ELECTRONIC EVIDENCE
SOCIAL MEDIA FACTS
In 2012, 56% of Americans had a profile on a social media site.

Up from 52% in 2011 and 48% in 2010.

Significantly more Americans have a social media profile than do not.
Consumers continue to spend more time on social networks than on any other category of sites.

Social media has overtaken pornography as the No. 1 activity on the web.
One out of eight couples married in the U.S. last year met via social media.
Facebook has 1.1 billion monthly active users.

(The U.S. population is 313.9 million.)

25% of Facebook users don’t bother with privacy settings.
Facebook has 751 million mobile users each month.

Facebook users “Like” 4.5 billion items daily.

23% of Facebook users check their account five or more times every day.
On a typical day, more than 500 million Tweets are sent on Twitter, averaging 5,700 per second.

The fastest-growing group on Twitter is the 55-64 age bracket.
YouTube reaches more US adults aged 18-34 than any cable network.

After Google, YouTube is the second largest search engine.
BASICS OF SOCIAL MEDIA
Law Enforcement & Third-Party Matters

How does Facebook work with law enforcement?

How do I tell law enforcement to get in touch with Facebook?

How can I report a convicted sex offender?

Does Facebook notify users prior to responding to subpoenas?

Where can I learn more about Facebook’s Privacy Policy?

What’s the difference between the Facebook Safety Center and the Help Center Security section?

Information on Civil Subpoenas

May I obtain contents of a user’s account from Facebook using a civil subpoena?

Federal law prohibits Facebook from disclosing user content (such as messages, timeline posts, photos, etc.) in response to a civil subpoena. Specifically, the Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits Facebook from disclosing the contents of an account to any non-governmental entity pursuant to a subpoena or court order.

Parties to civil litigation may satisfy discovery requirements relating to their Facebook accounts by producing and authenticating contents of their accounts and by using Facebook’s "Download Your Information" tool, which is accessible through the "Account Settings" drop down menu.

If a user cannot access content because he or she disables or deleted his or her account, Facebook will, to the extent possible, restore access to allow the user to collect and produce the account’s content. Facebook preserves user content only in response to a valid law enforcement request.
May I obtain any information about a user’s account using a civil subpoena?

Facebook may provide basic subscriber information (not content) to a party in a civil matter only where: 1) the requested information is indispensable to the case and not within the party’s possession; and 2) you personally serve a valid California or federal subpoena on Facebook. Out-of-state civil subpoenas must be domesticated in California and personally served on Facebook’s registered agent.

Parties seeking basic subscriber information as set forth above must specifically identify the account by providing the email address, Facebook user ID (UID) and vanity URL (if any). Names, birthdays, locations, and other information are insufficient to identify a Facebook account. UIDs and/or vanity URLs may be found in the uniform resource locator available in a browser displaying the account in question. For example, in the URL http://www.facebook.com/profile.php?id=12345678910, 12345678910 is the UID.

When will I receive a response to my civil subpoena?

Facebook requires a minimum of 30 days to process a civil subpoena for basic identifying information. Additional time may be required depending on various factors. Delivery may be delayed if you fail to include Facebook’s processing fee in your request.

Do I need a Facebook representative to testify at a civil trial?

No. The account owner, or any person with knowledge of the contents of the account, can authenticate account content. Further, under federal and California law, business records produced by Facebook are self-authenticating.
ADMISSIBILITY
What kinds of evidence?

