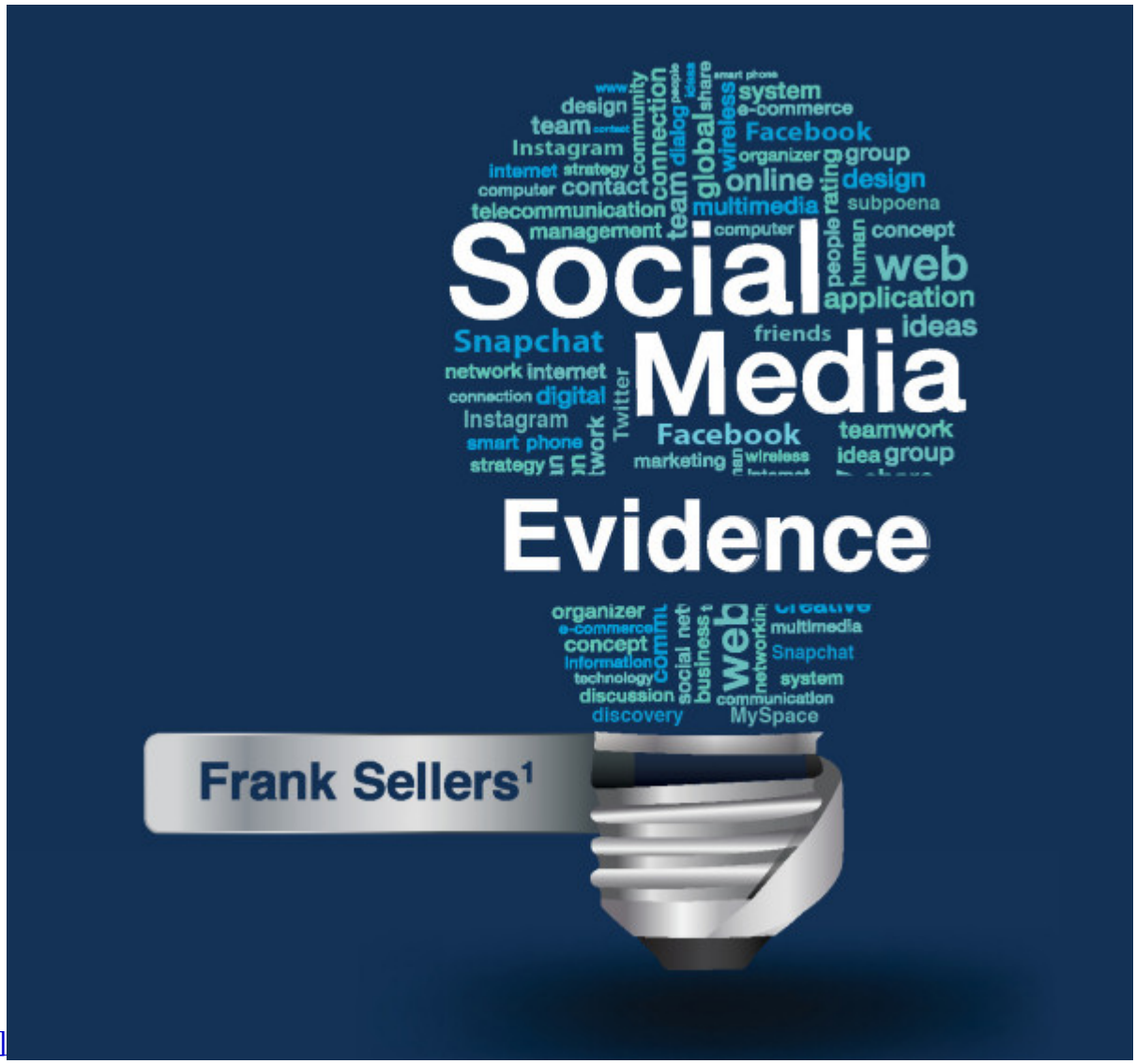
Published on *Voice For The Defense Online* (http://voiceforthedefenseonline.com)

Social Media Evidence

[1]Features
[2]Frank Sellers
Friday, September 1st, 2017

[3] 

I. Introduction

On October 17, 2009, at 11:49 a.m., Rodney Bradford posted ?ON THE PHONE WITH THIS FAT CHICK . . . WHERER MY IHOP? on Facebook.2 At the same time, a few miles away, an armed robbery was

happening. Bradford?s post, intended for his pregnant girlfriend, ended up saving him when it proved his whereabouts at the time of the robbery.3

Social media evidence is coming to a courtroom near you. A study done by the Pew Research Center (PRC) revealed that 85% of adults are internet users and 67% are smartphone users.4 Of those, 72% of online adults use Facebook, representing 62% of all American adults.5 And just when you thought social media could not possibly get any more popular, PRC reports, ?the proportion of Instagram, Pinterest, and LinkedIn users who use each respective site daily has increased significantly since September 2014.?6 Consequently, we as criminal lawyers must know how to capture, admit, and challenge social media evidence in our cases.

