NORTH CAROLINA
BAR ASSOCIATION
SEEKING LIBERTY & JUSTICE

January 23, 2012

VIA EMAIL (amine@ncbar.gov) & FIRST CLASS MAIL

Ms. Alice Neece Mine
North Carolina State Bar
Post Office Box 25908
Raleigh, North Carolina 27611-5908

RE: Comment of the NCBA Labor and Employment Law Section Council on Employer Email and Privilege:

Question: Is it ethical for a lawyer to advise a client (the employer) that it is appropriate for the client to review email messages between an employee and the employee's attorney when the client has a work policy that informs all employees that email sent or received using the employer's email system are monitored by the employer?

Question: Is it permissible in this situation for the client's lawyer to review the email exchanges between the employee and the employee's attorney sent and received using the client's email system?

Dear Ms. Mine:

The Labor and Employment Law Section of the North Carolina Bar Association (Section) is comprised of attorneys who represent employers and employees across the state. The Section's Council includes bar leaders and highly regarded practitioners who have taken on the important obligation of service as thoughtful leaders on emerging legal and ethics issues relevant to this practice area in North Carolina. In this capacity, we submit the following guidance on the above-posed questions.

Virtually every employment case now involves the discovery of email, and it is not uncommon for plaintiffs' lawyers to demand production of the plaintiff's own email (both sent and received), as well as the email of other material witnesses. Thus, it is likely that even where the employer has not actively monitored the employee's email or otherwise independently discovered questionable personal communications, at some point an employer will be called upon to recover, identify and produce those emails. A definitive resolution of the ethical issue is therefore important, potentially impacting at least four constituents:

(1) the employee's lawyer (who participated in the email and/or failed to instruct the client not to use the employer's devices to transmit email, and who now faces the prospect of disclosing confidential client information and/or litigation strategies and analyses to opposing counsel),

(2) the employer's lawyer (who is subsequently called upon to review the email communication, and consider the ethical and evidentiary issues surrounding it),

(3) their respective clients, and

(4) the administration of justice consistent with public policy, including just dispute resolution based upon the true facts of the case, and promoting legally informed decision-making by protecting client confidences.

There are many different issues that arise in the context of email communications. This letter is limited to the specific situation raised in the two inquiries above – that is, the employee's use of the employer's email system to transmit email to the employee's personal attorney. This letter does not address, and should not be read to address, any other issues, including, among other things, the ethical, evidentiary and discoverability issues surrounding (1) an employee's personal, internet-based email account[1] that the employee accessed via the employer's computer system or electronic device; or (2) employer-required use of an employee's "personal" email account whether through an employer-owned computer system, electronic device or otherwise. These issues are substantial and important given the common use of such communications in the work place and in society. The Council respectfully requests that any Ethics Opinion or other guidance from the Bar in response to the two poased questions posed be similarly limited.[2]

With respect to the first question posed above, we believe that the answer depends upon whether the attorney can ethically view the emails herself, as the North Carolina Rules of Professional Conduct expressly prohibit an attorney from violating the Rules of Professional Conduct by assisting or inducing another to do so, and prohibits an attorney from violating the Rules through the acts of a third party. N.C.R.Prof.Cond. 8.4(a). Obviously, the Rules do not apply to non-lawyers. Thus, the client would not be barred from independently reviewing the emails (and there would be no ethical repercussions to an attorney whose client did so, without the attorney's knowledge or input), but whether the attorney could *advise* the client employer to review the emails would depend on whether the attorney were herself barred from reviewing those emails.

So far as we can discern, the answer to the second question is not directly addressed in North Carolina law,[3] and requires more extensive analysis. Given our unique position "in the trenches" with respect to the proposed questions, we believe that the Bar's analysis might benefit from our insights and experiences. We therefore write to share the Council's views.

