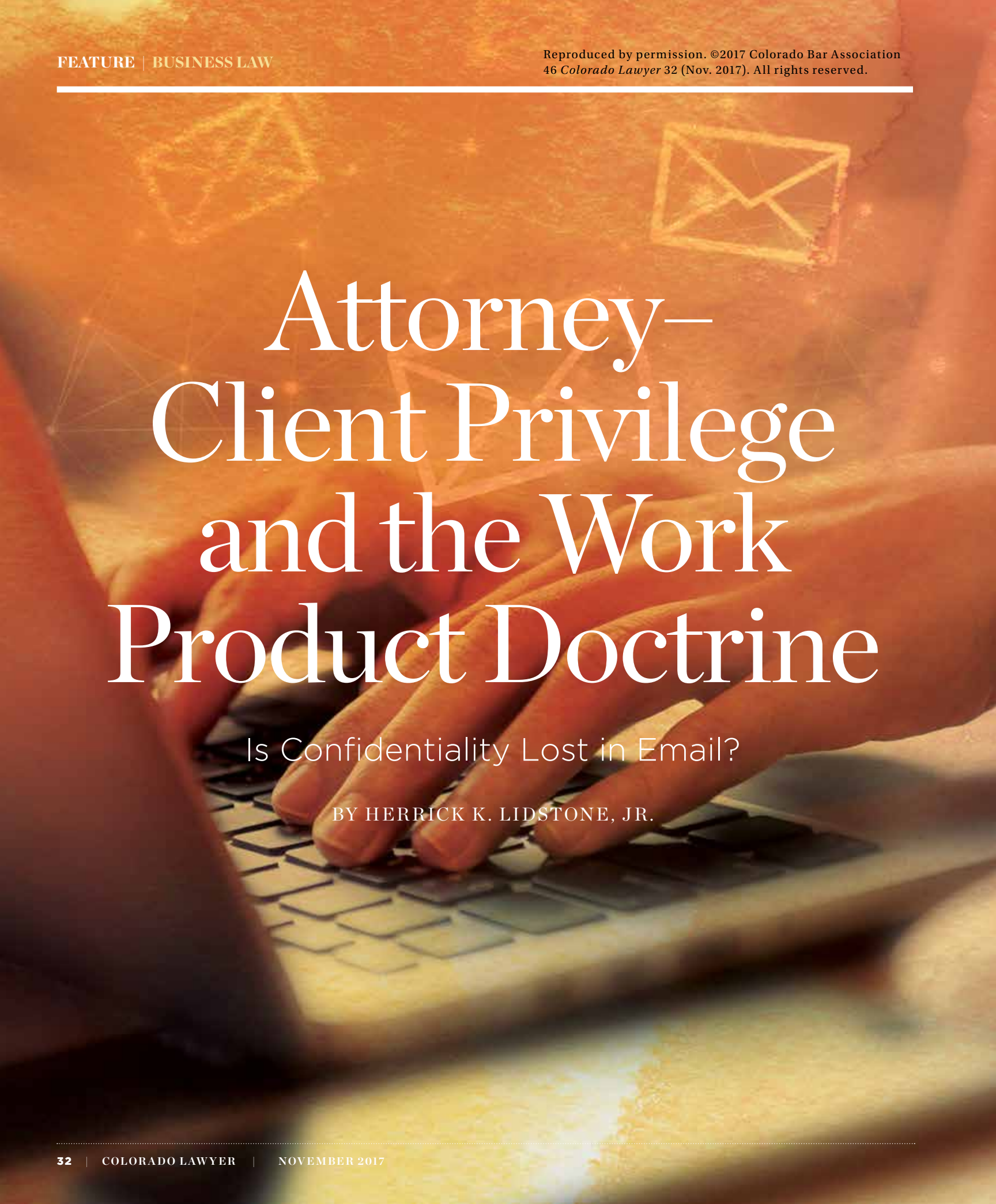

Attorney–Client Privilege and the Work Product Doctrine

Is Confidentiality Lost in Email?

BY HERRICK K. LIDSTONE, JR.

The attorney–client privilege and the work-product doctrine are crucial to the attorney–client relationship. This article discusses how the use of email may impact these privileges.