II. How to Obtain Social Media Evidence

A. The Stored Communications Act

The biggest obstacle for litigants trying to obtain social media evidence is the Stored Communications Act (SCA) of 1986.7 The SCA prohibits:

1. ?electronic communication service[s]??like Facebook, MySpace, Twitter, and Snapchat8? from
2. knowingly divulging
3. ?*the contents of a communication?*
4. ?to any person or entity.?9

As an issue of first impression, a California federal district court held private messages, comments, and wall postings were protected by the SCA.10 Consistent with this holding, Facebook says the ?contents of a communication? includes ?messages, timeline posts, comments, photos, and videos.?11 So Facebook refuses to provide them except when required.

Due to its age, courts have complained about the inapplicability of the SCA.12 Because it was written prior to the arrival of the internet and the World Wide Web, courts have struggled to analyze problems involving modern technology like Facebook, Instagram, and Snapchat.

This may soon change. In February 2017, the House of Representatives passed the Email Privacy Act.13 It would amend 18 U.S.C. 2702, 2703, 2705 to eliminate unnecessary distinctions between companies that transmit electronic communications versus companies that only store it. More importantly, however, it would require a finding of probable cause before a warrant or court order could issue for a subscriber?s content.14 Until the Senate and president approve the amendments, we are stuck with the SCA in its current form. As explained below, this current form allows law enforcement to obtain content without a warrant or probable cause.15

1. SCA Exceptions for Non-Governmental Entities

In a typical criminal case, only when a subscriber consents will a non-governmental litigant be entitled to the subscriber?s communication content. Courts have gone as far as compelling parties to give consent in order to provide litigants access to their private Facebook content.16

But Facebook no longer provides user content, even with user consent. In 2009, Facebook published a guide explaining that it would provide user content with ?the voluntary consent of the user,? consistent with the provisions of §?2702.17 But now, even with subscriber consent, Facebook may still refuse to comply. The current version of Facebook?s *Information for Law Enforcement Authorities* explains its operational guidelines for law enforcement officials seeking records.18 Facebook will disclose account records solely in accordance with their terms of service and applicable law, including the SCA and 18 U.S.C. 2701?2712. However, the ?User Consent? section states: ?[T]he user should be directed to obtain that information on

their own from their account. For account content, such as messages, photos, videos, and timeline posts, users can access Facebook?s ?Download Your Information? feature from their account settings.?19

In short, the best way to obtain content of communications is to bypass the provider altogether and go directly to the subscriber.

2. SCA Exceptions for Law Enforcement

The SCA provides two avenues for law enforcement to obtain easier access to the content of communications?required disclosure pursuant to a valid warrant or a court order.

The SCA requires a social media provider to disclose the contents of a communication (A) without notice to the subscriber if the request is pursuant to a valid state or federal search warrant, or (B) with notice if the request is pursuant to a valid administrative, grand jury, or trial subpoena.20 But often law enforcement seeks delayed notice under 18 U.S.C. §?2705.

Alternatively, a state or federal court may order release of the content of communications when ?the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.?21 This is something more than reasonable suspicion but less than probable cause.22

To accommodate, each of the major social media providers has compiled a law enforcement guide on how to obtain the content of communications:

- **? Facebook:** [4]www.facebook.com/safety/groups/law/guidelines/
- **? Twitter:** support.twitter.com/articles/41949
- **? Instagram:** help.instagram.com/494561080557017/
- **? Snapchat:** storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf

B. Other Ways to Obtain Content

Subpoena the Social Media Provider

As explained above, the SCA hamstrings the ability of a non-governmental entity to obtain social media communication content. If you attempt to subpoena a social media provider, you will receive a letter from the provider detailing objections to your subpoena.23

Nevertheless, you may attempt to subpoena a social media provider using the steps below.24 Because the main social media providers are all located in California, you must comply with both Texas and California subpoena laws to ?domesticate? your subpoena in California completing this checklist Michael Mowla put together:

1. Create a valid Texas subpoena duces tecum for the requested information
2. Complete Form SUBP-030, *Application for a Discovery Subpoena for an Action*25
3. Attach your Texas subpoena duces tecum to Form SUBP-030
4. Complete Form SUBP-035, *Subpoena for Production of Business Records in Action Pending Outside California*26
5. Prepare and enclose payment for the fee. Under Cal. Gov. Code §?70626(b)(5), the fee for Form SUBP-030 is $30
6. File the documents in the appropriate California superior court:

    - **? Facebook:** San Mateo County
    - **? Instagram:**

San Mateo County
? Twitter: San Francisco County
? Snapchat: Los Angeles County

7. Once you receive the documents from the Santa Clara Superior Court, send to the appropriate social media provider:27

Facebook: 1601 Willow Road, Menlo Park, CA 94025, or by email to: [5]legal@facebook.com
Instagram: Mail: Attn: Law Enforcement Response Team, 1601 Willow Road, Menlo Park, CA 94025, or by email to: [6]lawenforcement@instagram.com
Twitter: Twitter, Inc., c/o Trust & Safety?Legal Policy, 1355 Market Street, Suite 900, San Francisco, CA 94103, or by fax: 1-415-222-9958 (attn: Trust & Safety?Legal Policy)
Snapchat: Custodian of Records Snapchat, Inc. 63 Market Street Venice, CA 90291, or by email to lawenforcement@snapchat.com.