- Facebook
- Social Media
- Texts
- Voicemail
- Digital Photos
- Videos
- Recorded Calls
- Websites
- Emails
- Chats / IMs
Why?
Added 09 July 2007

Narlayp  haw, y u teachin her bad habbits amit lol
10 July 2007 at 20:57

Kiran  shud i laff or not?
17 September 2007 at 16:31
Sammatha 08.22.12
Share via PicsArt Photo Studio

Melissa: I'm going to try to lose the cig
Monday at 8:49pm · 7

Sarah: Oh my gosh is that a baby bump I see...
Monday at 8:51pm

Sammatha: I've cut down ALOT. I'm slowly quitting. That's a promise to my baby. ❤
Monday at 8:52pm · 3
Shannel  you are my babies daddy.....
Like - Comment - Yesterday at 1:36am - 2

Logan  are you fucking kidding me? out of all places to tell me this, you say it on facebook. k sweet.
Yesterday at 1:24pm - Like - 1

Shannel  sorry I couldn't get ahold of you :(
Yesterday at 1:54pm - Like

Logan  I could have messaged me instead of making it so public when we don't even know if it's mine yet.
Yesterday at 2:02pm - Like

Shannel  it's definitely yours. you asshole man up and take some responsibility.
Yesterday at 2:26pm - Like
Daniel added 5 new photos to the album *haters*.

Stevie: Where's my child support?
August 2, 2011 at 4:10pm · Like

Michael: Wow lol.
August 7, 2011 at 12:40am · Like
In this photo: Ellie [redacted] (photos)

FUCKKKK DADDYYYY
In this photo: Meggy *(photos)*

Added February 24

Kenny: Yes. We really did have Meggy's birthday party at Hooters. The wings are still the best and it's a fun environment.

February 24 at 6:55am · Report
Lulu: Hmmn what to eat?

Like · Comment · Unfollow Post · Share · Edit · Wednesday via mobile

Laurel: Probably nothing... There aint shit in there! Maybe if I received child support, I could afford to put food in my fridge!!!

14 minutes ago · Like

Aricro: I ain't payin shit bitch succ my dicc!!!

8 minutes ago · Like
BOTTOM LINE

- Use existing rules
- Electronic evidence is not inherently unreliable
- Same uncertainties exist with traditional written documents
- Threshold preliminary authentication, subject to cross examination
“In performing its...gate-keeping function, the trial court itself need not be persuaded that the proffered evidence is authentic. The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic.” Tienda
Circumstantial Evidence

- Numerous photos of defendant, showing unique tattoos
- References to victim’s death and funeral
- References to defendant’s gang
- References to defendant’s ankle monitor

- Support a finding that the MySpace pages belonged to defendant and that he created and maintained them
Forgery?

- Possibility that defendant is a victim of “elaborate and ongoing conspiracy”
- Jury assesses likelihood and weight of this alternate scenario
- State produces a prima facie showing that it was the defendant, not a fraudster, who created the page
AUTHENTICATION
Email

- E-mail address
- Unique information contained in email - references to nicknames or other facts
- Similarity of email content to other communications
- Reply letter doctrine
- Business record / trade inscriptions
Texts

- Same factors as emails
- 3rd parties permitted to testify about content of texts on others’ phones
- Objection: “just because text messages were found on a phone in his possession did not mean he sent or received them” …OVERRULED
Hey mom, I'm just going to maddies to do some meth

Uhh... I hope that is a joke syd.

Omg!!! I meant meth!!!!

Meth!

***METH

OMG MATH!! MATH!

Oh thank god!
How did things go with the French girl?

Went really bad she wasn't interested I ended up killing her sister in the barn next to her house ha

OH MY GOD, what happened???

Kissing ha ha auto correct

Spastic !!!!
:) . What are your plans for today then?x

Nothing beyond seeing you dead xx

DEAR!!!
Websites

- 2 separate issues:
  - Authentication as true and correct printouts of a website
  - Evidence showing that what appears on the website was put there by the party

- Foundation:
  1. What was actually on the website?
  2. Does the exhibit accurately reflect it?
  3. Is it attributable to the party?
Social Media

- *Tienda* factors – circumstantial evidence, distinctive characteristics
- Personal facts
- Other friends
- History of sending/receiving messages
Emily Miskel

**Work and Education**

**Employers**

- **Koons Fuller, P.C.**
  - Attorney | Sep 2009 to present | Plano, Texas
  - Emily Miskel is a divorce and family law attorney at Koons Fuller, the largest firm in the southwest practicing exclusively family law.
  - Emily handles complex divorce matters including property valuation and division, child issues, and pre- and post-marital agreements.
  - In addition to litigation experience, Emily is trained in alternative dispute resolution, including mediation, arbitration, and collaborative law.