Electronic mail communications are a fact of life. There is no getting around this benefit and burden. Yet the careless use of email devices and networks by both attorneys and clients risks the loss of confidentiality and other privileges. This is especially true when clients communicate with their lawyers using their employer-established email accounts on office computers or email their lawyers from computers they share with others, including family members. Issues can also arise when clients store personal emails and information on a business or shared laptop, smartphone, or tablet. Carelessness includes using inadequate passwords that are seldom, if ever, changed. These actions risk the loss of confidentiality and any attendant privilege that may be claimed for the electronic communications.

The risks inherent in email communications are well-documented. As described by the ABA Law Practice Division,

> The headlines continue to be filled with reports of data breaches, now including law firms. A common adage in security (that applies to attorneys and law firms) is "there are two kinds of companies, those that have been breached and those that will be breached." A respected security consultant has aptly called the first hour of a breach response as "the upchuck hour."[1]

This environment raises issues regarding confidentiality and lawyer competence that 20th century lawyers never had to deal with—particularly the potential loss of attorney–client privilege and work-product protection as a result of uninformed communication techniques.

The Colorado Rules of Professional Conduct (Rules) require that lawyers "provide competent representation to a client,"[2] and that within the parameters of that competent representation "a lawyer should keep abreast of . . . changes in communications and other relevant technologies."[3] The implication is that it is the lawyer's obligation to protect the client's confidences in the face of electronic hacking and email sloppiness. This confidentially obligation is discussed below.

> "The attorney's confidentiality obligation established in Rule 1.6, the attorney–client privilege, and the work-product doctrine are key to the relationship between attorneys and clients."

Confidentiality, Attorney–Client Privilege, and the Work-Product Doctrine

The attorney's confidentiality obligation established in Rule 1.6, the attorney–client privilege, and the work-product doctrine are key to the relationship between attorneys and clients.

Rule 1.6 and Confidentiality

The principle of client–lawyer confidentiality found in Rule 1.6 "is given effect by related bodies of law: the attorney–client privilege, the work-product doctrine and the rule of confidentiality established in professional ethics."[4] The lawyer's duty of confidentiality in Rule 1.6 is much broader than either the attorney–client privilege or the work-product doctrine. "The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law."[5]

Attorney–Client Privilege

The attorney–client privilege is the "client's right to refuse to disclose and to prevent any other person from disclosing confidential communications between the client and the attorney."[6] The attorney–client privilege is "one of the oldest recognized privileges for confidential communications"[7] and is codified in Colorado law.[8] The U.S. Supreme Court has stated that by assuring confidentiality, the privilege encourages clients to make "full and frank" disclosures to their attorneys, who are then better able to provide candid advice and effective representation.[9]

Although there are minor variations, generally the elements necessary to establish the attorney–client privilege are:

- the asserted holder of the privilege is (or sought to become) a client;
- the person to whom the communication was made is a member of the bar of a court, or a subordinate of such a member, and is acting as an attorney in connection with this communication; and
- the communication was for the purpose of securing legal advice.[10]

Most jurisdictions provide exceptions to the attorney–client privilege. Chief among the exceptions are that the communication (1) was made in the presence of individuals who were neither attorney nor client, or (2) was disclosed to such individuals. When a client discloses attorney–client privileged information to a third party, the privilege may be lost. This may occur when

- a member of the board of directors of a company discloses attorney–client privileged information to a third party not in the management group in a casual conversation or by forwarding an email;
- an operator receives a title opinion that includes attorney–client privileged information and then discloses the information to working interest owners; or
- a client claims reliance on the advice of counsel for certain actions taken based on attorney–client privileged information.

Attorney–client information may also be disclosed inadvertently, such as when the attorney or client sends an email or attachment to an erroneous address.[11] Many attorneys believe that the ubiquitous email disclaimer protects a misdirected communication containing attorney–client privileged information or attorney work-product, but this is not necessarily the case.[12]

In *DCP Midstream LP v. Anadarko Petroleum Corp.*,[13] the Colorado Supreme Court reviewed claims of attorney–client privilege relating to an attorney's title opinion to determine "whether a particular communication concerns or contains confidential matters communicated by or to the client in the course of obtaining counsel, advice or direction." The argument made to the district court was that a title opinion was merely a recitation of facts in the public record and, therefore, not protected. Anadarko countered that "title opinions are privileged as a matter of law."[14] In conclusion, the Colorado Supreme Court stated:

> [W]e avoid making any sweeping pronouncement that all title opinions are, or are not, protected by the attorney–client privilege. Just as "there is no flat rule exempting all communications between a title attorney and a client from the reach of the attorney–client privilege," there is no flat rule including them. [Citation omitted.] Rather, a particular title opinion, like any document sought in discovery, may contain privileged attorney–client communications if the parameters of that doctrine are met. To make this determination, the particular title opinions must be examined.
>
> . . . [T]he party asserting the privilege bears the burden of establishing that a particular communication is privileged, and the party must claim the privilege "with respect to each specific communication." . . . To withhold discovery under a claim of privilege, C.R.C.P. 26(b)(5) requires a party to "make the claim expressly" and describe the nature of the withheld information in a privilege log. . . . The withheld information must be described "with sufficient detail so that the opposing party and, if necessary, the trial court can assess the claim of privilege *as to each withheld communication*."[15] [Emphasis in original.]

Furthermore, the attorney–client privilege is the client's privilege to maintain or waive; it is not the attorney's privilege.[16]

"Many attorneys believe that the ubiquitous email disclaimer protects a misdirected communication containing attorney–client privileged information or attorney work-product, but this is not necessarily the case."

The Work-Product Doctrine

The work-product doctrine is separate from and should not be confused with the attorney–client privilege. Under the work-product doctrine, "tangible material (or its intangible equivalent)"[17] that is collected or prepared in anticipation of litigation is not discoverable unless the party seeking the information has no other means of obtaining the information without undue hardship.[18] Where the required showing is made, the court will still protect mental impressions of an attorney by redacting the part of the document containing the mental impressions. The Colorado Supreme Court has described the work-product doctrine by reference to the U.S. Supreme Court's opinion in *Hickman v. Taylor*[19]:

> In Hickman the Court held that "written statements, private memoranda and personal recollections prepared by an adverse party's counsel in the course of his legal duties" are not discoverable in the absence of a showing of necessity or justification. In the wake of Hickman conflicting views developed over (1) whether discovery of trial preparation materials required only a showing of relevancy and lack of privilege, or an additional showing of necessity, (2) whether the work product doctrine extends beyond work actually performed by lawyers, and (3) what relationship, if any, existed between the "good cause" requirement of Rule 34 and the "necessity or justification" of the work product doctrine.[20]

The work-product doctrine is more inclusive than the attorney–client privilege. Unlike the attorney–client privilege, which includes only communications between an attorney and the client, work-product includes materials prepared by persons other than the attorney. The materials may have been prepared by anybody as long

as they were prepared with an eye toward the realistic possibility of impending litigation. Additionally, it includes materials collected for the attorney, such as interrogatories, signed statements, and other information acquired for the prosecution or defense of a case. However, "memoranda, briefs, communications, and other writings prepared by counsel for his own use in prosecuting his client's case, and . . . mental impressions, conclusions, opinions, or legal theories" are never discoverable by an opposing party.[21]

The work-product doctrine, which has been codified in the federal and Colorado rules of civil procedure,[22] is also less powerful than the attorney–client privilege. As set forth in CRCP 26(b)(3), a party may obtain discovery of documents otherwise protected by the work-product doctrine "only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the case and is unable without undue hardship to obtain the substantial equivalent of the materials by other means."

Even when work product is discoverable, the rule requires the court to "protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation"—that is, information within the attorney–client privilege.

When is the Privilege Lost through Electronic Communications?

It is human nature to take the easy approach. Thus individuals often do not consider the implications of sending personal emails from their work email account, or signing into their personal email account on their work equipment. But these actions can affect confidentiality and privileges in unintended ways.

Using Employer's Email or Equipment for Personal Communications

Many individuals are accustomed to communicating electronically while at work and use their employer's email for personal communications—arranging personal events, online shopping, and many other things. Frequently, this includes dealing with personal lawyers, whether handling a personal traffic matter, estate planning, or even dealing with complaints against the employer itself. Individuals also frequently use their employer's equipment (laptop, tablet, smartphone, etc.) to access personal email accounts. Any of these actions can result in loss of confidentiality, and consequently the loss of the attorney–client privilege and work-product defenses.

In re Asia Global Crossing, Ltd. established four factors to be considered in determining whether an employee has a reasonable expectation of privacy in email transmitted over a company system:

1. does the corporation maintain a policy banning personal or other objectionable use,
2. does the company monitor the use of the employee's computer or e-mail,
3. do third parties have a right of access to the computer or e-mails, and
4. did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[23]

Where the reasonable expectation of privacy *does not* exist, an employee's use of the employer's email system or equipment may result in a waiver of attorney–client and other privileges and attorney-work product. This could apply to emails that flow through the employer's email or are stored on the employer's electronic equipment.