If you are seeking content (messages, comments, likes, postings, and tweets), the social media provider will most likely object in writing and disregard your subpoena. If your subpoena seeks ?non-content information? about the account holder, the social media provider will most likely comply, assuming you properly domesticated your subpoena. But no one really cares that much about the non-content information. The best way?and the method preferred by providers?to obtain content is to subpoena the subscriber directly.

1. Issue a Subpoena Duces Tecum to the Subscriber

Most providers prefer non-governmental litigants seeking communication content to subpoena the subscriber directly. Even when law enforcement has obtained consent from a user, social media providers prefer law enforcement use that consent to direct the user to download and provide the content sought rather than requesting it from the provider itself:

Facebook: ?If a law enforcement official is seeking information about a Facebook user who has provided consent . . . , the user should be directed to obtain that information on their own from their account.?28
Instagram: ?If law enforcement seeks information about an Instagram user who has provided consent for the official to access or obtain the user?s account information, the user should be directed to obtain that information on their own from their account.?29
Twitter: ?Registered Twitter users can obtain a download of Tweets posted to his or her Twitter account.?30

Each provider?s law enforcement guide provides steps on how to direct a user to download their own content. 31 Because this download contains your profile information, you should keep it secure and be careful when storing, sending, or uploading it to any other services.

But if you are looking for likes, comments, and searches, that information may only be available by compelling the person to download their ?Activity Log.? This is apparently only accessible by the actual user while signed into the account.32

2. Take Screenshots

By far the easiest way to capture social media evidence is to take a screenshot. Known by different names, ?[a] screenshot, screen capture, screen cap, cap, screen dump, or screengrab is an image taken by a person to record the visible items displayed on the monitor, television, or other visual output device in use.?33 By taking a screenshot, you can see exactly what was posted, by whom, and typically when it was posted. You can then print the screenshot, take it to court, and mark it with an exhibit sticker. All that?s left is to

overcome hearsay issues and authenticate the evidence, which is explained in Part VIII.B.

C. Identifying Information Required and What to Request From Social Media Provider

Each social media provider varies in the type of information available. Facebook, for example, collects all kinds of data. By contrast, Snapchat really does not save the data (?snaps?) transmitted over its airwaves. The most Snapchat can provide is a log of previous snaps that have been sent and received by a user. Conveniently, each provider delineates between what content is protected by the SCA and what data may be obtained by a proper subpoena. Below are examples of what to request from each provider and what information the provider will need from you to find the specific subscriber?s account content.34

1. Facebook

Information Required: The email address, user ID number (e.g., [7] www.facebook.com/profile.php?id=1000000XXXXXXXX) or username (e.g., [8] www.facebook.com/username) of the Facebook profile.35

What to Request: Basic Account Information?may be obtained through a valid subpoena or court order:

- **?** Name,
- **?** Length of service,
- **?** Credit card information,
- **?** Email address(es), and
- **?** Login/logout IP address(es).36

Non-content Account Information?may be obtained through ?court order issued under 18 U.S.C. Section 2703(d)[:]?

- **?** Message Headers and
- **?** All login/logout IP address(es).37

Stored Account Content (Communications)?may only be ob-tained through a ?search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equiva-lent state warrant procedures upon a showing of proba-ble cause[:]?

- **?** Messages,
- **?** Photos,
- **?** Videos,
- **?** Timeline posts,
- **?** Likes,
- **?** Comments, and
- **?** Location information.38

2. Twitter

Information Required: The @username and URL of the subject Twitter account in question (e.g., @safety and [9]https://twitter.com/safety).39

What to Request: Basic Account Information??A Twitter account profile contains a profile photo, header photo, background image, and status updates, called Tweets. In addition, the account holder has the option to fill out a location (e.g., San Francisco), a URL (e.g., twitter.com), and a short ?bio? section about the account for display on their public profile.?40

Non-content Private Account Information??Non-public information about Twitter users will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process ? or in response to a valid emergency request[:]?

- **?** Payment Information,
- **?** Log Data,
- **?** Location Information, and
- **?** Commerce Services.41

Stored Account Content? ?Requests for the contents of communications . . . require a valid search warrant or equivalent from an agency with proper jurisdiction over Twitter[:]?

- **?** Tweets,
- **?** Direct Messages, and
- **?** Photos.42

3. Instagram

Information Required: ?The username of the Instagram account in question on the date you viewed the account and details regarding specific information requested and its relationship to your investigation. Usernames are not static and we are unable to process requests that do not include the date viewed combined with the username. If you have access to an image?s short URL, you can go to the link and find the username at the top right next to the image. If you have access to the Instagram app, you can locate the username at the top of the account?s profile.?43

What to Request: Basic Subscriber Information?may be obtained through ?a valid subpoena issued in connection with an official criminal investigation[:]?

