Ethics Issues in Email and Third-Party Software*

(*Read the Terms of Service Agreement!)

By Michael D. Witt and Nicholas J. Goldsworthy

At a Glance

The surge in the number of individuals and businesses working from home and increased reliance on various online communication platforms has heightened the risk of a data breach due to a cyberattack and disclosure of client confidences to third parties. Legal professionals should ask themselves: Do I know enough about the technology to communicate sensitive information and am I doing enough to uphold my ethical duty to maintain client confidences?

Unfettered private communications between attorneys and clients have long been protected under common law and are a bedrock principle of American jurisprudence. The vigorous use of electronic communications during the COVID-19 outbreak heightens the need for attorneys to understand new and developing technologies and how using those technologies impact attorney-client confidentiality. Due to the utility of email and other online communication platforms like Zoom, Microsoft Teams, and Slack, law firms employ these various tools widely to communicate with clients under the assumption they are protected by attorney-client privilege.

But are they? What potential is there for inadvertent disclosures due to cyberattacks or, perhaps worse yet, through authorization by the firm itself when it adopts third-party software technologies?

With a growing number of cyberattacks and a variety of communication platforms, lawyers must be diligent in selecting email and third-party software services. By reviewing the firm's existing information technology security policies, including an extensive review of the terms of service (TOS) of email and third-party software providers used to communicate client confidences, law firms can mitigate the risk of a data breach and avoid ethics violations.

Business email compromise

In the United States, companies saw a 29 percent increase in the cost of cybercrime between 2017 and 2018.[1] Of the various cyberattacks, business email compromise/email account compromise (BEC/EAC) is among the most common. The FBI's Internet Crime Report highlights crimes reported by businesses and individuals to the Internet Crime Complaint Center (IC3); its "Hot Topics for 2019" report showed it received more than 23,000 BEC/EAC complaints with adjusted losses of more than $1.7 billion for that year.[2] The IC3 characterizes BEC/EAC as a "sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests."[3] One variation involves compromising legitimate business email accounts and requesting employees' personally identifiable information or W-2 forms. In 2018, Michigan ranked among the top 10 states for BEC/EAC losses[4] with more than $27 million in losses to businesses and individuals in the state.[5]

For law firms, instances of BEC/EAC magnify exposure for both the firm and the client whose data was breached. If the firm causes the breach through sloppy security practices, the client may suffer identity theft, fraud, negative publicity, and financial loss. Similarly, the firm must face the consequences, including potential violations of the Michigan Rules of Professional Conduct (MRPC) 1.1 regarding competence and MRPC 1.6 regarding confidentiality of information.

Attorney use of email and confidentiality

Email has been around for a while, but it hasn't always an acceptable form of communication for attorneys because its use would have violated the duty to safeguard client confidences. Before Congress made intercepting email a crime,[6] the American Bar Association and several state bars considered unencrypted email too insecure. Within two years of Congress passing the National Information Infrastructure Protection Act,[7] the ABA issued a formal opinion stating that attorneys now had a reasonable expectation of privacy when using *unencrypted email*.[8]

The ABA 20/20 Committee on Ethics updated its Model Rules of Professional Conduct in 2012 to provide guidance regarding attorneys' use of technology and confidentiality.[9] Most notably, ABA Rule 1.6 (Confidentiality) was changed by adding subsection (c): "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to representation of a client." A violation of MRPC 1.6(b), in contrast, would require a lawyer to knowingly reveal client confidences. Despite the differences between ABA Rule 1.6 and MRPC 1.6, attorneys may violate either or both by failing to review the email service provider's TOS. Under ABA Model Rule 1.6, the lawyer could be viewed as failing to make reasonable efforts to prevent the unauthorized disclosure of information relating to representation of a client; under MRPC 1.6, the lawyer could be viewed as knowingly revealing client confidences by using an email service provider—or any other third-party communication platform—if the TOS grant the provider an interest in the content of the communication, which is often in the form of a license. If the TOS license terms are sufficiently broad, the standard for violating MRPC 1.6(b)—knowingly revealing client confidences—is surprisingly easy to trip over.

