

TECH BYTES

15 Tech Laws and Cases to Protect Your Clients

Lisa Angelo
Angelo Law Firm
Houston, Texas

Pierre Grosdidier
Haynes and Boone
Houston, Texas

Shawn Tuma
Scheef & Stone
Frisco, Texas



Competence

ABA Model Rule 1.1

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment 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.

Requires that lawyers understand:

1. The responsibility to properly manage privacy and data security;
2. How to best leverage technology to serve clients
3. The technology the client is using.

The SCA does not apply to cell phones and home PCs
Garcia v. City of Laredo, Tex., 702 F.3d 788 (5th Cir. 2012).

- Stored Communications Act, 18 U.S.C. §§ 2701–2711.
- SCA protects the privacy of Internet communications much like the Fourth Amendment protects the privacy of the home.
- SCA criminalizes certain unauthorized computer access and authorizes a civil claim.
- SCA protects “only communications intercepted during transmission and those stored by communications providers.”
- SCA “does not apply to data stored in a personal cellphone.”
- No claim for phone or home computer spying; phone wipe.

Business Duty to Protect Sensitive Personal Information

Texas Bus. & Comm. Code § 521.052

- Business must implement and maintain reasonable procedures to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.
- Businesses must have an appropriate data destruction procedure to destroy customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business
- Does not apply to certain financial institutions.
- "Business" includes a nonprofit athletic or sports association.

CYBERBULLYING

Education Code Section 37

- Code requires school districts develop programs to address consequences, policies, and procedures, including procedure for reporting bullying.
- “**Cyberbullying**” = the use of any electronic communication device to engage in bullying or intimidation.
- “**Bullying**” = includes expression though electronic means.

The Relationship Privacy Act

- Unlawful Disclosure or Promotion of Intimate Visual Material.
- Revenge porn = the practice of posting sexually explicit pictures of other persons on the internet without consent.
- Civil Practice and Remedies Code Chapter 98B - actual damages (mental anguish, court costs, attorney fees), exemplary damages, injunctive relief, fines.
- Penal Code Chapter 21 - Class A misdemeanor.

Authenticating text messages and Internet postings

Tienda v. State, 358 S.W.3d 633, 638-39 (Tex. Crim. App. 2012).

- TRE 901(a) authentication “Proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.”
- TRE 901(b)(1) Personal knowledge
- TRE 901(b)(4) Distinctive characteristics and circumstantial evidence
- That email emanates from sender’s phone is not enough.
 - Phones can be stolen
 - Need “something more”

Notification Required Following Data Breach

Texas Bus. & Comm. Code § 521.053

- An entity doing business in Texas that owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- Notice must be given as quickly as possible after discovering or receiving notification of the breach, unless requested to delay by law enforcement, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- “Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.”

Confidentiality

ABA Model Rule 1.6

- A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
- 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.

Texas Disciplinary Rules of Professional Conduct 1.05

- A lawyer shall not knowingly reveal confidential information.

Kiddie porn reporting obligations

Penal Code § 43.27; Bus. and Com. Code § 110.002(a)

- Penal Code Chap 43 Public Indecency
 - (b) A business that develops or processes visual material and determines that the material may be evidence of a criminal offense under this subchapter shall report the . . . material to [the] law.
- Texas Business and Commerce Code § 110.002(a)
 - (a) A computer technician who, in the course and scope of employment or business, views an image on a computer that is or appears to be child pornography shall immediately report . . .
- § 43.26(a) “prohibits only possession of material that depicts an actual child, not material that merely ‘appears’ to depict a child.”
 - *Porath v. State*, 148 S.W.3d 402 ([14th Dist.] 2004, no pet.).
 - *Webb v. State*, 109 S.W.580 (Fort Worth 2003, no pet.).

Texas Unauthorized Access Laws

Breach of Computer Security (BCS), Tex. Penal Code § 33.02

- The BCS prohibits knowingly accessing a computer, computer network, or computer system without the effective consent of the owner.
- The elements are (1) an individual knowingly and intentionally accessed a computer, computer network, or computer system; (2) the individual did not have the effective consent of the owner to do so; and, (3) the owner suffered damages as a result.