- **?** ?subscriber name,
- **?** account creation date,
- **?** email address, and
- **?** a signup IP address, if available.?44

Non-content Account Information?may be obtained through a valid state or federal warrant, or a proper court order:

- **?** photographs,
- **?** photo captions, and
- **?** other electronic communication information.45

Stored Content of Account? may only be obtained through a valid state or federal warrant issued upon probable cause:

- **?** Messages,
- **?** Photos,
- **?** Comments, and
- **?** Location information.46

4. Snapchat

Information Required: ?Before sending a legal request to Snapchat, you must first identify the username of the account. If you are unable to locate a username, Snapchat can try?with varying degrees of success?to locate the account with a phone number or email address.?47

What to Request: Basic Subscriber Information?may be obtained through subpoena (including administrative or grand jury), civil investigative demand, court order, or federal or state search warrant:

- **?** Snapchat username,
- **?** Email address,
- **?** Phone number,
- **?** Snapchat account creation date, and
- **?** Timestamp and IP address of account logins and logouts.48

Log of Previous Snaps?may be obtained by court order or federal or state search warrant. Snapchat only retains logs of previous messages sent and received (does not include content, i.e., the actual picture or message sent).49

Message Content?only provided pursuant to federal or state search warrant. Most likely, Snapchat will not be able to provide actual ?snaps? because ?Snapchat deletes each Snap . . . once all recipients have viewed it. And even when a Snap remains unopened, it will be deleted 30 days after it was first sent.?50

D. Requests Must Be Narrowly Tailored

Discovery requests for content from a social media site must still comply with applicable discovery rules.51 In *Mailhoit v. Home Depot,* the defendant moved the court to compel the plaintiffs to produce a laundry list of social media evidence, including profiles, postings, messages, status updates, wall comments, causes joined, groups joined, and pictures posted or tagged with the defendant. The *Mailhoit* court concluded that nearly all of the requests failed the ?reasonable particularity? requirement and therefore were not ?reasonably calculated to lead to the discovery of admissible evidence,? as required by Fed. R. Civ. P. 34.52

No Texas criminal cases have touched on discovery of social media evidence. As explained above, this fight will most likely occur when a social media user is subpoenaed by a party to bring his or her entire social media identity in response to a sub-poena. Under Tex. Code Crim. P. art. 24.02, a witness can be required by a subpoena duces tecum to bring certain items to a scheduled trial or hearing. If either party files a motion to quash, the non-moving party must show that the testimony and documents or items subpoenaed are material, meaning ?the testimony[, documents, and items] would be admissible and logically relevant to some matter at issue in the proceeding.?53

E. Do Not Advise Clients or Witnesses to Delete Data

[10]

Whatever you do, do *not* advise a potential witness to ?clean up? their social media accounts before turning over properly requested discovery. In *Allied Concrete Co. v. Lester*, a Virginia personal injury case following a truck wreck that injured a husband and killed his wife, the husband?s lawyer, through his paralegal, advised his client to delete 16 pictures from his Facebook page before responding to discovery requests from the defense.[54] One of the deleted photos depicted the grieving husband ?holding a beer can while wearing a T-shirt emblazoned with ?I ª hot moms.?[55] The paralegal emailed the husband multiple times, saying things like, ?We do NOT want blow-ups of other pics at trial so please, please clean up your facebook and myspace!? After a sizeable verdict?and the trial court ordered, at the defendant?s request, sanctions of $542,000 against the lawyer and $180,000 against the husband for attorney?s fees in discovering and proving the misconduct?the trial court further ordered remittitur of $4,127,000 of the husband?s $6,227,000 wrongful-death award.56

Although the remittitur was reversed on appeal, this case serves as a cautionary tale for all lawyers advising clients about requested social media evidence.57

For his part, Lester?s lawyer, Matthew B. Murray, resigned from the Allen, Allen, Allen & Allen law firm, and the Virginia Bar suspended his law license for five years.58

III. How to Admit Social Media Evidence

A. Must Be Relevant & Authentic

The initial question of whether the proponent of the evidence ?has supplied facts that are sufficient to support a reasonable jury determination that the evidence he proffered is authentic,? is answered by the trial court.59 But the trial court itself ?need not be persuaded that the proffered evidence is authentic.?60 Rather, after the trial court makes an initial determination that the proponent ?has supplied facts that are sufficient to support a reasonable jury determination that the [proffered evidence] is authentic,? the jury (in a jury trial)

answers the ?ultimate question [of] whether an item of evidence is what its proponent claims? it to be.61

B. Ways to Authenticate Social Media Evidence

Texas? leading case on authentication of social media evidence is *Tienda v. State*.62 The Court recognized ?there is no single approach to authentication that will work in all instances.?63 So what will work?