Competence and confidentiality

MRPC 1.1 requires lawyers to provide "competent representation to a client." Regarding maintaining competence, the comments to MRPC 1.1 suggest that lawyers "should engage in continuing study and education, including the knowledge and skill regarding existing and developing technology that are reasonably necessary to provide competent representation for the client in a particular matter." Failure to stay abreast of existing and developing technology can lead to violating MRPC 1.6. Without careful inspection of incoming emails, firms and businesses are at risk of a data breach, be it from BEC/EAC or some other cyberattack. Similarly, these organizations should carefully scrutinize the method of communication and the TOS of email and software service providers. To meet the standards of MRPC 1.1 and 1.6, legal professionals must ask themselves: do I know enough about the

technology to communicate sensitive client information, and am I doing enough to uphold my ethical duty to maintain client confidences?

The answer depends on the email provider and/or third-party communication software used by the firm, the TOS agreements, and a diligent review of those agreements. By glossing over the TOS without careful review ("click here to accept the Terms of Service Agreement"), attorneys may unknowingly reveal client confidences or secrets.

Review the TOS

When using email, attorneys should be concerned about risks to confidentiality due to the general legal uncertainty of privacy expectations for email, broad waivers of email privacy through an email provider's TOS, and disclosures to third parties—particularly third-party applications. Attorneys must understand the TOS related to existing and developing technologies so they may effectively communicate the risks to clients, who need to understand them before providing informed consent. In this regard, MRPC 1.6(c)(1) reads, in relevant part "[a] lawyer may reveal confidences or secrets with the consent of the client or clients affected, but only after full disclosure to them[.]" The lawyer is thus required to inform the client of the risk of waiving the attorney-client privilege through the use of an email service provider that allows a third party (e.g., the email service provider) to access the content of communications.

Know how to identify bad TOS

Since we all use email, consider the example of the most commonly used free provider: Google's Gmail. When reviewing the TOS of any email service provider, lawyers must carefully review how the provider defines "content"; transfers of ownership of any intellectual property contained therein; and any licenses to the email provider to use the information being transmitted. License grants of content, if any, should be limited only to the service provider for the limited purpose of improving email service to the user. If the provider requests a broad license grant of content for its use—perhaps with the right to sublicense content to third parties—the risk of violating client confidences is high.

Gmail users grant Google a license to use email content—including attorney-client communications intended to be treated as confidential—in almost any manner.

Google's TOS, especially as it relates to email content and how it uses that content, is notorious and beyond the scope of reasonable. Under its TOS, Google defines content as "things you write, upload, submit, store, send, receive, or share with Google using our services, such as…emails you send through Gmail."[10] Gmail users grant Google a license to use email content—including attorney-client communications intended to be treated as confidential—in almost any manner. In relevant part, the Google's TOS reads as follows:

> Some of our services are designed to let you upload, submit, store, send, receive, or share your content. You have no obligation to provide any content to our services and you're free to choose the content that you want to provide. If you choose to upload or share content, please make sure you have the necessary rights to do so and that the content is lawful.
>
> Your content remains yours, which means that you retain any intellectual property rights that you have in your content. For example, you have intellectual property rights in the creative content you make, such as reviews you write. Or you may have the right to share someone else's creative content if they've given you their permission.
>
> We need your permission if your intellectual property rights restrict our use of your content. You provide Google with that permission through this license.
>
> This license is:
>
> - worldwide, which means it's valid anywhere in the world.
> - non-exclusive, which means you can license your content to others.
> - royalty-free, which means there are no fees for this license.
>
> This license allows Google to:
>
> - host, reproduce, distribute, communicate, and use your content—for example, to save your content on our systems and make it accessible from anywhere you go.
> - publish, publicly perform, or publicly display your content, if you've made it visible to others.
> - modify and create derivative works based on your content, such as reformatting or translating it.
> - sublicense these rights to:
>   - other users to allow the services to work as designed, such as enabling you to share photos with people you choose.

- our contractors who've signed agreements with us that are consistent with these terms, only for the limited purposes described in the Purpose section below.

