CLYDE&CO | GEMINI RISK PARTNERS

Lawyers' Risk Management Newsletter

January 2023

The Scope of the Duty to Protect Client Confidences – Both When Traveling and Generally

Now that lawyers and clients are traveling to meetings again, even if with less frequency than before the pandemic, it is worth considering lawyers' ethical responsibilities to preserve client's confidential information when on the road, and their duties to advise their clients of the protections required of the clients themselves to preserve confidentiality and privilege while on the move.

In Fourth Dimension Software v. Der Touristik Deutschland GMBh, No. 19CV05561CRBAGT, 2021 WL 4170693, at *1 (N.D. Cal. Sept. 14, 2021), the parties had a discovery dispute about whether attorney-client privilege was waived when plaintiff Fourth Dimension Software's ("FDS") President and CEO, Ilya Pavolotsky, forwarded an email from former in-house counsel, John Pavolotsky, to a hotel front desk at "info.berlin@hilton.com," with the subject line "Please print one copy. I'm waiting at the front desk. Thanks." The Court found that FDS failed to demonstrate that Ilya's disclosure to the hotel front desk was a reasonably necessary exception to waiver by disclosure. Id. at *3. The Court found that disclosure to a general email address for printing was not necessary to transmit the information, especially considering Ilya was already in possession of John's email. Id.

In addition, the Court found that there was no indication that Ilya intended or reasonably expected the communication to be treated as confidential. Id. Specifically, Ilya forwarded the email to a generic email address that any number of hotel staff presumably could access and the email contained no confidentiality warnings or other language alerting the recipient(s) not to read or share its contents and to delete it after printing. Id. The client's waiver of the attorney-client privilege in this case thus serves as a valuable reminder of an attorney's (and their client's) responsibility of maintaining confidentiality of electronic communication when traveling or working remotely.

Lawyers need to be mindful of ABA Model Rule ("Rules") 1.6(c) (and most states' equivalents), which requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to" the confidential information of current, former and prospective clients. Rule 1.6(a), in turn, provides that confidential information consists of "information relating to the representation of a client."

Rule 1.1 governing competence is equally central to lawyers' duties the context of cybersecurity, reminding lawyers to "keep abreast… [of] the benefits and risks associated with relevant technology." Rule 1.1, cmt. [8]. A lawyer's duty to remain technologically competent also implicates the lawyer's ethical duties regarding diligence (Rule 1.3), communication (Rule 1.4), confidentiality (Rule 1.6) and supervisory standards (Rules 5.1, 5.2 and 5.3). *See* ABA Eth. Op. 498 (2021); MI Eth. Op. RI-381 (2020); PA Eth. Op. 2020-300 (2020); IL Adv. Op. 18-01 (2018); OH Adv. Op. 2017-05 (2017); CT Eth. Op. 07 (2013); VA Legal Eth. Op. 1872 (2013); CA Eth. Op. 2012-184 (2012); PA Eth. Op. 2011-200 (2011). Helpful guidance may also be found in ABA Formal Opinion 477R (2017), which notes that lawyers have a variety of options when seeking to safeguard communications such as securing access methods, password management, implementing firewalls and cybersecurity software on all devices that store

confidential information, updating security patches for operational and communications software, and data encryption.

In sum, lawyers must make reasonable efforts to prevent the unauthorized access of a client's information. Because electronic devices are more susceptible to unintended unauthorized access, lawyers must be mindful that any electronic devices are susceptible to interceptions that can range from a smartphone app accessing client contacts, an email service provider scanning emails, and border patrol agents securing and inspecting a phone. NYSBA 1240 (2022); NYC 2017-5 (2017); NYSBA 820 (2008). Nevertheless, it is common practice, recognized in the ethics opinions, to use emails that are not encrypted, telephones that are not "scrambled," faxes that are not "coded," and mail that is not hand delivered by an office courier — even though all of these communications can be intercepted by unintended third parties. And in normal circumstances there is no requirement of special mitigating efforts in those contexts because interception is unlikely. ***See***, e.g., CT 99-52 (1999); AK 98-2 (1998); D.C. 281 (1998); IL 96-10 (1997); VT 97-5 (1997); SC 97-08 (1997).

However, Comment [16] to Rule 1.6 points out that Rule 1.6(b) permits "disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose." To that end, "the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable." In addition, since the rule standard is "reasonable efforts," if in fact client confidential information is compromised, the client is likely to argue that the lawyers' efforts failed to meet the reasonableness standard, and perhaps violated the lawyer's duty of care. Accordingly, lawyers are well advised to explain to all their clients at the time of the initial engagement (presumably in the engagement letter) what the lawyers' standard protections regarding preserving confidentiality and technology use are, and to give clients the opportunity to request special or additional protections.

Finally, lawyers (and their clients) should not share confidential information with third parties unless that individual is serving as an agent of either the attorney or the client. Green v. Beer, 2010 WL 3422723 (S.D.N.Y. 2010) (Wood, J.) (no waiver when party, due to lack of technical proficiency, necessarily relied on son to send and receive e-mails to counsel). This includes correspondence over a client's employer's email address. In re Reserve Fund Sec. & Derivative Litig., 275 F.R.D. 154, 164 (S.D.N.Y. 2011) ("Because Bent II had no reasonable expectation of privacy in emails he sent over RMCI's system, they were not sent 'in confidence' and are not protected by the marital communications privilege"). Again, it is prudent to alert clients of these issues at the outset of engagements.

Further information

If you would like further information on any issue raised in this update please contact:

Contacts

David B. Kramer
Principal, Gemini Risk Partners, LLC
dkramer@geminiriskpartners.com
+1 248 433 7604

Theo C. Nittis
Principal, Gemini Risk Partners, LLC
tnittis@geminipartners.com
+1 248 433 7934

J. Richard Supple, Jr.
Partner, Clyde & Co LLP
richard.supple@clydeco.us
+1 212 710 3914

Anthony E. Davis
Of Counsel, Clyde & Co LLP
anthony.davis@clydeco.us
+1 212 710 3976

Janis M. Meyer
Of Counsel, Clyde & Co LLP
janis.meyer@clydeco.us
+1 212 710 3942

Aaron Lawson
Associate, Clyde & Co LLP
aaron.lawson@clydeco.us
+1 212 702 6778