---

[1] Case law indicates that an employee would have a greater expectation of privacy in those accounts. *See, e.g., Thygeson v. U.S. Bancorp Equip. Fin'g, Inc.* No. CV-03-467, 2004 U.S.Dist.LEXIS 18863 (D.Or. 9/15/04) (employee had higher expectation of privacy with respect to personal internet email account); *Stengart v. Loving Care Agency*, 990 A.2d 650 (N.J. 2009)(employee had reasonable expectation of privacy with respect to forensically recovered emails she transmitted on company laptop through her personal, password-protected web-based email account); *National Economic Research Assocs. v. Evans*, 21 Mass.L.Rep. 337, 2006 Mass.Super.LEXIS 371(Mass. Super. 2006)(employee retained privilege as to emails sent through personal, password-protected Yahoo account, using employer's laptop).

[2] The Council is happy to provide its thoughts on these issues if you would like us to do so.

[3] On August 4, 2011, the American Bar Association issued a formal opinion on this fact scenario with respect to the Model Rulesof Professional Responsibility, concluding that because Model Rule 4.4(b) contained no specific requirement with respect to receipt of potentially attorney-client privileged emails, no ethical issue arose and counsel's behavior was instead governed by standards of professionalism and the applicable rules of the jurisdiction. *See* ABA Comm. On Ethics and Prof'l Resp., Formal Op. 11-460 (Aug. 4, 2011). However, North Carolina has not previously taken such a strictly literal approach to the Rules of Professional Responsibility, *see, e.g.* 2009 Formal Ethics Opinion 1 (review and use of metadata).

Context and Practicality[4]

It is now commonplace for employers to provide email and internet access to its employees, and to require that the employee use that technology.[5] These tools are typically provided via computer networks, servers, desktop/laptop computers, smartphones or other PDAs, notepads, and the like. Employers often purchase, set up, service, and maintain these systems at considerable expense. These systems – and email in particular – allow for fast and easy communication (both internally and externally) and enable employees to share large volumes of information, often with only a few mouse clicks. Given both the financial investment in IT systems and the risks associated the fast and easy flow of information, many (but not all) employers restrict employee use of employer-provided email systems and internet access to business uses and prohibit (or significantly restrict) personal usage. Many (but not all) employers also actively monitor employee usage of employer-provided email systems.[6] Employers typically codify these restrictions in written policies that outline permitted use and notify employees that their usage may be monitored.[7] Employer monitoring of employee use of its email systems is not unlawful and serves legitimate goals, including, among other things, protecting trade secrets and other confidential employer information, and ensuring compliance with various federal and state anti-discrimination and anti-harassment statutes.[8]

However, as longer and irregular hours of work overlap into personal time,[9] employees are more prone to mix business use and personal use of employer-provided technology resources, or to feel justified in using normal work hours to take care of personal matters. Given the volume of forms and paperwork many employees are provided upon hire, some employees may honestly be unaware of policies that restrict or prohibit non-business uses of the employer's email and computer systems and/or disclose that the employer will monitor usage.[10] Additionally even in those cases where the employee was

---

[4] The contents of this section are, in part, generalizations based on the observations of Council members in the course of their individual practices representing employers and employees. They are not intended to be all-inclusive.

[5] One source states that over 60 million employees in the United States have email or internet access, or both, at work. *See* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 28 Am.Bus.L.J. 285, 308 (Summer 2011)(citing Marc A. Sherman, *Webmail at Work: The Case for Protection against Employer Monitoring*, 23 Touro L.Rev. 647, 656 (2007); and Mary Madden & Sydney Jones, Pew Internet & Am. Life Project, Networked Workers: Most Use Email, but Say Technology is a Mixed Blessing 2 (2008, available online at http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Networked_Workers_FINAL.pdf.pdf (hereinafter "Pew Report").

[6] According to one source, by 2007 65% of companies monitored employee internet use, and 43% monitored email with the majority of that monitoring occurring in incoming/outgoing messages, rather than internal company email. Seventy-three percent (73%) of those companies used technology tools to automatically monitor, but 40% stated that they assigned an individual to manually read and review the email. AMA/EPolicy Institute Research, 2007 Electronic Monitoring & Surveillance Survey.