This license is for the limited purpose of:

- operating and improving the services, which means allowing the services to work as designed and creating new features and functionalities. This includes using automated systems and algorithms to analyze your content:
  - for spam, malware, and illegal content.
  - to recognize patterns in data, such as determining when to suggest a new album in Google Photos to keep related photos together.
  - to customize our services for you, such as providing recommendations and personalized search results, content, and ads (which you can change or turn off in Ads Settings).
- using content you've shared publicly to promote the services. For example, to promote a Google app, we might quote a review you wrote. Or to promote Google Play, we might show a screenshot of the app you offer in the Play Store.

In short, Google "…can host, reproduce, communicate, and use your content…developing new technologies and services for Google consistent with these terms."[11] This analysis occurs as the content is sent, received, and when it is stored. By granting this license, client and attorney communication is shared with a third party, destroying the privilege of attorney-client communications under MRPC 1.6.

Creating a Gmail account requires users to first create a Google account, which in turn requires one to agree to Google's TOS before using any of its products. The offending clause is not listed on the account signup page; rather, you must open a different link to read the complete TOS agreement. As is common with most point-and-click agreements, many users gloss over the license language and by accepting the terms without a complete understanding of the property rights conferred, the user grants Google a limited license to the content of their communications.

Despite limiting language that appears to protect the user's rights of intellectual property ownership, Google's license is not limited to improving Gmail's services. On the contrary, based on a plain reading of the TOS, Google could use your information—or worse, your client's information—to develop new services unrelated to Gmail. The TOS are not restricted to Gmail; Google's TOS apply to almost every software service it offers. To further cement its rights in your content, the user agrees to a term "for as long as your content is protected by intellectual property rights."[12] Signing up for and using Gmail may be free, but if you communicate client confidences using this service, you likely violate MRPC 1.1 and 1.6(b) which, depending on the sensitivity of the information communicated, could cost your license to practice law.

Google allows third-party developers to read your emails

The Wall Street Journal reported in 2018 that Google continues to allow third-party application developers to scan and share data from Gmail accounts if Google determines the privacy policies of those developers adequately disclose potential uses.[13] The article further revealed that "outside app developers can access information about what products people buy, where they travel and which friends and colleagues they interact with the most. In some cases, employees at these app companies have read people's actual emails in order to improve their software algorithms."[14] This appears to still be the case, as Google's TOS permit them to "sublicense these rights to…our contractors."[15]

If a lawyer has read and agreed to Gmail's TOS or knows of the ability of third-party application developers to read emails sent through Gmail, he or she is likely to have knowingly violated MRPC 1.6(b)(1) by continuing to use Gmail to communicate with clients.

Inform your clients

Attorneys should adopt the practice of informing clients at the outset of an engagement that using Google's services constitutes a waiver of attorney-client privilege—specifically, Google's TOS agreement grants a third party (Google and Google's contractors) license to purportedly confidential communications. In the litigation context, this waiver would have to be disclosed where the privilege is asserted. By adopting this practice of informing clients at the outset of an engagement, attorneys can uphold their ethical obligations under MRPC 1.1 and MRPC 1.6(b).

TOS of other common email providers

Google is not the only email service provider with a troublesome TOS. By way of comparison, other free email providers, as a condition to using the service, also require prospective users to grant a limited license to content, but how the content is used or how "content" is defined varies. In granting a license to your content, some providers restrict the use of that content to enhance the delivery of the provider's services[16] and the license terminates when the user terminates use of the service.[17] Other providers limit the license where your content is published in areas accessible to the public.[18] Still other free email service providers do not have access to the content of your email messages.[19] The TOS of these

providers do not require granting a license as a condition to using their services[20] and providers cannot read any of the emails in the user's inbox.[21]

Key takeaways

Attorneys should understand the technology they elect to use before adopting it as part of regular practice. Carefully review providers' TOS to ensure that the content of any communications will not be revealed to anyone but the attorney and client. The increase in businesses and individuals working remotely has increased reliance on email and other communication platforms. As a consequence, there is an increased risk of a cyberattack; email appears to be the most susceptible to an attack and subsequent data breach.