**Graduate School**

- **Harvard University**
  - Class of 2003 | Cambridge, Massachusetts

**College**

- **Stanford University**
  - Class of 2002 | Mechanical Engineering | Stanford, California

**High School**

- **Texas Academy Of Math And Science**
  - Class of 1999 | Denton, Texas

**Arts and Entertainment**

- Share Your Interests
Chat / Instant Message

- No ISP / forensic testimony required

- Circumstantial evidence:
  - Party used the screen name
  - When a meeting was arranged with screen name, party showed up
  - Identifying characteristics in chat content
  - Party possessed information given to screen name
  - Computer evidence from party’s computer showed use of screen name
Digital Photographs

- Same as normal photograph – fairly and accurately represents scene depicted
- Digitally enhanced or edited photos – digital enhancement process produces reliable and accurate results (expert)
Voicemail and Audio Recordings

- Opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.
- Witness does not have to identify every voice in the recording.
- Witness should recognize voice and connect the recording with circumstances.
Stored vs. Processed Data

- Records merely stored in a computer raise no computer-specific authentication issues

- Computer *processed* data may require more technical authentication
Unreflective Statements

- Present sense impression
- Excited Utterance
- Then-existing condition
Reliable Documents

- Recorded recollection
- Records of regularly-conducted activity
- Market reports, commercial publications
Non-Hearsay

- Computer-generated “statements”
- Metadata
- Admissions by party-opponent
ILLEGAL EVIDENCE
Illegal Evidence

Wiretapping
- Texas – Tex. Penal Code 16.02
  Tex. CPRC Ch. 123

Electronic Data
- Federal – 18 U.S.C. 2701-2712
- Texas – Tex. Penal Code 16.04, 33.02
Federal Wiretap Act

Offense:

“intentionally intercepts…any wire, oral, or electronic communication”

“wire communication” = “aural transfer”
“oral communication” = “oral communication”
“electronic communication” = “signs, signals, writing, images, sounds, data”
Federal Wiretap Act

Offense:

- “intentionally discloses, or endeavors to disclose, … knowing or having reason to know that the information was obtained through interception”

- “intentionally uses, or endeavors to use, … knowing or having reason to know”
Federal Wiretap Act

Criminal Penalty:
- Fined and/or imprisoned up to 5 years

Civil Cause of Action:
- Actual damages, or statutory damages of $100/day or $10,000 -- whichever is greater
- Punitive damages, equitable relief
- Attorney’s fees
Federal Wiretap Act

Civil Cause of Action:

Case between husband and wife in which 18 U.S.C. 2510 provided the civil cause of action. Held that there is no spousal exemption in state and federal wiretapping laws.

Ex-wife placed spyware on ex-husband’s computer that forwarded all of his emails to her own private account. Court held that this was a violation of the Federal Wiretap Act and that ex-husband was entitled to $10,000 in liquidated damages.
Federal Wiretap Act

Exclusionary Rule:

“Whenever any wire or oral communication has been intercepted, no part of the contents…and no evidence derived therefrom may be received in evidence”
Texas Wiretap Law
Tex. Penal Code 16.02

Offense:
“intentionally intercepts…a wire, oral, or electronic communication”

“wire communication” = “aural transfer”
“oral communication” = “oral communication”
“electronic communication” = “signs, signals, writing, images, sounds, data”
Texas Wiretap Law

Offense:

- Intentional disclosure, knowing or having reason to know the information was obtained through interception.
- Intentional use, if the person knows or is reckless about whether the information was obtained through interception.
Texas Wiretap Law

Criminal Penalty:

- 2\textsuperscript{nd} degree felony
Texas Wiretap Law
Tex. Penal Code 16.02


Ex-wife taped conversations between her ex-husband and his adult son in which they planned to take her car keys and prevent her from using her car. She then took the recordings to the police station. No action was taken against ex-husband and son, but she was sentenced to 6 years in jail for recording a telephone conversation without consent of any of the parties to the conservation.