[7] These documents are commonly promulgated in employee handbooks or policies, email notices, written notices, intranet postings, and/or on-site training. *See Pew Report* (reporting that eighty-three percent (83%) of employers who monitored computer use informed workers that they were doing so, either via an employee handbook (70%), email notices (40%), written notices (35%), intranet postings (32%) and/or on-site training (27%)).

[8] For example, racially inappropriate emails can create or contribute to a racially hostile work environment in violation of Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e, *et seq.* *See Brown v. Nucor Corp.*, 576 F.3d 149, 151 (4th Cir. 2009)(emails sent using company email system that depicted black people in racially offensive ways, such as by showing them with nooses around their necks, contributed to racially hostile work environment).

[9] Nearly half (45%) of all workers perform some work at home during personal time, but that figure rises to 56% when workers have workplace internet or email. Twenty percent (20%) of the latter report that they perform work at home every day or almost every day. *See Pew Report.*

[10] Whether or not such an assertion is credible will, by necessity, vary based on the facts and circumstances of each situation including, among other things, the location of the relevant policy, how that policy was communicated, reminders the employer provided regarding that policy, training regarding the policy, employer statements or actions inconsistent with its stated policies, and the like. *See also* Jessi Knox, *Email in the Workplace: Employees Perceive Email Differently than Employers*, Orange

aware of the employer's policy at the time of emailing, he or she may not have understood that (a) the employer's monitoring is undetectable by the employee user, and/or (b) deleted emails are easily recoverable and reviewable by the employer.

N.C. Rules of Professional Conduct Provide Limited Guidance

Like the ABA and most other States, North Carolina does not prohibit client communication via email, and does not treat email communications differently from more traditional forms of communication. *See* N.C.R.Prof.Cond. ("Rule") 1.6, Comment [18]; RPC 215 (Jul. 21, 1995)(counsel must use care to minimize risks that confidential information will be disclosed in a communication via cell phone and email).[11] No specific guidance is provided with respect to emails sent via an employer's email system, or the balance (if any) a lawyer must strike between her obligations to her employer client versus any obligations to other parties and the Bar.

North Carolina's Rules of Professional Conduct (the "Rules") require that counsel diligently and zealously represent her client, taking whatever lawful and ethical measures are required to vindicate the client's cause or endeavor. Rule 0.1 and Rule 1.3. With respect to litigation, a lawyer is required to make reasonably diligent efforts to comply with discovery requests and to disclose evidence or information that the lawyer knew or should have known was subject to disclosure – such as, an employee's email. Rule 3.4(d)(2), (3). On the other hand, Rule 4.4 requires a lawyer to respect the rights of others, and requires an attorney to promptly notify counsel when the lawyer receives an inadvertently disclosed writing that relates to the other lawyer's representation, so that the other lawyer may take appropriate protective measures. Rule 4.4(b). [12] Additionally, a lawyer's advice with respect to the use of another party's emails must be competent, Rule 1.1, with due regard to the consequences of using improperly obtained information.[13] Further, as an advisor, a lawyer must provide candid and independent advice that may

---

Journal (Jan. 23, 2006), available online at http://orange.eserver.org/issues/5-1knox.html, quoting *Patricia A. Chociey, Who's Reading my email?": A study of professionals' e-mail usage and privacy perceptions in the workplace*, 40 Professional Communication, IEEE Transactions 34, 34-35 (1997) ("Most employees underestimate their employer's legal right to monitor email activities. In addition, employees tend to believe their employers have no right to read their email correspondences, discover abuses, and take legal action. Contrary to this opinion, employers and network administrators argue that monitoring is justifiable, since the company owns the electronic mail system and the data it contains."). *See also, e.g.*, DeLoitte & Touche USA, LLP, *2007 Ethics & Workplace Survey Results* (72% of employees considered it acceptable to use employer's technology for personal purposes), available online at http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2007_ethics_workplace_survey_011009.pdf.