Social media evidence is most commonly authenticated in three different ways:

1. By direct testimony from a witness with personal knowledge of the account and account holder;
2. By comparison with other authenticated evidence; or
3. By circumstantial evidence.64

Importantly, however, ?the fact that an electronic communication on its face purports to originate from a certain person?s social networking account is generally insufficient, standing alone, to authenticate that person as the author of the communication.?65 The concern is two-fold: (1) Anyone can create a fake profile, and anyone viewing that profile would have ?no way of knowing whether the profile is legitimate[;]? and (2) A person?s account can be accessed by anyone who obtains the user?s name and password.66

Because of the various types of social media evidence, the ?best or most appropriate method of authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case.?67

C. Must Have More Than Just the Post

In *Dering v. State*, the trial court refused to admit Facebook posts offered by Dering on the grounds that the posts were not authenticated.68 Dering was charged with sexual assault of an el-derly person in Jones County, Texas.69 He moved to transfer venue due to negative publicity, including numerous inflammatory remarks from community members about Dering and his case on Facebook. The posts in questions were neither made by Dering nor posted to his account and were sponsored by Dering?s friend, who was neither the author nor recipient of the posts.70 The original post was created by a third party and commented on by other third parties, none of whom testified during any of the proceedings.71 The witness who sponsored the posts did recognize the original author and some of the subsequent commenters.72 The only evidence offered to authenticate the posts was the names and photos of the posters as shown on their accounts.73

The court held that the circumstantial evidence was insufficient to authenticate the Facebook posts, noting that this case is distinguished from the previous line of cases in that the party offering the evidence was neither the author nor recipient of the post.74 ?The fact that an electronic communication on its face purports to originate from a certain person?s social networking account is generally insufficient, standing alone, to authenticate that person as the author of the communication.?75

There are at least two ways to fix the *Dering* problem. First, the original posts are usually by some news/media outlet. You could subpoena the news reporter who posted the information on the news site?s social media account. Today, news stations keep track of what is trending and can likely comment on whether or not this was a ?hot? story in the particular jurisdiction. Second, you could subpoena each of the named users. If you?re not sure who they are or only have a username, you could subpoena their non-content information?i.e., name, email address, credit card information, and login IP address(es) with a properly domesticated Texas subpoena to the provider.76 Using the information you receive, you or an investigator can likely track down good contact information for the subscriber. Then, subpoena them to testify and ask them enough questions to establish whether they are responsible for the particular post. This should satisfy *Tienda* and overcome *Dering.*

IV. Challenges to the SCA & Social Media Evidence

If the SCA seems one-sided in favor of the government, it is. It only allows *governmental entities* to obtain user content by warrant or probable-cause court order.77 The Federal Rules of Criminal Procedure specifically allow only the government to seek a warrant.78 The Texas rules are silent, but it is unlikely a judge would issue a warrant requested by the defense. This leaves defendants needing subscriber content to prove a defensive theory in a tough place. There are a few challenges that can, and need to be, made to the SCA in its current form.

First, object that the SCA violates your client?s procedural and substantive due process rights. By allowing the government unilateral access to content evidence, this seems to violate the Fifth and Fourteenth amendments?especially if the content of the communications contain evidence of your client?s innocence.79

Second, object that your client is being denied the effective assistance of counsel. The Sixth Amendment imposes a duty on counsel to investigate and, when necessary, present defensive evidence.80 The federal statutory restriction on the defense?s access to the evidence prohibits defense counsel from fulfilling this constitutional duty.

Third, object that the SCA violates your client?s right to confrontation and compulsory process.81

Finally, object that the SCA violates the separation of powers provisions of the Federal Constitution.82 Courts have the inherent power to issue orders necessary to affect their jurisdiction.83 The legislature is not permitted to interfere with a court?s exercise of its jurisdiction.84

Fortunately but infrequently, courts started recognizing the sweeping nature of the scope of warrants and court orders for user data.85 Commonly, if the state or federal government obtained evidence from your client?s social media, they did it pursuant to an ?any and all? warrant or court order.86 Undoubtedly this data contains all types of private communication, most of which will not be relevant to whatever law enforcement was initially after.

Watch out for ?any and all? social media evidence warrants. You must object that the warrant or court order was overbroad and did not limit its request to the particular data it sought. For example, the government should limit message content to messages between specific users and times it has probable cause of evidence of wrongdoing.87 Social media providers already segregate data, so limiting requests is not difficult.

Interestingly, providers are starting to fight back. All providers post ?transparency? reports for their users to show how many requests they receive, for what types of data.88 They all boast about how many government requests they refuse or narrow before fulfilling.89 Big corporations are banding together to assert the privacy rights of their users, hopefully reinvigorating the Fourth Amendment in the increasingly digital world.90

V. Conclusion

As long as social media continues to saturate our everyday lives, it will continue to play a huge role in our courtrooms. When a Rodney Bradford walks into your office, you must know how to obtain and authenticate social media evidence.91 The best ways to obtain social media content are to get a search warrant, subpoena the user directly, or have someone screenshot the particular post, tweet, message, or snap you want to use as evidence. By presenting sufficient evidence for a reasonable jury to link the accountholder to the account, and the particular social media, you have satisfied *Tienda?*s authentication test. On the other hand, constitutional challenges need to be made to the SCA in its current form. If the prosecution has social media evidence in its discovery, you must scrutinize the authorizing affidavit, specifically looking for overbroad requests lacking particularity.

