

CYBERSECURITY AND DATA PRIVACY LAW

By Shawn E. Tuma

Lawyers' Cybersecurity and Data Breach Obligations

On October 17, 2018, the American Bar Association issued Ethics Opinion 483 titled *Lawyers' Obligations After an Electronic Data Breach or Cyberattack*¹ that made clear that lawyers' ethical obligations require them to address cybersecurity and data privacy issues.

Texas lawyers, like others engaging in business in Texas, have existing cybersecurity and data privacy duties to: (1) implement and maintain reasonable procedures to protect sensitive personal information, or SPI, they collect or maintain;² (2) follow appropriate data destruction procedures;³ and (3) notify any individual whose electronic SPI was or is reasonably believed to have been acquired by an unauthorized person.⁴ Existing federal laws, as well as laws in all 50 states, include some or all of these duties (including more stringent duties). Ethics Opinion 483 does not supplant these laws.

The opinion is both narrower and broader than existing federal and state laws. It focuses only on cyber incidents that involve information relating to the actual representation of a client. But, though its title states that it applies "after an electronic data breach," it contains proactive cybersecurity obligations required before there has been a data breach and what it considers a "data breach" is substantially broader than most traditional "data breach notification" laws.

Ethics Opinion 483 defines a "data breach" as "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."⁵ The last component makes it atypical for a "data breach notification" law because it involves situations where an event may make data unavailable, such as a ransomware attack (or even a service provider network outage) that significantly impairs the lawyer's ability to perform legal services, even when there was no access to or exfiltration of the client's data.

The opinion focuses on the overall process of protecting information, not just the outcome. From a high level it requires lawyers to do the following: (1) be competent by keeping abreast of the benefits and risks associated with relevant technology; (2) have reasonable cybersecurity safeguards in place; (3) follow appropriate data destruction procedures; (4) actively monitor for breaches of client information; (5) address third-party risk; (6) investigate, respond to, and mitigate incidents; (7) develop and implement an incident response plan; and (8) notify clients in an appropriate manner when there has been a "data breach," as defined therein.

IT Service Provider Locking Customer Out of Server—Violation of Hacking Law?

An information services provider that locked a customer

out of a server it was providing, after the customer stopped paying, did not violate the Harmful Access by Computer Act.⁶ Under the contract it had a greater right to possess the server and was considered its owner.⁷

Viewing Pictures on Boyfriend's iPhone—Violation of Hacking Law?

Girlfriend accessing her boyfriend's iPhone to view pictures did not violate the Breach of Computer Security⁸ law because she did not know that she lacked his effective consent.⁹

Notes

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018) [hereinafter Ethics Opinion 483].
2. Tex. Bus. & Comm. Code § 521.052(a).
3. Tex. Bus. & Comm. Code § 521.052(b).
4. Tex. Bus. & Comm. Code § 521.053(b).
5. Ethics Opinion 483 at 4.
6. Tex. Civ. Prac. & Rem. Code § 143.001, et seq.
7. *Puig v. High Standards Networking & Computer Services*, 2017 WL 4820171 (Tex. App.—Houston [1st Dist.] 2017).
8. Tex. Penal Code § 33.02, et seq.
9. *Thomas v. State*, 2017 WL 4400116 (Tex. App.—Houston [14th Dist.] 2017).



SHAWN E. TUMA

is an attorney widely recognized in cybersecurity and data privacy law, areas in which he has practiced for nearly two decades. He is co-chair of the Cybersecurity & Data Privacy Practice Group at Spencer Fane and works in its Dallas and Collin County offices.

BUSINESS
or **Leisure**

SHOP texasbar.com/merchandise