This issue is also discussed in ABA Formal Opinion 11-459,[24] which suggests that it is the lawyer's obligation to advise the client about the risks associated with the possible loss of the attorney–client privilege in these circumstances.

Using employer's email for personal communications. An interesting case on point arose from litigation that was commenced in Florida, but was based on a subpoena for production of emails served in and adjudicated by New York state courts. The chief executive officer of Marvel Entertainment, Isaac Perlmutter, owned a luxury condominium in West Palm Beach, Florida. Harold Peerenboom also owned a condominium in the same complex. Bad blood developed between the two, and ultimately Peerenboom accused Perlmutter of defamation and brought suit against him in Florida.[25] In the Florida litigation, Peerenboom subpoenaed all of Perlmutter's emails from his employer, Marvel Entertainment. Peerenboom sought to enforce the subpoenas, while Perlmutter moved the New York County Supreme Court for a protective order based on (among other things) attorney–client privilege, spousal (or marital) privilege, and the work-product doctrine.[26] The trial court granted the protective order based solely on spousal privilege,[27] and denied it on the other grounds. Both Peerenboom and Perlmutter appealed.

On appeal, the appellate court noted Marvel's written policy, which specifically allowed employees to receive personal emails but also stated that Marvel owned all emails on its system.[28] Marvel's written policy also reserved the right to audit networks and systems to ensure compliance with its email policies. Marvel further reserved the right "to access, review, copy and delete any messages or content" and to "disclose such messages to any party (inside or outside the Company)."[29] The court found that even if Perlmutter was "not actually aware of Marvel's email policy, [he was] constructively on notice of its contents" in light of his role as CEO of Marvel.[30] As a result, "Perlmutter's use of Marvel's email system for personal correspondence"[31] lacked the reasonable expectation of privacy "that is an essential element of the attorney–client privilege"[32] and he "waived the confidentiality necessary for a finding of spousal privilege."[33]

However, the New York appellate court also found that, because there was no evidence that Marvel had actually viewed the emails or that there was any other actual disclosure of the emails to a third party, "Perlmutter's use of Marvel's email for personal purposes does not, standing alone, constitute a waiver of attorney work product protections."[34] The appellate court remanded the case to the New York trial court "for in camera review and a determination of whether such documents are in fact protected attorney work product."[35]

Using employer's equipment for personal communications. Most people have personal email accounts through various providers. These accounts are generally "cloud-based" because they do not reside on the electronic device, but rather, in the electronic cloud maintained by the service provider. However, images of cloud-based

email are often stored on the electronic device used for transmission.

It is common for employees to use their employer's electronic devices for personal email communications through these cloud-based email providers. The use of employer equipment to receive and send cloud-based, personal email raises the same questions about a "reasonable expectation of privacy" as discussed in *In re Asia Global Crossing, Ltd*.[36] This "reasonable expectation" analysis also depends on written company policies.

In *Stengart v. Loving Care Agency, Inc.*,[37] an employee brought a discrimination action against her employer, who immediately copied the employee's hard disk in the employer-supplied computer. Although the employee had communicated with her attorney using her personal Yahoo email account, the employer computer kept images of her pre-litigation communications with her attorney. The employer's litigation attorneys found these emails and used them in the litigation without notifying the employee's counsel. The employer argued that there could be no reasonable expectation of privacy in an employee's use of company computers, even when using a personal email account. The employer's policy said that emails "are not to be considered private or personal to any individual employee," and "[o]ccasional personal use [of email] is permitted."[38]

The New Jersey Supreme Court rejected the employer's argument. The Court held that because the employer's policy was ambiguous about whether it was intended to include personal email accounts, the employee's expectation of privacy in using her personal email account was "objectively reasonable."[39] "Under all of the circumstances, [the Court found] that [the employee] could reasonably expect that e-mails she exchanged with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, would remain private."[40] Consequently, the Court found that the employee's emails were protected by the attorney–client privilege and that the employer's attorneys' review and use of the emails in litigation violated Rule 4.4(b) of the New Jersey Rules of Professional Conduct.[41] The Court remanded the case to the trial court "to decide whether disqualification of the Firm, screening of attorneys, the imposition of costs, or some other remedy is appropriate."[42]

