Confidentiality in the Digital World

Aviva Meridian Kaiser, Ethics Counsel
State Bar of Wisconsin

A Little Humor

Peep Shenanigans!

Oh this is bullshit...
SCR 20:1.6(a) "Shall Not Reveal" and SCR 20:1.6(b) "Shall Reveal"

"(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in pars. (b) and (c).
(b) A lawyer shall reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to prevent the client from committing a criminal or fraudulent act that the lawyer reasonably believes is likely to result in death or substantial bodily harm or in substantial injury to the financial interest or property of another."

SCR 20:1.6(c) "May Reveal"

"(c) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
(1) to prevent reasonably likely death or substantial bodily harm;
(2) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;
(3) to secure legal advice about the lawyer's conduct under these rules;"
SCR 20:1.6(c) "May Reveal"

"(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; (5) to comply with other law or a court order; or (6) to detect and resolve conflicts of interest, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client."

SCR 20:1.6(d): Acting Competently to Preserve Confidentiality

"(d) 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."
ABA Comment [18] to SCR 20:1.6(d)
Acting Competently to Preserve Confidentiality

- "SCR 20:1.6(d) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.
- The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (d) if the lawyer has made reasonable efforts to prevent the access or disclosure."

ABA Comment [18] to SCR 20:1.6(d)
Acting Competently to Preserve Confidentiality

"Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to,
- the sensitivity of the information,
- the likelihood of disclosure if additional 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)."
- See also Wisconsin Revised Formal Ethics Opinion EF-15-01
SCR 20:1.1 ABA Comment [8]

- "[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

Competence and Functionality

New York City Bar Association Formal Opinion 2012-2

- A lawyer must understand the functionality of any social media service he or she intends to use.
- If an attorney cannot ascertain the functionality of a website, the attorney must proceed with great caution.
A Functionality Example: The Extent of the Data Held by Facebook

- Consider an Android smartphone user who has installed Facebook on his smartphone and has given Facebook access to his contacts.
- When this Android user places a cell phone call or text message, Facebook captures a record of who he called or texted, even though he was not using the Facebook application to place the call or text message.
- What if this Android user was a lawyer and was communicating with a client who had originally contacted him through his Facebook page?

Dylan McKay
@dylanmckayrc

metadata about every text message I've ever received or sent

spoiler: I don't use messenger for SMS
A Functionality Example: The Extent of the Data Held by Facebook

- Consider now any smartphone user, not just an Android user, who has installed Facebook on her smartphone and has given Facebook access to her contacts.
- Facebook now has a record of all contacts on the user's smartphone.
- In addition, Facebook logs and tracks all messages that occur on the Facebook Messenger application, unless the message is deleted by both sender and receiver. Even if one user deletes the message, it would still appear on the other user's application.

Mocking Lawyer Posts Photo of Her Client's Leopard Print Underwear on Facebook Causing Mistrial in Murder Case
The defendant’s family brought him a fresh set of clothes to wear during his trial for stabbing his girlfriend to death.

While the clothes were being held up for routine inspection, his lawyer snapped a photo of his underwear on her cell phone.

During a break, his 31-year-old lawyer posted the picture to her personal Facebook page with a mocking caption suggesting that the defendant’s family believed the animal print underwear was ‘proper attire for trial’.

Although her Facebook page is only open to her friends, someone who saw the photo reported it to the judge.

The judge declared a mistrial, and the lawyer was immediately fired from representing the defendant.

The Public Defender said that clients are entitled to lawyers’ loyalty and respect; posting humiliating photos undermines the client-lawyer relationship.

---

Treat Every Email with Caution!
No Phishing Here!

- Most “phishing scams” happen by email.
- Phishing scams are generally an attempt to get you to hand over sensitive personal details. They often appear as emails or messages from a legitimate company and request that you send personal details in reply or click a link in an email to be taken to a website where you will be asked for log in details.
- These website fronts are false, although they may look like the real thing, and if you input your details then the scammers can use them to steal your or your client’s identity.
Watch Out for Spoofed Emails!

- Often emails will show only the name of the sender and not the full email address. When you reply to that email, you may be replying to someone posing as your client. Think it can’t happen to you?

Watch Out for Spoofed Emails!

WilmerHale partner Jamie Gorelick, who represents Jared Kushner for his ethics and security-clearance needs, fell for an internet prankster.

- Starting the evening of Sept. 30, a person using the email Kushner,jared@mail.com sent Gorelick a one-sentence email: “Our mutual friend Mr. McGahn is really stirring things up,” referring to current White House Counsel, Donald McGahn. “What is he doing?” Gorelick replied.

- After the phony Kushner expressed more frustration with McGahn, Gorelick wrote back: “I can speak with him as I need to call him anyway.” Gorelick then told the emailing twice that the rest of their communication would have to wait until Monday. Gorelick stopped responding after 1:30 a.m. Sunday, after she got five emails from the address.

- Gorelick then realized that she wasn’t emailing with her client. Her excuse was that she responded while on her iPad which only displays the screen name, not the full email address.
Watch Out for Spoofed Emails!

Gorelick should have learned from Norton Rose Fulbright partner, Abbe Lowell, who got fooled by the same prankster using the exact same spoofed email address.