Endnotes

1. Special thanks to Rudy Moisiuc, a third-year law student at Texas Tech University School of Law, for his help writing and editing this article.

2. Vanessa Juarez, *Facebook Status Update Provides Alibi,* CNN (Nov. 13, 2009), [11] www.cnn.com/2009/CRIME/11/12/facebook.alibi/index.html?eref=rss_us.

3. *Id.*

4. Maev Duggan, *Mobile Messaging and Social Media,* Pew Research Center (Aug. 19, 2015), [12] www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/. An update of the study found Facebook continues to be America?s most popular social networking platform by a substantial margin: Nearly eight-in-ten online Americans (79%) now use Facebook, more than double the share that uses Twitter (24%), Pinterest (31%), Instagram (32%), or LinkedIn (29%). Shannon Greenwood, Andrew Perrin, & Maeve Duggan, *Social Media Update 2016,* Pew Research Center (Nov. 11, 2016), [13] www.pewinternet.org/2016/11/11/social-media-update-2016/.

5. *Id.*

6. *Id.*

7. 18 U.S.C. §§?2701?12

8. ?The SCA defines an ECS [Electronic Communication Service] provider as ?any service which provides to users thereof the ability to send or receive wire or electronic communications.?? *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 972 (C.D. Cal. 2010) (quoting 18 U.S.C. §?2510(15)). The *Crispin* court also drew a distinction between whether entities qualified as ECSs or Remote Computing Services (RCS), concluding that an entity providing messaging services is an ECS for messages that were unopened and unread by the recipient, but the same entity transforms to an RCS after the messages were opened, read, and retained by the recipient. *Id.* at 987. The opinion has been widely criticized as ?applying outdated law to new technology.? Rick E. Kubler & Holly A. Miller, *Recent Developments in Discovery of Social Media Content,* at 7, *available at* goo.gl/jGEZkb (last visited Feb. 24, 2017) (citing Joshua Briones and Ana Tagvoryan, Social Media as Evidence 40 (2013)).

9. 18 U.S.C. §?2702(a)(1) (emphasis added). Separately, the SCA also prohibits: 1. electronic communications services from 2. knowingly divulging, 3. ?a record or other *information pertaining to a subscriber* to or customer of such service,? 4. ?to any governmental entity.? *Id.* §?2702(a)(3) (emphasis added).

10. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

11. Letter from Facebook Security to author (Oct. 9, 2013) (on file with author) [hereinafter Facebook Objections].

12. *See,* e.g., *Konop v. Hawaiian Airlines,* 302 F.3d 868 (9th Cir. 2002).

13. Email Privacy Act, H.R. 387 115th Cong. (2017), *available at* [14]www.congress.gov/bill/115th-congress/house-bill/387/text. The bill has not yet been voted on by the Senate.

14. *Id.*

15. See Part II.A.2 *infra*.

16. *See,* e.g., *Romano v. Steelcase,* 907 N.Y.S.2d 650, 654 (N.Y. Sup. Ct. 2010); Kubler & Miller, Recent Developments in Discovery of Social Media Content, at *8.

17. *Facebook Law Enforcement Guidelines,* Facebook (2009), available at [15] www.eff.org/files/filenode/social_network/facebook2009_sn_leg-doj.pdf (last visited Apr. 17, 2017).

18. *Information for Law Enforcement Authorities,* Facebook, [4] www.facebook.com/safety/groups/law/guidelines/ (last visited Apr. 17, 2017).

19. *See* [16]www.facebook.com/help/131112897028467. Users can also view recent IP addresses in their Account Settings under Security Settings/Active Sessions. *Id.* Users do not have access to historical IP information without legal process. *Id.*

20. 18 U.S.C. §?2703(b).

21. *Id.* §?2703(d).

22. The phrase ?reasonable belief? first appeared in *Payton v. New York,* 445 U.S. 573, 576 (1980) (discussing police entry into home to make a warrantless arrest). Since *Payton,* legal scholars have debated its meaning but, at bottom, it is at least the amount of proof required for a detention under *Terry v. Ohio,* and ?may require something more than an investigative stop based on reasonable suspicion.? *Duran v. Indiana,* 930 N.E.2d 10, 16 (Ind. 2010).

23. *See* Facebook Objections, *supra* note 14.

24. Special thanks to Michael Mowla of Cedar Hill for researching and compiling this list of steps to domesticate a Texas subpoena in California.

25. [17]www.courts.ca.gov/documents/subp030.pdf.

26. [18]www.courts.ca.gov/documents/subp035.pdf.

27. Each of the providers listed includes a caveat on their guides that they will accept service for ?convenience,? but that they do not waive objections to jurisdiction or proper service.

28. *Information for Law Enforcement Authorities,* Facebook, [4] www.facebook.com/safety/groups/law/guidelines/ (last visited Apr. 17, 2017).

29. *Information for Law Enforcement,* Instagram, [19]https://help.instagram.com/494561080557017/ (last visited Apr. 17, 2017).