Harmful Access by Computers (HACA), Civ. Prac. & Rem. Code § 143.001(a)

- A person who is injured or whose property has been injured as a result of a violation under Chapter 33, Penal Code, has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally.

Anti-Cybersquatting Consumer Protection Act

Creuzot v. Green, Civil No. 3:17-CV-0404-M (N.D. Tex. 2017) – Injunctive relief awarded when domain registrant used political opponent's name for domain. Registrant violated the Anti-Cybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 8131.

Elements:

1. Person registered a domain name;
2. Consisting of the name of another living person, or a name substantially and confusingly similar thereto;
3. Without the person's consent; and
4. With the specific intent to profit from such name by selling the domain name for financial gain to the a person or any third party.

→ Court considered registrant's offer to sell domain to the mark owner without having used the domain in offering goods or services, and registrant's past similar behavior.

EXCEPTION: Domain is registered in good faith & is protected IP (copyright, trademark)

Cell phone is a computer under Penal Code § 33.01(4)

Miller v. Talley Dunn Gallery, LLC, 2016 WL 836775 (Tex. App.—Dallas 3/3/16, no pet.).

- Miller accessed his soon-to-be ex-wife Talley Dunn's cell phone and took screen shots of text messages between Dunn and another man and examined the phone's log.
- Dunn sued under the HACA.
- Held: A cell phone qualifies as a computer.
- Court also rejected Miller's claim that he had effective consent to access the phone because it was community property.
- The phone belonged to Dunn; she used it "on a daily basis" and "it was the only way to reach her." She had the right to password-protect the phone, and Miller used her sleep to access the phone.

Merritt Hawkins & Associates v. Gresham

2017 WL 2662840 (5th Cir. June 21, 2017)

- An employee's accessing his employer's computer system without its effective consent and taking or deleting data for non-company business related purposes may violate Texas' *Harmful Access by Computer Act* (HACA) or *Breach of Computer Security* (BCS) laws.
- Recall, "[g]ood faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner." Notification Required Following Data Breach, Texas Bus. & Comm. Code § 521.053(a).

Authenticating Evidence from Facebook

Murray v. State, No. 04-16-002227-CR (Tex. App.—San Antonio 2017)

- Private messages & subscriber info from a Facebook page admitted to evidence.
- Issue: Authenticity of FB evidence
 - *Tienda* case
 - FB's Records Custodian executed a "Certificate of Authenticity of Domestic Records Regularly Conducted Activity" = self authenticating (Tex. R. Evid. 902(10)(B)).
 - Circumstantial evidence established prima facie evidence such that a jury could reasonably find that the FB content was authentic.
 - Whether a jury could reasonably find the evidence within the zone of a reasonable disagreement.

No car tracking devices without owner consent

Tex. Penal Code 16.06

- (b) A person commits an offense if the person knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person.
- (c) An offense under this section is a Class A misdemeanor.
- (d) It is an affirmative defense to prosecution under this section that the person:
 - (1) obtained the effective consent of the owner . . .
 - [others]
- Think *Miller v. Talley Dunn Gallery, LLC*

Computer Fraud and Abuse Act (CFAA) –Access

18 U.S.C. § 1030(a)

- The CFAA prohibits the knowing or intentional access of a protected computer that is without authorization or exceeds authorized access.
- Elements of broadest CFAA claim:
 - Intentionally access protected computer;
 - Without authorization or exceeding authorized access;
 - Obtained information from protected computer; and
 - Victim incurred a loss to one or more persons during any 1-year period of at least \$5,000.
- Covers things like obtaining information or something of value, committing fraud, transmitting damaging information, causing damage, trafficking in passwords, and committing extortion.
- Circuit Split.

TECH BYTES



COMPUTER AND
TECHNOLOGY
SECTION

Lisa Angelo
Angelo Law Firm
Houston, Texas

Pierre Grosdidier
Haynes and Boone
Houston, Texas

Shawn Tuma
Scheef & Stone
Frisco, Texas

The Section's mission is to education and involve the legal profession in and about the use and law of computer and information technology.

www.sbot.org

The State Bar of Texas Computer & Technology Section is a voluntary organization consisting of licensed attorneys throughout Texas who are involved with and interested in the use of computers and technology in the legal profession.

This presentation was delivered as part of the State Bar of Texas Computer & Technology Section's Education Initiative.