In *Miller v. Zara USA, Inc.*,[43] a New York case decided shortly after *Peerenboom*, the appellate court reviewed the trial court's decision to issue a protective order for the benefit of the employee in a dispute between employer Zara USA, Inc. and its former general counsel. The employee retained personal documents on a company-owned laptop, but claimed that they were protected by the attorney–client privilege and the work-product doctrine. The company handbook specifically "restricted use of company-owned electronic resources, including computers, to 'business purposes'" and warned that "[a]ny data collected, downloaded and/or created" on such resources was "the exclusive property of Zara" and "may be accessed by Zara at any time, without prior notice."[44]

As in *Peerenboom*, but contrary to *Stengart*, the New York appellate court found that, in light of the published company policy, the employee did not have a reasonable expectation of privacy with respect to those documents and therefore could not assert the attorney–client privilege. The court found that the work-product privilege "is waived upon disclosure to a third party only when there is a likelihood that the material will be revealed to an adversary under conditions that are inconsistent with a desire to maintain confidentiality."[45] Although Zara was an adversary, Zara stated that it never actually viewed any documents stored on the employee's laptop. The court remanded the case to the trial court for an in camera review of the documents for the applicability of the other factors involved in determining the availability of work-product privilege.[46]

Using Dropbox or other file sharing mechanism. It is easier today to share electronic files with clients, co-counsel, and even opposing counsel. Attorneys must be careful with respect to how files are shared, however. In *Harleysville Insurance Co. v. Holding Funeral Home, Inc.*,[47] the plaintiff used a file-sharing service to exchange files with a number of users, including its counsel. The plaintiff unfortunately did not limit access to these files and, as a result, opposing counsel in litigation was able to obtain the attorney–client communication and work product. The magistrate judge made two significant holdings: (1) plaintiff's actions were equivalent to publishing the files on the Internet, and therefore attorney–client privilege and work-product protection had been waived. "In essence, Harleysville has conceded that its actions were the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they could find it";[48] and (2) citing FRCP 26(b)(5)(B) and Virginia rules similar to Colo. RPC 4.4(b), the court sanctioned defendant's counsel for improperly accessing the unsecured files and not notifying opposing counsel of their privileged nature.[49]

Rule 1.6 and the Electronic Age

Attorney–client privilege and the work-product doctrine remain alive and well in Colorado and elsewhere, but retaining the privileges and the right to withhold disclosure is much more likely to be challenged in this electronic age. It is the lawyer's obligation to protect the communication, even if that requires educating the client. Rule 1.6(c) provides that "[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 2016 amendments to Rule 1.6, comment [18] address confidentiality, specifically with respect to electronic communications. The comment also states that unauthorized access to or inadvertent or unauthorized disclosure of communications "*does not* constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure" (emphasis added). Thus, any unauthorized access or disclosure will be judged based on "reasonableness."

According to the comment, the factors considered in determining reasonableness are considered on a cost-benefit basis, and include, but are not limited to:

- the sensitivity of the information (with the presumption that the more sensitive the information, the more protections should be in place);
- the likelihood of disclosure if addi-

tional safeguards are not employed;
- the cost of employing additional safeguards;
- the difficulty of implementing the safeguards; and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

The comment suggests that a client may require the lawyer to implement special security measures or may "give informed consent to forgo security measures that would otherwise be required by this Rule." Because it is the client that must give informed consent to avoid adequate security measures for electronic communication, it is the lawyer who must educate the client, and thus be able to obtain informed consent.[50]

Similarly, ABA Formal Opinion 17-477R[51] discusses the lawyer's ability to communicate with his client electronically and concludes (based on the Model Rules):

> Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.
>
> A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

Attorney's Duty to Advise Client of Risks

Like their lawyers, clients have varying degrees of technological skills and knowledge, and some clients may not realize the risk of the loss of confidentiality when using electronic communications. Unlike their clients, lawyers need to develop that technological knowledge to meet their ethical obligations to their clients.[52] ABA Formal Opinions 11-459[53] and 17-477R suggest that it is the lawyer's obligation to advise the client as to the risks associated with the

possible loss of the attorney–client privilege in these circumstances.[54] Relying on Model Rule 1.6 (and specifically comments [16] and [17]), Formal Opinion 11-459 note 4 states:

> Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of e-mail communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others. In particular, as soon as practical after a client–lawyer relationship is established, a lawyer typically should instruct the employee–client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney–client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.