[11] *Accord* ABA Formal Op. 99-413 (1999)(lawyers have reasonable expectation of privacy in communications made by email, and may communicate with client via email; encryption is not required, but unusual circumstances involving extraordinarily sensitive information might warrant enhanced security measures); Ark. Ethics Op. 98-2 (1998)(same); D.C. Ethics Op. 281 (1998)(same); Ill. Ethics Op. 96-10 (1997)(same); Ky. Ethics Op. E-403 (1998)(same); N.D. Ethics Op. 97-09 (1997)(same); Ohio Sup. Ct. Ethics Op 99-2 (1999); Vt. Ethics Op. 97-5 (1997). *See also* Ariz. Ethics Op. 97-04 (1997)(lawyers should use email cautiously and should consider encryption); Iowa Ethics Op. 97-1 (1997)(client must give written consent to transmission of information via email or internet, after disclosure of potential for loss of confidentiality); S.C. Ethics Op. 97-08 (1997)(lawyers may use email to communicate with clients but should discuss encryption options).

[12] RPC 252 (Jul. 18, 1997) required counsel to refrain from reviewing inadvertently disclosed materials due to obligation of honesty and courtesy to all persons involved in legal process, and required that counsel notify opposing counsel of receipt and follow opposing counsel's instructions re disposition of materials. The current version of Rule 4.4 only requires notification. Comment 2 specifies that the return or destruction of inadvertently disclosed documents is beyond the scope of the rules. However, both the federal and state rules of civil procedure were recently amended to codify (generally speaking) the steps outlined in RPC 252. *See* Fed.R.Civ.P. 26(b)(5)(B); N.C.Gen.Stat. § 1A-1, Rule 26(b)(5)(b)(2011). It is seems unusual that the Rules of Civil Procedure would provide more protection to inadvertently disclosed materials than the Rules of Professional Conduct. However, this helps illustrate the difficulty of Ms. Ewalt's inquiries and the conflicting ethical issues involved.

[13] *See, e.g., Van Alstyne v. Electronic Scriptorium*, 560 F.3d 199 (4th Cir. 2009)(employer liable to former employee for punitive damages under Stored Communications Act, 18 U.S.C. § 2707(a), when it accessed employee's personal email without her consent; employer's actions discovered when, during employee's deposition in post-termination Title VII case against employer, employer's counsel confronted employee with her own emails); *Leor Exploration & Prod'n LLC v. Aguiar*, No. 09-60136-CIV,

refer to moral and social factors that may be relevant to the situation. Rule 2.1. Ultimately, a lawyer may not engage in acts that are prejudicial to the administration of justice. Rule 8.4(d). *See also* Formal Ethics Opinion 1 (Jan. 15, 2010)(prohibiting counsel from searching for confidential metadata in electronic communications received from opposing party or counsel because doing so interfered with the other attorney's relationship with his/her client, "undermine[d] the confidentiality that is the bedrock of the relationship," and inhibited the efficient functioning of the modern justice system, thereby prejudicing the administration of justice, and requiring that counsel notify opposing counsel if information was inadvertently viewed, barring subsequent use of such information absent consent).

A Factors-Based Approach To Answering These Questions

Given the paucity of guidance in the Rules regarding this issue, it may be useful to consider how the courts have approached similar issues. Before turning to the cases, however, it is important to note that they do not address a lawyer's ethical obligations when faced with the circumstances of the two inquiries at issue here. Instead, the cases focus on whether, based on the specific facts and circumstances of each case,[14] the email communications between an employee to her personal attorney via an employer-provided email system are protected from use and/or disclosure in litigation based on the attorney-client privilege.[15]

The Council is aware of only one North Carolina case that has dealt with the applicability of attorney-client privilege to emails. In *Mason v. ILS Techs., LLC*, No, 3:04-CV-139, 2008 U.S.Dist.LEXIS 28905 (W.D.N.C. Feb. 29, 2008),[16] ILS's counsel produced, during the course of depositions, copies of email communications between the plaintiff, Mr. Mason, and Lee Rimler, his personal attorney, which were sent and received via the ILS email system and obtained by ILS from its email server and Mr. Mason's company-issued laptop. ILS also sought to depose Mr. Rimler regarding those emails. Magistrate Judge Keesler found that the communications were subject to attorney-client privilege under the Fourth Circuit's formulation of the rule:

2010 U.S.Dist.LEXIS 101824 at *35 (S.D.Fla. Sep. 28, 2010)(defendant's pleadings stricken and judgment entered as sanction after defendant obtained unauthorized access to plaintiff's privileged emails over a period of years, by which defendant gained an unfair advantage in the litigation: "Knowledge is power. Access to this protected information gives an opponent an unfair advantage that strikes at the heart of the adversarial system."). *See also* Fla. Prof. Ethics, Bar Op. 7-1 (Sep. 7, 2007)(attorney who receives email from client who was not authorized to access or disclose them must discuss with client the ethical dilemma presented by the client's actions in light of Rules 1.6 (confidentiality), 1.2(d)(cannot assist in fraudulent/criminal conduct), 8.4(a), (c), and (d)(cannot violate rules through acts of another), and 3.4(a)(duty to comply with discovery); must advise client that counsel is subject to disqualification for receiving or reviewing materials that were improperly obtained; must inform client that the client could be sanctioned; and must inform client that the materials cannot be retained, reviewed or used without informing the opposing party that the inquiring attorney and client have the documents at issue; if the client refuses to consent to disclosure the attorney must withdraw from the representation).

[14] It is beyond dispute that each situation in this context must be viewed on its individual facts. *O'Connor v. Ortega*, 480 U.S. 709, 718, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987)("Given the great variety of work environments, ... the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."). This is especially true where workplace email/internet/monitoring policies and practices can vary significantly from employer to employer.

[15] The attorney-client privilege is, undeniably, a more limited concept than the duty of confidentiality contained in Rule 1.6. *See* Rule 1.6, Comment [3]. As for emails from the employee/client to her attorney, it does not appear that Rule 1.6 is implicated as the employee's attorney has not disclosed (or potentially disclosed) "information relating to the representation of a client acquired during the lawyer's representation of th[at] client." Instead, it is the *client's actions* in sending the email to her lawyer via her employer's email system that created this issue. However, Rule 1.6 may be implicated when the employee's attorney responds to an email from the employee/client and directs this response to the employee's employer-provided email account.

[16] *Mason* was an employment law case involving the alleged non-payment of wages due pursuant to an employment agreement between Mr. Mason and ILS.

> Plaintiff sought to become a client of Mr. Rimler, ... Mr. Rimler is a member of the bar; ... the communications in dispute related to a fact of which Mr. Rimler was informed by his client, without the presence of strangers,[17] for purposes of securing either an opinion on law or legal services, and not for the purpose of committing a crime; and ... the privilege has been claimed and not waived.

Id. at **5-6.[18] The magistrate found that "the only close question" was whether Mason waived the privilege by using ILS's email system to transmit the emails to Rimler. In concluding that Mason had not waived the privilege, Judge Keesler focused on Mason's affidavit testimony (which was unrebutted by ILS) that he was unaware of any ILS policy prohibiting the personal use of the company email system or allowing for monitoring of email.[19] Based on this evidence, Judge Keesler concluded that "[i]f Plaintiff lacked knowledge of the email policy, and Defendant cannot show that Plaintiff was notified of that policy, then Plaintiff had a reasonable expectation of privacy and confidentiality in his email communications with his personal attorney." *Id.* at *10.[20]

A similar thread runs through cases on this issue from other jurisdictions as well. Specifically, the existence of a clear, unambiguous policy regarding email usage and monitoring that is effectively communicated to employees is a significant factor in determining (1) whether the privilege attached to the communications in the first instance and (2) if so, whether the client waived the privilege. Courts have considered a number of other factors as well. The relevant factors that can be gleaned from the case law are as follows:

1. Employer policy (*Convertino, Garrity, Holmes, In re Asia Global, Kaufman, Leor Exploration, Mason, Scott, Sims, Thygeson, Simon*[21]):
    a. Does the employer have a policy banning personal use of the employer's email or internet access?
    b. Did the employer's policy prohibit the specific use as to which a privilege may apply?
    c. Did the employer have a policy permitting email monitoring, to which the employee consented?
2. Employee Notice (*Convertino, In re Asia Global, Mason*) –
    a. Did the employer notify the employee of its use and/or monitoring policies?
    b. If so, how/when?

