UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

32nd Annual Conference on State and Federal Appeals

June 16-17, 2022
Austin, Texas

What Every Attorney Needs to Know About Cybersecurity

Jennifer S. Freel & David Springer

Author Contact Information:
Jennifer S. Freel
Partner
Jackson Walker
Austin, Texas
jfreel@jw.com
512.236.2330

David Springer
Legal Counsel
Dropbox, Inc.
Austin, Texas
springer@dropbox.com
202.476.9480

The current practice of law relies on the use of electronic devices just as lawyers of the past relied on quills and ink.[1] But unlike the tools of the past, modern technology is susceptible to attacks that could breach the confidentiality attorneys must hold for their clients. In this paper, we look at an attorney's ethical duty to safeguard client information and how that duty intersects with cyber threats, including hacks, ransomware, and data braches. The paper will also provide practical advice for securing your devices at home and while traveling.

I. An Attorney has an ethical obligation to safeguard confidential client information.

The Texas Disciplinary Rules of Profession Conduct include strict requirements on confidentiality. The preamble says, "A lawyer should keep in confidence information relating to representation of a client except so far as disclosure is required or permitted by the Texas Disciplinary Rules of Professional Conduct or other law."[2] Rule 1.01 says that in representing a client, a lawyer shall not "fail to carry out completely the obligations that the lawyer owes" to the client.[3] Those obligations include keeping information confidential.

The Rules define confidential information as including both "privileged information" and "unprivileged client information."[4] The latter includes "all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client."[5] Absent identified exceptions,[6] a lawyer cannot "knowingly . . . reveal confidential information of a client or a former client to:

> (i) a person that the client has instructed is not to receive the information; or
>
> (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm."[7]

Under the Rules, "knowingly" "denotes actual knowledge of the fact in question."[8] Knowledge "may be inferred from circumstances."[9]

The Rules also include commentary on what it means to be competent as a lawyer.[10] Important to the discussion at hand, to maintain competence, "each lawyer should strive to become and remain proficient and competent in . . . the benefits and risks associated with relevant

---

[1] The opinions contained in this paper belong to the authors and not necessarily their current or past employers.
[2] Tex. Disciplinary Rules of Prof'l Responsibility, Preamble.
[3] *Id.* R. 1.01(b)(1).
[4] *Id.* R. 1.05(a).
[5] *Id.*
[6] The exceptions are identified in Rule 1.01(c) & (d) and include when the client expressly authorizes the disclosure, to address a controversy between the client and the attorney, when disclosure is necessary to prevent the client from committing a crime, and to prevent the client from dying by suicide.
[7] *Id.* R. 1.05(b).
[8] *Id.* Terminology.
[9] *Id.*
[10] *Id.* R. 1.01 (Comments).

technology."[11] The Texas Supreme Court added this language to the Rules in February of 2019, mirroring a change the American Bar Association ("ABA") made to the model rules in 2012.

The Professional Ethics Committee for the State Bar of Texas has issued two opinions that touch on the risks of technology and its relationship to confidentiality. In Opinion 648, the Committee was asked if a lawyer could communicate confidential information via email.[12] The Committee said a lawyer could do so but added a caveat.[13] It said, some circumstances may "cause a lawyer to have a *duty* to advise a client regarding risks incident to the sending or receiving of emails . . . and to consider whether it is prudent to use encrypted email or another form of communication."[14]

In Opinion 680, the Committee considered whether a lawyer could "use cloud-based client data storage systems or use cloud-based software systems for the creation of client-specific documents where confidential client information is stored or submitted to a cloud-based system."[15] The Committee said a lawyer could use cloud-based services.[16] It cautioned, however, that "lawyers must remain alert to the possibility of data breaches, unauthorized access, or disclosure of client confidential information and undertake reasonable precautions in using those cloud-based systems."[17]

II. Attorneys should encrypt data when third parties are likely to have access to the information.

Even though a lawyer generally may transmit information relating to the representation of a client over the internet so long as they take reasonable efforts to prevent inadvertent or unauthorized access, the ABA's Standing Committee on Ethics and Professional Responsibility has formally opined that lawyers "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."[18] Like the Texas Committee opinions referenced above, this ABA opinion contemplates encryption as one way to protect client information.

In Opinion 648, the Professional Ethics Committee identified six situations in which a lawyer should consider whether to encrypt a communication (or use some other type of security precaution):

---

[11] *Id.* R. 1.01, cmt. 8.
[12] The Professional Ethics Committee for the State Bar of Texas, Opinion 648, Apr. 2015, *available at* https://www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-648 (emphasis added).
[13] *Id.*
[14] *Id.*
[15] The Professional Ethics Committee for the State Bar of Texas, Opinion 680, Sept. 2018, *available at* https://www.legalethicstexas.com/getattachment/4bad0ccd-9157-4d3f-b14c-0a7fe2ac05f6/Opinion-680.
[16] *Id.*
[17] *Id.*
[18] American Bar Association Standing Committee on Ethics and Professional Responsibility, May 2018, *available at* https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf.

Title search: What Every Attorney Needs to Know About Cybersecurity

Also available as part of the eCourse
First Friday Ethics (October 2022)

First appeared as part of the conference materials for the
32nd Annual Conference on State and Federal Appeals session
"What Every Attorney Needs to Know About Cybersecurity"