Formal Opinion 11-459 note 7 specifically states that "if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer or other device owned or controlled by the employer, then a duty arises to caution the client not to do so, and if that caution is not heeded, to cease sending messages even to personal e-mail addresses." Thus, under the Formal Opinion (which has not been adopted in Colorado), it is the lawyer's obligation to protect the client from the client's own careless acts.

ABA Formal Opinion 11-460[55] addresses what happens when an attorney receives communications between an opposing party and counsel that is not transmitted, but rather is stored on a third party (employer-owned, in the case of an employer-employee dispute) computer. The ABA Formal Opinion states that in this case Rule 4.4(b) of the Rules of Professional Conduct is not applicable because the email was not "inadvertently sent."[56]

Formal Opinion 11-460 also suggests that other law, court decisions, or civil procedure rules may require disclosure to the opposing party that personal emails have been retrieved from the third-party computer, and Rule 1.6(b)(6) permits that disclosure by the attorney.[57] Where no law requires notification, Formal Opinion 11-460 suggests that the decision to provide the disclosure must be made by the client following the lawyer's explanation of the implications of disclosure and available alternatives.[58]

Conclusion

Peerenboom, *Stengart*, *Zara*, and other cases have focused on the language in the employer's written policies for the protection and use of employer's email and employer's equipment in analyzing the reasonable expectation of privacy under *In re Asia Global Crossing, Ltd.* Storage of electronic materials on an employer's laptop alone is not sufficient to waive the work-product doctrine, but may be sufficient for waiver of the attorney–client privilege, depending on the language of the written policies. *Harleysville* is simply a recognition that everything not protected on the Internet by a password or other mechanism is available to everyone.

Rule 1.6 and ABA Formal Opinions 11-459, 11-460, and 17-477R reaffirm the lawyer's obligation to educate the client appropriately to maintain confidentiality or to obtain the client's informed consent where the client wants to deviate from best practices. Given the ease with which confidentiality and privileges can be lost through electronic communication by misdirected emails, hacking, phishing, or lost equipment, lawyers and their clients must take adequate precautions. CL

Herrick K. Lidstone, Jr., is a shareholder of the Greenwood Village firm of Burns, Figa & Will, P.C., where he has been president and managing director since 2012. Lidstone practices in the areas of business transactions, including partnerships, limited liability companies, and corporate law; federal and state securities compliance; mergers and acquisitions; contract law; tax law; real estate law; and natural resources law. He is a member of the CBA Business Law Section's executive council. Lidstone is the author of *Securities Law Deskbook* (Colorado Bar Association CLE 2016) and (with Allen Sparkman) *Limited Liability Companies and Partnerships in Colorado* (Colorado Bar Association CLE 2d ed. 2017).

Coordinating Editor: David P. Steigerwald, dps@sparkswillson.com

NOTES

1. Email received June 19, 2017, from the ABA Law Practice Division (lp@americanbar.org) for the course "Your Law Firm Has Been Breached: What's Next?" The course was held on July 13, 2017. *See* description at https://shop.americanbar.org/ebus/ABAEventsCalendar/EventDetails.aspx?productId=277018622.
2. Colo. RPC 1.1.
3. Colo. RPC 1.1, cmt. [8].
4. Colo. RPC 1.6, cmt. [3].
5. *Id.*
6. Garner, ed., *Black's Law Dictionary*, definition of "attorney-client privilege" at 1391 (10th ed. 2014).
7. *Swidler & Berlin v. United States*, 524 U.S. 399, 403 (1998), citing *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) and *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888). Some date the attorney–client privilege back to *Berd v. Lovelace*, Cary 62, 21 Eng. Rep. 33 (1577), which found that a solicitor was exempt from being compelled by subpoena or otherwise to be examined on any matter for which he had served as counsel. *See* Wunnicke, *Ethics Compliance For Business Lawyers* at § 3.1 (John Wiley & Sons Inc. 1987).
8. CRS § 13-90-107(1)(b) provides:

   > An attorney shall not be examined without the consent of his client as to any communication made by the client to him or his advice given thereon in the course of professional employment; nor shall an attorney's secretary, paralegal, legal assistant, stenographer, or clerk be examined without the consent of his employer concerning any fact, the knowledge of which he has acquired in such capacity.