---

[17] On the facts presented – particularly Mr. Mason's belief that ILS had no email usage/monitoring policy – Magistrate Judge Keesler concluded that the emails were made in confidence and not in the presence of strangers.

[18] The elements of privilege under North Carolina law are similar: (1) relation of attorney and client at the time of the communication; (2) the communication was made in confidence, (3) the communication relates to a matter about which the attorney is being professionally consulted, (4) the communication is made in the course of giving or seeking legal advice for a proper purpose although litigation need not be contemplated, and (5) the client has not waived the privilege. *Brown v. American Partners Fed. Credit Union*, 645 S.E.2d 117 (N.C.App. 2007).

[19] Given Mason's clear testimony, Magistrate Judge Keesler declined to find that Mason *should* have known about an ILS's email usage policy that apparently existed.

[20] In reaching this conclusion, Judge Keesler cited *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 258 (S.D.N.Y. 2005), favorably and distinguished *Kaufman v. Sungard Inv. Sys.*, No. 05-CV-1236, 2006 U.S.Dist.LEXIS 28149 (D.N.J. 2006)(unpub.), as a case in which the employer had a clear, unambiguous policy regarding email usage and monitoring which it effectively communicated to its employees.

[21] *See* attached Appendix for the full citation and a brief synopsis of each of the italized case names referenced in this list.

c. Did the employee actually know about the employer's use and/or monitoring policies, or should the employee have known about them under all the circumstances?

3. Ambiguity:

   a. Is the employer's policy clear and unambiguous? (*Curto, Simons*);

   b. Did the employer make conflicting statements or have other policies that implied privacy? (*Holmes*)

   c. Did/does the employer actually monitor its employees' use of the employer's computers/email/internet access? (*Curto, Haynes, In re Asia Global, Leventhal)*

   d. Had the employer previously enforced its use/monitoring policies? (*Curto*)

4. Third Party Access:

   a. Do other workers have access to the employee's email account on the employer's system ? (*In re Asia Global, Leventhal*);

   b. Is the employee aware (via a policy or otherwise) that other employees have (or may have) access to her email account on the employer's system? (*In re Asia Global, Restuccia, Thygeson*)

5. Where/when did the potentially privileged communication occur (e.g., was the employee using a laptop in her home office and therefore may have had a subjectively greater expectation of privacy?)(*Curto*);

6. Did the employee take affirmative steps to preserve the privacy of the communication? (*Curto, Garrity, Holmes, Thygeson*)[22]

   a. Did the employee require password protection for access, which the employee did not know the employer had or could acquire?

   b. Did the employee save the password on the employer's device?

   c. Was the use of the employer-provided email system a one time, inadvertent error that the employee or her counsel sought to correct?

   d. Does the communication contain indicia of attorney communication (i.e., statement warning readers that emails are personal, confidential, and may be attorney-client communications)?

   e. Did the employee attempt to delete the email/file from the device to protect the privacy of the communication?

7. Was the employee's conduct so careless as to suggest that she was not concerned with the protection of the privilege? (*Curto*);

8. Public policy: What best balances and advances competing public policy considerations? (*Curto*)

Given the fact-intensive inquiry[23] necessary to determine whether the employee had a reasonable expectation of privacy in the email communications with her attorney via her employer's email system,[24]

---

[22] *See also* Fed.R.Evid. 502(b) (inadvertent disclosure will waive privilege and work product unless the holder of the privilege took reasonable steps to prevent disclosure, and promptly took steps to rectify the error).

[23] *See O'Connor v. Ortega*, 480 U.S. 709, 718, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987) and note 20, above.

it is the Council's view that the Bar's guidance regarding the inquiries here should incorporate the consideration of these factors. In our view there cannot be and should not be a bright line rule in this context. Rather, an employer's attorney in this situation should consider and analyze the above factors – objectively and independently, with due regard for the nature of the email communications and the fair administration of justice and in light of the lawyer's personal sense of professionalism – and advise the employer/client accordingly. Similarly, the Bar's response to these inquiries should also include guidance for attorneys representing employees regarding the risks of using an employer provided email system to communicate with clients.