Firms of all sizes should evaluate existing information security policies, including a thorough review of the TOS of all software products that can read, write, or otherwise access confidential client information. Attorneys must weigh the utility of the services offered by email and software service providers against the risk that the TOS of those providers exposes client confidences. Law firms should avoid any service provider whose TOS require a broad license grant and an expansive definition of "content." If clients utilize a service provider whose TOS contain similarly broad language, the attorney should inform the client of the risks of using the service. If the content of the communication is particularly sensitive, attorneys should counsel their clients to communicate on a platform that does not grant the provider carte blanche to it. By adopting these practices, attorneys uphold their ethical obligations under MRPC 1.1 and MRPC 1.6. ■

Michael D. Witt, PharmD, JD is a partner at Witt & Howard, PLLC and entrepreneur in residence and lecturer at the University of Michigan–Flint School of Management. His practice areas include technology licensing, early-stage venture business development, healthcare law, and general corporate practice. He is licensed to practice in Michigan, California, and Massachusetts.

Nicholas J. Goldsworthy, JD is an associate at Witt & Howard, PLLC. His practice area includes working with startup, family, and closely held businesses and e-commerce businesses. He is licensed to practice in Michigan, Wisconsin, and Illinois.

ENDNOTES

1. *The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study*, Ponemon Inst, LLC (2019), available at <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50> [https://perma.cc/3C38-BU2Z]. All websites cited in this article were accessed February 24, 2021.
2. *2019 Internet Crime Report*, Internet Crime Complaint Center, FBI, available at <https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf>.
3. *Business E-Mail Compromise—The $26 Billion Dollar Scam*, Alert No I-091019-PSA, FBI (September 10, 2019) <https://www.ic3.gov/media/2019/190910.aspx#ref3> [https://perma.cc/TXM6-LLZC].
4. *Id.*
5. *Internet Crime Report*, Internet Crime Complaint Center IC3, FBI (2018), available at <https://www.ic3.gov/media/annualreport/2018State/StateReport.aspx#?s=25> [https://perma.cc/J4G2-CBEK].
6. 18 USC 2511.
7. PL 104-294; 110 Stat 3488.
8. Formal Op 99-413, ABA Comm on Ethics & Prof'l Responsibility (1999), available at <https://cryptome.org/jya/fo99-413.htm> [https://perma.cc/5PU2-XFYX].
9. 105A Revised: Resolution, ABA Comm on Ethics 20/20 (2012), p 3, available at <https://www.americanbar.org/groups/professional_responsibility/committees_commissions/aba-commission-on-ethics-20-20/> [https://perma.cc/AZ4Y-N7TW]. The comment to ABA Rule 1.1 Competence was amended to add "including the benefits and risks associated with technology."
10. *Terms of Service*, Google (March 31, 2020), available at <https://policies.google.com/terms?hl=en#footnote-your-content> [https://perma.cc/RA7U-YNZ9].
11. *Id.*
12. *Id.*
13. McKinnon & MacMillan, *Google Says It Continues to Allow Apps to Scan Data From Gmail Accounts*, Wall Street Journal (September 20, 2018) <https://www.wsj.com/articles/google-says-it-continues-to-allow-apps-to-scan-data-from-gmail-accounts-1537459989> [https://perma.cc/7N9Y-HQGD].
14. *Id.*
15. *Terms of Service.*
16. *Services Agreement*, Microsoft (October 1, 2020), available at <https://www.microsoft.com/en-us/servicesagreement> [https://perma.cc/N74F-X4A8].
17. *Id.*
18. *Welcome to iCloud*, Apple (September 19, 2019), available at <https://www.apple.com/legal/internet-services/icloud/en/terms.html> [https://perma.cc/BC33-PES7].
19. E.g., see ProtonMail <https://protonmail.com/> [https://perma.cc/79D7-ET42] and Tutanota <https://tutanota.com/pricing> [https://perma.cc/S5LB-CXPX].
20. https://protonmail.com/terms-and-conditions.
21. *Ask Your Question: What is encrypted?*, ProtonMail <https://protonmail.com/support/knowledge-base/what-is-encrypted/#:~:text=All%20messages%20in%20your%20ProtonMail,them%20over%20to%20third%20parties.&text=Subject%20lines%20and%20recipient%2Fsender,end%2Dto%2Dend%20encrypted> [https://perma.cc/5NWQ-4BHR].