9. *Upjohn Co.*, 449 U.S. at 389. *See also DCP Midstream LP v. Anadarko Petroleum Corp.*, 303 P.3d 1187, 1200 (Colo. 2013); *Gordon v. Boyles*, 9 P.3d 1106 (Colo. 2000); *Law Offices of Bernard D. Morley, P.C. v. MacFarlane*, 647 P.2d 1215, 1221 (Colo. 1982); *A. v. Dist. Court of Second Judicial Dist.*, 550 P.2d 315, 324 (Colo. 1976).
10. *See, e.g., Colton v. United States*, 306 F.2d 633, 637 (2d Cir. 1962), *cert. denied* 371 U.S. 951 (1963), citing *United States v. United Shoe Mach. Corp.*, 89 F.Supp. 357, 358–59 (D.Mass. 1950).
11. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459: Duty to Protect the Confidentiality of E-mail Communications with One's Client (Aug.

11, 2011), www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_459_nm_formal_opinion.authcheckdam.pdf; ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-460: Duty When Lawyer Receives Copies of a Third Party's Email Communications With Counsel (Aug. 4, 2011), www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_460_nm_formal_opinion.authcheckdam.pdf.

12. *See* Lidstone, Jr., "E-mail Disclaimers: A Worthwhile Endeavor or a Waste of Electronic Ink?" http://ssrn.com/abstract=2656466; Kelly, "E-mail Disclaimers, Inadvertent Disclosures, and the Attorney–Client Privilege," 39 *Colorado Lawyer* 97 (May 2010).

13. *DCP Midstream LP*, 303 P.3d at 1199.

14. *Id.*

15. *Id.* at 1199–1200.

16. Note that clients can elect to waive attorney–client privilege by, for example, claiming an "advice of counsel" defense. In that case, the scope of the waiver is usually "that the waiver applies to all other communications relating to the same subject matter." *In re EchoStar Commc'ns Corp.*, 448 F.3d 1294, 1299 (Fed. Cir. 2006).

17. Fed. R. Evid. 502.

18. FRCP 26(b)(3); CRCP 26(b)(3). In *Hickman v. Taylor*, 329 U.S. 495 (1947), the Court recognized the work-product doctrine, that information obtained or produced by or for attorneys in anticipation of litigation may be protected from discovery under the Federal Rules of Civil Procedure.

19. *Hickman*, 329 U.S. 495.

20. *Hawkins v. Dist. Court in and for Fourth Judicial Dist.*, 638 P.2d 1372, 1375–76 (Colo. 1982).

21. *Hickman*, 329 U.S. at 508.

22. FRCP 26(b)(3); CRCP 26(b)(3).

23. *In re Asia Glob. Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005).

24. ABA Formal Op. 11-459, *supra* note 11.

25. According to the New York County Supreme Court, "Peerenboom commenced an action in the Circuit Court of Palm Beach County, Florida, alleging that Perlmutter and his wife . . . defamed Peerenboom by sending anonymous defamatory letters to persons living or working at the Palm Beach condominium development where they all reside." *Matter of Harold Peerenboom v. Marvel Entm't, LLC*, No. 162152/2016, 2016 WL 6070823 at *2 (Sup. Ct.N.Y. County Sept. 30, 2016).

26. *Id.*

27. Note that Colorado has extended the spousal privilege, CRS § 13-90-107(1)(a), to partners in a civil union, CRS § 13-90-107(1)(a.5).

28. *Peerenboom v. Marvel Entm't, LLC*, 148 A.D.3d 531 (N.Y.App.Div. 2017).

29. *Id.* at 532.

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id. See also* an earlier New York case, *In re The Reserve Fund Sec. & Derivative Litig.*, 2010 WL 11248673 (S.D.N.Y. 2010) (not reported in F.Supp.), where the court determined that an investment adviser was constructively aware of his company's policy regarding emails and moreover was aware of Rule 204-2 under the Investment Advisers Act (17 CFR § 275.204-2), which requires that all registered investment advisers maintain email communications with customers—and there was no practical way of isolating personal emails to his wife to protect the spousal privilege.

36. *In re Asia Glob. Crossing, Ltd.*, 322 B.R. at 257.

37. *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010).

38. *Id.* at 657.

39. *Id.* at 663.

40. *Id.* at 664.