We appreciate the opportunity to provide these thoughts to the Bar on this important and difficult issue. We would be pleased to provide further input, if that would be helpful to the Bar's determination. Please let us know if we can be of further assistance.

Sincerely,

Corie Pauling, Chair of NCBA Labor and Employment Law Section
Richard M. Klein, Chair of Labor and Employment Law Section's Ethics Committee
Laura Wetsch, Council Co-Chair and Member of Labor and Employment Law Council's Legislative Committee
Prof. Brian Clarke, Co-Chair of Labor and Employment Law Council's Legislative Committee
Nicole Gardner, Co-Chair of Labor and Employment Law Council's Legislative Committee

---

[24] As the cases make clear, if the employee's expectation of privacy was unreasonable then either (1) the attorney-client privilege never attached to the communication, in that the communication was not made "in confidence" or "without the presence of strangers" or (2) the employee/client waived the privilege by communicating with counsel through the employer's email system.

APPENDIX: Case list

Convertino v. US DOJ, 674 F.Supp.2d 97, 110 (D.D.C. 2009)(employee's expectation of privacy was reasonable (and privilege applied) where employer did not have policy banning personal use of employer email, employee did not intend for his employer to read his emails to legal counsel; and employee did not know employer would regularly access and save emails sent from employee's account);

Curto v. Medical World Comms. Inc., 2006 U.S.Dist.LEXIS 29387 (E.D.N.Y. 2006)(although employer had policy stating that employees had no expectation of privacy to, and expressly waived any right of privacy and authorized employer's access and review of, all materials created, stored, sent or received on the employer's computer system, and the employee signed two acknowledgements of that policy, employee did not waive attorney-client privilege or work product with respect to documents she previously deleted and employer forensically restored from its computers that she used from a home office; moreover, employer's limited enforcement of its policy created a false sense of security that lulled employees into believing policy would not be enforced

Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S.Dist.LEXIS 8343 (D.Mass. May 7, 2002)(plaintiff employees had no expectation of privacy with respect to sexually explicit emails they sent which were discovered during employer's investigation of co-worker complaint because, even though employer instructed employees in how to create "public" and "private" mail folders, the employer had a written policy prohibiting such emails that specified it would inspect when business or legal situations necessitated company review, the employees admitted the employer had the ability to look at emails on its intranet system, they knew they "needed to be careful" about sending emails, and they assumed that recipients of their emails might forward their offensive emails to others);

Haynes v. Office of the Attorney General, 298 F.Supp.2d 1154, 1161-62 (D.Kan. 2003)(employee had reasonable expectation of privacy despite computer screen warning that there was no such expectation of privacy, where there was no evidence public employer ever monitored private files or emails, employees were allowed to use computers for private emails, employers were told how to create "public" and "private" files, employees were told that unauthorized access to another's email was prohibited, and employees were given passwords to prevent access by others);

Holmes v. Petrovich Dev. Co., LLC, 191 Cal.App.4th 1047, 1068, 119 Cal.Rptr.3d 878, 896 (2011) (where employee believed her emails (and faxes) to lawyer would be private because she used a private password to access email and deleted emails after they were sent, and she had no knowledge of any actual access or auditing of the employer's computers, her belief was nevertheless unreasonable and therefore not protected by privilege, when the employer had expressly advised that email was only for company business, that emails were not private, that the employer would randomly and periodically monitor its technology resources to ensure compliance with the policy, and the employer never conveyed a conflicting policy);

In re Asia Global Crossing, Ltd., 322 B.R. 247, 258 (S.D.N.Y. 2005)(in considering whether employee has objectively reasonable expectation of privacy in emails sent to the employee's attorney over the employer's computer systems, court should consider (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, and explaining that "sending a message over [an] email system was like

placing a copy of that message in the company files. Short of encryption, ... [e]mails could be reviewed and read by anyone with lawful access to the system.");