- Lowell received an email from kushner.jared@gmail.com asking his advice about dealing with embarrassing emails featuring adult content sent to his personal email address from a White House official. "Can I remove these?" the prankster asked.
- "Forwarded or received from WH officials?" Lowell responded.
- "I think one was forwarded from a White House official, we had discussed a shared interest of sorts," the prankster said. "It was unsolicited. Then there are a handful more, but not from officials."
- "I need to see I think all emails between you and WH (just for me and us)," Lowell wrote.
- "But we can bury it?" the prankster responded. "I'm so embarrassed. It's fairly specialist stuff, half naked women on a trampoline, standing on legs... the tag for the movie was #standingOnTheLittlePeople:"
- Lowell replied: "Don't delete. Don't send to anyone. Let's chat in a bit."

“You Complete Me”: Not Always a Good Idea!

- Be cautious when using your email program’s “auto-complete” feature.
- Auto-complete is a feature in which an application predicts the rest of a word a user is typing. In your email program, it is the one that pops up names/email addresses as soon as you start to type them.
- A staffer at Wilmer Hale, one of the world’s largest and most prestigious law firms, sent client confidential SEC-Whistleblower strategies of PepsiCo, the client, to the Wall Street Journal by accident.
- How could this happen? The staffer was sending the internal client secret memo to other staffers and accidentally added a journalist at the Wall Street Journal as one of the recipients. It appears that the email program’s "auto-complete" feature populated the journalist's address, and the staffer who sent the email did not notice.
To Encrypt or Not To Encrypt: That Is the Question

ABA Formal Opinion 99-413
- "Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."

To Encrypt or Not To Encrypt: That Is the Question

ABA Formal Opinion 477R (2017)
- "In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication."
To Encrypt or Not To Encrypt: That Is the Question

• “However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.”

To Encrypt or Not To Encrypt: That Is the Question

• “A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances.”
• “Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters.”
• “For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it, and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.”
To Encrypt or Not To Encrypt: That Is the Question

Wis. Stat. § 134.98 Notice of Unauthorized Acquisition of Personal Information

(b) "Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:

1. The individual's social security number.
2. The individual's driver's license number or state identification number.
3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a).
5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation."

The Risks of Blind Carbon Copies and Reply to All

- A New York ethics opinion mentioned the risks of using blind carbon copies as a way to communicate with a client. If the client uses the "reply to all" function, that new correspondence may inadvertently be sent to the opposing counsel.
- As a result, it is a far better practice for the lawyer to send a copy of the email correspondence to himself or herself and then forward that correspondence to the client to avoid the potential of an inadvertent communication to the opposing counsel or someone else.

- Lawyers comment on legal topics in various formats.
- The newest format is online publications such as blogs, listserves, online articles, website postings, and brief online statements or microblogs (such as Twitter®) that "followers" read.
- Lawyers continue to present education programs and discuss legal topics in articles and chapters in traditional print media such as magazines, treatises, law firm white papers, and law reviews. They also make public remarks in online informational videos such as webinars and podcasts (collectively "public commentary").


- Lawyers who communicate about legal topics in public commentary must comply with the Rules of Professional Conduct, including the Rules regarding confidentiality of information relating to the representation of a client.
- A lawyer must maintain the confidentiality of information relating to the representation of a client, unless that client has given informed consent to the disclosure, the disclosure is impliedly authorized to carry out the representation, or the disclosure is required by SCR 20:1.6(b) or is permitted by SCR 20:1.6(c).

- The plain language of SCR 20:1.6 dictates that information relating to the representation, **even information that is provided in a public judicial proceeding**, remains protected by the duty of confidentiality.
- Rule 1.6 does not provide an exception for information that is "generally known" or contained in a "public record." Accordingly, if a lawyer wants to publicly reveal client information, the lawyer must comply with SCR 20:1.6.
- A lawyer may not voluntarily disclose such information, unless the lawyer obtains the client's informed consent, the disclosure is impliedly authorized to carry out the representation, or another exception in SCR 20:1.6(b) or (c) applies.

The Transmission and Receipt of Electronic Documents Containing Metadata

Wisconsin Formal Ethics Opinion EF-12-01 (Revised April 27, 2018) provides the following guidance.

- A lawyer who processes and transmits electronic documents containing information relating to the representation of clients to third parties must act competently to prevent the disclosure of significant information in the form of metadata contained in such documents.
- A lawyer who receives an electronic document is not prohibited by the Rules from searching for metadata contained in such a document. However, a lawyer who chooses to review such a document for metadata and discovers information of material significance must normally assume such information was inadvertently disclosed and comply with SCR 20:4.4(b) or (c).
The Transmission and Receipt of Electronic Documents Containing Metadata

- A lawyer who reviews an electronic document for metadata and discovers information that the lawyer knows or reasonably should know is protected by the lawyer-client privilege or the work product rule that has been disclosed inadvertently, must comply with SCR 20:4.4(c). Paragraph (c) requires the lawyer to immediately terminate review or use of the document or electronically stored information, promptly notify the person or the person's lawyer if communication with the person is prohibited by SCR 20:4.2 of the inadvertent disclosure, and abide by that person's or lawyer's instructions with respect to disposition of the document or electronically stored information until obtaining a definitive ruling on the proper disposition from a court with appropriate jurisdiction. If the lawyer does not know or cannot reasonably know that the inadvertently disclosed information is protected by the lawyer-client privilege or the work product rule, the lawyer is required by SCR 20:4.4(b) to promptly notify the sender.
- Lawyers are not required to routinely search electronic documents for metadata.

*Thank You!*