30. Twitter, however, ?does not currently offer users a self-serve method to obtain other, non-public information (e.g., IP logs) about their Twitter accounts. If a Twitter user requires his or her non-public account information, please direct the user to send a request to Twitter via our privacy form. We will respond with further instructions.? *Guidelines for Law Enforcement,* Twitter, [20] https://support.twitter.com/articles/41949#8 (last visited Apr. 17, 2017).

31. *EInformation for Law Enforcement Authorities,* Facebook, [4] www.facebook.com/safety/groups/law/guidelines/ (last visited Apr. 17, 2017).

32. *Accessing Your Facebook Data,* Facebook, [21] www.facebook.com/help/405183566203254?helpref=faq_content (last visited April 17, 2017). For more information about how to download data, and what is included, see *Id.*

33. *Screenshot,* Wikipedia, [22]https://en.wikipedia.org/wiki/Screenshot (last visited April 17, 2017).

34. To find out what is actually collected, however, you should take a look at the privacy policies of the specific social media service for the information you seek.

35. *Information for Law Enforcement Authorities,* Facebook, [4] www.facebook.com/safety/groups/law/guidelines/ (last visited April 17, 2017).

36. *Id.*

37. *Id.*

38. *Id.*

39. *Guidelines for Law Enforcement,* Twitter, [23]https://support.twitter.com/articles/41949 (last visited April 17, 2017).

40. *Id.*

41. *Id.*

42. *Id.* For other information to request, see *Twitter Privacy Policy,* Twitter [24] https://twitter.com/privacy?lang=en.

43. *Information for Law Enforcement,* Instagram, [25]https://help.instagram.com/494561080557017 (last visited April 17, 2017).

44. *Id.*

45. *Id.*

46. *Id.*

47. *Snapchat Law Enforcement Guide* at 5, Snapchat, [26] www.snapchat.com/static_files/lawenforcement.pdf?version=20150604 (last visited April 17, 2017).

48. *Id.*

49. *Id.* at 6.

50. *Id.*

51. *Mailhoit v. Home Depot,* 285 F.R.D. 566 (C.D. Cal. 2012).

52. *Id.*

53. George E. Dix & John M. Schmolesky, 43 Tex. Prac., Criminal Practice & Procedure §?32:26 (3d ed.) (citing various cases on materiality).

54. *Allied Concrete Co. v. Lester,* 736 S.E.2d 699, 702 (Va. 2013).

55. *Id.* at 703.

56. *Id.*

57. *Id.* at 708?09.

58. Agreed Disposition Memorandum Order, *In the Matter of Matthew B. Murray,* No. 11-070-088405 and 11-070-088422 (Va. State Bar Disciplinary Board filed July, 2013), *available at* [27] www.vsb.org/docs/Murray-092513.pdf.

59. *Tienda v. State,* 358 S.W.3d 633, 638 (Tex. Crim. App. 2012) (discussing Tex.R. Evid. 401, 402, 901).

60. *Id.*

61. *Id.*

62. *Id.* at 633. In *Tienda v. State,* three MySpace pages, their accompanying subscriber reports, and affidavits subpoenaed from MySpace were offered as evidence against a defendant who was a suspect in a drive-by shooting. *Id.* at 635. The court looked at four specific sets of facts involving the account in determining whether a rational jury could find that the MySpace page was created and posted to by the defendant: (1) that the accounts had pictures posted to them displaying the defendant?s unique tattoos, eyeglasses, and earring; (2) that at least one account referenced music played at a victim?s funeral; (3) that the accounts made references to the defendant?s associated gang; and (4) messages sent from the account referring to (a) specific shootings involved, (b) a party the defendant believed was a ??snitch??, and (c) the ankle monitor defendant had been wearing for the past year, all of which were sent from accounts of users with defendant?s name or nickname, and sent from an email address of defendant?s name. *Id.* at 645. The court held that there was ?ample circumstantial evidence . . . to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them.? *Id. See also United States v. Barnes,* 803 F.3d 209, 215 (5th Cir. 2015).

63. *Tienda,* 358 S.W.2d at 640 (citation omitted).

64. *Id.* at 638.

65. *Dering v. State,* 465 S.W.3d 668, 671 (Tex. App.?Eastland 2015, no pet.) (citing *Tienda,* 358 S.W.3d at 642).

66. *Id.*

67. *Tienda,* 358 S.W.3d at 639.

68. *Dering v. State,* 465 S.W.3d 668, 670 (Tex. App.?Eastland 2015, no pet.).

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.* at 673.

74. *Id.*

75. *Id.*

76. *See supra,* Part II.B.1.

77. 18 U.S.C. §§?2703 Required Disclosure of Customer Communications or Records.

78. Fed. R. Crim. P. 41(b).

79. *Cf. Brady v. Maryland*, 373 U.S. 83, 87 (1963).

80. *Strickland v. Washington*, 466 U.S. 668, 680 (1984).