Kaufman v. Sungard Inv. Sys., No. 05-CV-1236, 2006 U.S.Dist.LEXIS 28149 (D.N.J. 2006) (unpub.) (where employer's policy clearly stated that company property included all information stored on its computers and email, and that employer had right to access and inspect all electronic systems including password-protected computer files and email, and internet usage, employee had no reasonable expectation of privacy as to emails with counsel via company's laptop and email system);

Leor Exploration & Prod'n LLC v. Aguiar, No. 09-60136-CIV, 2009 U.S.Dist.LEXIS 87323 (S.D.Fla. Sept. 23, 2009)(employees did not have an objectively reasonable expectation of privacy with respect to memoranda their lawyer transmitted through the employer's server, where the employee handbook stated the employer owned all electronic communications, that individuals using its email system had no expectation of privacy, that the employer's representatives could access and monitor the use of its systems and equipment "from time to time," and that employees should not use the employer's electronic communications systems to communicate, receive, or store information that they wish to keep personal or private)

Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001)(the public employee had a reasonable expectation of privacy in contents of workplace computer where the employer's policy prohibited personal "use" but did not prohibit mere storage of personal materials in the office computer, the employer did not have a practice of unannounced searches of office computers and only engaged in infrequent and selective searches for maintenance purposes or to retrieve a needed document, and the employee had exclusive use of his computer, desk and file cabinets);

Mason v. ILS Techs., LLC, No, 3:04-CV-139, 2008 U.S.Dist.LEXIS 28905 (W.D.N.C. Feb. 29, 2008) (where employee testified he did not know of employer's policy with respect to personal use and monitoring of emails transmitted through the employer's system, and employer could not prove that he did, attorney-client privilege was not waived);

Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002)(in case where employee was arrested for receiving and possessing child pornography on employer's laptop and then sued employer for violating his federal/state rights when it turned that evidence over to federal authorities, court ruled, "If the [private] employer equips the employee's office with a safe or file cabinet or other receptacle in which to keep his private papers, he can assume that the contents of the safe are private. ... But Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and thus destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim.");

Restuccia v. Burk Tech., 5 Mass.L.Rep. 712, 1996 Mass.Super.LEXIS 367 (Mass.Super.Ct. 1996) (employees terminated for "excessive talking" could have reasonable expectation of privacy for purposes of invasion of privacy claim, where employer had no policy prohibiting using company email system for personal messages, employees were not told that supervisor had access to their email via supervisory passwords, and employees were not specifically told that their computer files (including email messages) were automatically saved onto back-up files to which supervisors had access);

Scott v. Beth Israel Medical Center, Inc., 17 Misc.3d 934, 847 N.Y.s.2d 436, 441-43 (N.Y.Sup.Ct. 2007) (attorney-client privilege did not exist when company computer was used to send emails, and the

company's policy prohibited the personal use of emails, warned they were not private, and stated they could be monitored);

Sims v. Lakeside School, No. CO6-1412RSM, 2007 U.S.Dist.LEXIS 69568 (Sep. 20, 2007)(employee did not have reasonable expectation of privacy in the contents of his employer-provided laptop or the emails sent/received using the employer's email accounts, where employee manual clearly stated that user accounts and email on its computer networks were the employer's property, could be used for academic and administrative purposes only, and its laptops were subject to inspection);

Thygeson v. U.S. Bancorp Equip. Fin. 'g, Inc., No. CV-03-467-ST, 2004 U.S.Dist.LEXIS 18863 (D.Or. Sept. 15, 2004)(private employee could not prevail on invasion of privacy claim with respect to emails from the employer's email account saved in a "personal" folder on his work computer, because the employer had express warnings in its employee handbook that personal use was prohibited and monitored, and transmission of those emails through the employer's server necessarily made those emails accessible by third parties, so that the employer "retained the key" to the employee's "lock");

United States v. Simons, 205 F.3d 392, 398 (4th Cir. 2000)(government employer's policy stating that electronic auditing *shall* be implemented, and that users *shall* understand that employer will periodically audit, inspect, and/or monitor the user's internet access (including "all file transfers, all websites visited, and all e-mail messages") was sufficient to place employees on notice that they could not reasonably expect their internet activity would be private)