41. New Jersey Rule 4.4(b) has a similar effect (although different wording) to Colo. RPC 4.4(b), which provides: "A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."

42. *Stengart*, 990 A.2d at 666.

43. *Miller v. Zara USA, Inc.*, 56 N.Y.S.3d 302 (App.Div.Sup.Ct. NY, First Dept. June 6, 2017).

44. The company handbook also states that employees "do not have an expectation of privacy or confidentiality in any information transmitted or stored in Zara's electronic communication resources (whether or not such information is password-protected)." *Id.* at 304.

45. *Id. See also Bluebird Partners, L.P. v. First Fid. Bank, N.J.*, 248 A.D.2d 219, 225 (N.Y.App. Div. 1998).

46. In various factual situations, courts have reached different conclusions with respect to the use of employer equipment for otherwise confidential emails. *See* cases cited in ABA Formal Opinion 11-460, *supra* note 11 at footnote 5. *See also* Porter, "Going Mobile: Are Your Company's Electronic Communications Policies Ready to Travel?" *Business Law Today* (ABA Business Law Section Dec. 19, 2011), http://apps.americanbar.org/buslaw/blt/content/2011/12/article-4-porter.shtml. Porter's article includes the section "Case Law on the Right to Monitor."

47. *Harleysville Insurance Co. v. Holding Funeral Home, Inc.*, Case No. 1:15cv00057, 2017 WL 1041600 (W.D. Virginia Feb. 9, 2017).

48. *Id.*, slip op. at 9. Colo. RPC 4.4(b) provides: "A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."

49. *Harleysville Insurance Co.*, slip op. at 13–17. Notably the court did not disqualify defense counsel, because as a result of the waivers, the information would also be available to successor counsel. The court required defense counsel to bear the parties' costs in obtaining the court's ruling.

50. *See also* Evans et al., "Keeping Client Confidences in the Digital Age," 45 *Colorado Lawyer* 69 (June 2016).

51. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 17-477R: Securing Communication of Protected Client Information (rev. May 22, 2017), www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf.

52. *See* Striker, CEO, Savvy Training and Consulting (www.savvytraining.com), "You Have a Duty to Be Tech-Savvy" in Solo In Colo (August 15, 2017) available at http://soloincolo.com/duty-tech-savvy and at http://www.savvytraining.com/single-post/2017/05/09/You-Have-a-Duty-to-Be-Tech-Savvy.

53. ABA Formal Op. 11-459, *supra* note 11.

54. Recall that Colo. RPC 1.1, comment [8] requires that lawyers, as a factor of "provid[ing] competent representation to a client," must "keep abreast of . . . changes in communications and other relevant technologies."

55. ABA Formal Op. 11-460, *supra* note 11.

56. In the 2017 case *McDermott Will & Emery LLP v. Superior Court of Orange Cty.*, 10 Cal. App.5th 1083 (Cal.Ct.App. 4th Dist. 2017), a California appeals court affirmed the trial court's disqualification of Gibson, Dunn & Crutcher, LLP as defense counsel in a high-profile legal malpractice case based on its allegedly unethical exploitation of the opposing party's inadvertently disclosed, privileged communications. In this case, Dick Hausman, an 80-year old with multiple sclerosis, forwarded an email he received from his attorney. This email made its way, through several transmissions, to opposing counsel, Gibson, Dunn & Crutcher, which used the email in depositions and motions. The California trial court found that Hausman forwarded the email unintentionally and no subsequent transmission waived the attorney–client privilege because only Hausman could have made such a waiver. The court explained that "Gibson Dunn had an ethical obligation to return the privileged material and refrain from using it under *State Comp. Ins. Fund v. WPS, Inc.* (1999) 70 Cal. App.4th 644." Further, Gibson Dunn's disqualification was necessary because there was a genuine likelihood that Gibson Dunn's improper use of the email could affect the outcome of the lawsuit, the integrity of the judicial proceedings, and the public's confidence in the proceedings. *Id.* at 1092. The California appellate court affirmed the trial court's findings. The California Rules of Professional Conduct, www.calbar.ca.gov/Attorneys/Conduct-Discipline/Rules/Rules-of-Professional-Conduct/Current-Rules, do not have an equivalent rule to Model Rule 4.4 (Respect For Rights of Third Persons).

57. ABA Formal Op. 11-460, *supra* note 11 at 3.

58. *Id.*