81. *Cf. Davis v. Alaska*, 415 U.S. 308, 320, 94 S. Ct. 1105, 1112, 39 L. Ed. 2d 347 (1974) (?The State could have protected Green from exposure of his juvenile adjudication in these circumstances by refraining from using him to make out its case; the State cannot, consistent with the right of confrontation, require the petitioner to bear the full burden of vindicating the State?s interest in the secrecy of juvenile criminal records.?); *Washington v. Texas*, 388 U.S. 14, 19, 87 S. Ct. 1920, 1923, 18 L. Ed. 2d 1019 (1967) (?Just as an accused has the right to confront the prosecution?s witnesses for the purpose of challenging their testimony, he has the right to present his own witnesses to establish a defense. This right is a fundamental element of due process of law.?).

82. *Stern v. Marshall*, 131 S. Ct. 2594, 2620 (2011) (?A statute may no more lawfully chip away at the authority of the Judicial Branch than it may eliminate it entirely.?).

83. *See Heckers v. Fowler*, 69 U.S. 123, 128, 17 L.Ed. 759 (1864) (explaining that federal courts have authority to make all necessary rules for orderly conduct of their business provided such rules are not repugnant to the laws of the United States); *see also Degen v. United States*, 517 U.S. 820, 827, 116 S.Ct. 1777, 135 L.Ed.2d 102 (1996) (?A federal court has at its disposal an array of means to enforce its orders, including dismissal in appropriate case; its powers include those furnished by federal rule, and by inherent authority?); *see*, e.g., Fed. R. Civ. Proc. 37, 41(b); Tex. Gov?t Code §?21.00l(a).

84. *Id.*; *cf. Williams v. State*, 707 S.W.2d 40, 45?46 (Tex. Crim. App. 1986) (citing Tex. Const. art. V) (?[T]he Legislature may not interfere with the functions and powers of the judicial branch so as to usurp those functions and powers.?).

85. *United State v. Comprehensive Drug Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (?This pressing need of law enforcement for broad authorization to examine electronic records, so persuasively demonstrated in the introduction to the original warrant in this case [] creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.?).

86. *See generally*, Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 Vand. L. Rev. 585 (2016).

87. *See Id.* at 633, ?If there is probable cause for incriminating text messages, but not for photos, videos, or any other data on the phone, then magistrates should limit the search warrant to the text messaging application, rather than the whole phone.?

88. E.g., *United States Law Enforcement Requests for Data*, Facebook, [28] https://govtrequests.facebook.com/country/United%20States/2016-H1/.

89. E.g., *2016 Transparency Report: January to June 2016*, Dropbox, [29]www.dropbox.com/transparency.

90. *See Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016); *see also* Brief of Amici Curiae Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, Whatsapp, and Yahoo in Support of Apple, Inc. *In the Matter of the Search of an Apple iPhone*, No. CM 16-10 (SP) (C.D. Cal. 2016), *available at* [30] http://images.apple.com/pr/pdf/Amazon_Cisco_Dropbox_Evernote_Facebook_Go....

91. Juarez, *Facebook Status Update Provides Alibi*, *supra* note 5.
.

Source URL: http://voiceforthedefenseonline.com/story/social-media-evidence

Links:
[1] http://voiceforthedefenseonline.com/channel/1/stories
[2] http://voiceforthedefenseonline.com/source/frank-sellers
[3] http://voiceforthedefenseonline.com/image/social-media-evidence
[4] http://www.facebook.com/safety/groups/law/guidelines/
[5] mailto:legal@facebook.com
[6] mailto:lawenforcement@instagram.com
[7] http://www.facebook.com/profile.php?id=1000000XXXXXXXX
[8] http://www.facebook.com/username
[9] https://twitter.com/safety
[10] http://voiceforthedefenseonline.com/image/social-media-evidence-1
[11] http://www.cnn.com/2009/CRIME/11/12/facebook.alibi/index.html?eref=rss_us
[12] http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/
[13] http://www.pewinternet.org/2016/11/11/social-media-update-2016/
[14] http://www.congress.gov/bill/115th-congress/house-bill/387/text
[15] http://www.eff.org/files/filenode/social_network/facebook2009_sn_leg-doj.pdf
[16] http://www.facebook.com/help/131112897028467
[17] http://www.courts.ca.gov/documents/subp030.pdf
[18] http://www.courts.ca.gov/documents/subp035.pdf
[19] https://help.instagram.com/494561080557017/
[20] https://support.twitter.com/articles/41949#8
[21] http://www.facebook.com/help/405183566203254?helpref=faq_content
[22] https://en.wikipedia.org/wiki/Screenshot
[23] https://support.twitter.com/articles/41949
[24] https://twitter.com/privacy?lang=en
[25] https://help.instagram.com/494561080557017
[26] http://www.snapchat.com/static_files/lawenforcement.pdf?version=20150604
[27] http://www.vsb.org/docs/Murray-092513.pdf
[28] https://govtrequests.facebook.com/country/United%20States/2016-H1/
[29] http://www.dropbox.com/transparency
[30] http://images.apple.com/pr/pdf/Amazon_Cisco_Dropbox_Evernote_Facebook_Google_Microsoft_Mozilla_Nest_Pin