On appeal, she unsuccessfully made defenses of necessity and self-defense.
Texas Wiretap Law
Tex. Penal Code 16.02

Vicarious Consent – exception for recording a child


Parent believed her minor child was being abused, so she recorded a telephone conversation between her minor child and the defendant/alleged abuser. Court found that the vicarious consent was proper, and it complied with case law that required that the vicariously-consenting parent have an objective, reasonable belief that consenting to the recording of the conversation on behalf of the child is in the best interest of the child.
TX Wiretap Civil Cause of Action
TX CPRC Chapter 123

Cause of Action:

- Intercepts or attempts to intercept a communication
- Uses or divulges information – knows or reasonably should know was obtained by interception
TX Wiretap Civil Cause of Action

“Communication”: 

- Speech uttered by a person
- Information (including speech) that is transmitted with the aid of a wire or cable
TX Wiretap Civil Cause of Action

- Injunction,
- Statutory damages of $10,000 per occurrence,
- Actual damages in excess of $10,000,
- Punitive damages, AND
- Attorney’s fees

Ex-husband recorded conversations between him and his ex-wife, as well as between her and their minor son. Ex-wife sued under Ch. 123. Court ruled that ex-husband was permitted to record conversations with ex-wife because TX law only requires one-party consent. Court also held that ex-husband was allowed to record conversations between his son and ex-wife because parents may consent to such recordings on behalf of a minor child.
Federal Stored Comm. Act

Offense:
- Intentionally accesses
- Without authorization, or exceeds authorization
- And obtains access to a wire or electronic communication
- While it is in **electronic storage**
“Electronic storage”:

Temporary, intermediate storage of a wire or electronic communication incidental to its electronic transmission
Federal Stored Comm. Act

**Criminal Penalty:**
- 1st offense – fined, imprisoned up to 5 years
- Subsequent – fine, imprisoned up to 10 years

**Civil Cause of Action:**
- Actual damages not less than $1,000
- Punitive damages, equitable relief
- Attorney’s fees
Federal Stored Comm. Act

Civil Cause of Action:


Ex-husband placed key-logging software on ex-wife’s computer during divorce. The software allowed him to discover various passwords which he then used to access her email account. He used information he found in her email account against her, and admitted all this to the court. Summary judgment as to his liability for violating the Stored Communications Act was awarded by the court, with damages to be determined at trial.
Federal Stored Comm. Act


H used key-logging software to acquire W’s email password, accessed her email, and discovered sexual communications with various individuals. H shared emails with his attorney (co-Defendant) who sent them to W’s attorney for W to admit or deny their authenticity. W then sued H and his attorney for violating the Wiretap Act and the Stored Communications Act.

Holding: H’s MSJ granted as to Wiretap Act because the emails were not viewed by H contemporaneously with their transmission (he read them after she had already opened them). H’s MSJ denied as to Stored Communications Act claim; Court disagreed with his interpretation of whether accessed emails were in “electronic storage.”
Criminal Penalty:

- State jail felony
Texas Computer Security Law
Tex. Penal Code 33.02

**Offense:**

knowingly accesses a computer, network, or system without the effective consent of the owner
Texas Computer Security Law

Criminal Penalty:
- Amt. involved < $20,000 – state jail felony
- < $100,000 – 3rd degree felony
- < $200,000 – 2nd degree felony
- > $200,000 – 1st degree felony
- If not to “harm another” - misdemeanor

On her last day of work at the Dallas Fire Department, Defendant (a disgruntled employee) corrupted department documents on her work computer as retaliation. As a result of her actions, the department was forced to have the documents recreated at a cost of $1,400. The court found that because she was not authorized to access these documents for the purpose of corrupting them, her conduct was in violation of Tex. Penal Code 33.02.
Hypotheticals

We need guidance!