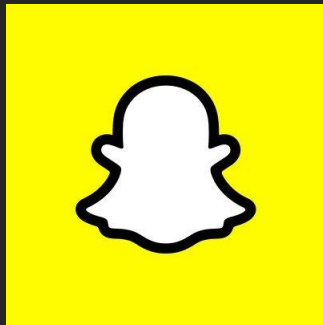


Capturing and Utilizing Social Media as Evidence



Capturing and Utilizing Social Media as Evidence



Notice of Copyright Use

This presentation contains the creative works of others which are used either by permission, license, or under 17 U.S.C. 107 (fair use). The presentation was created under the Fair Use Guidelines and further use or distribution of the presentation is not permitted.

Roadmap for Today

- How to identify that your case involves social media
- How do you obtain the materials
 - Capturing, downloading, extractions, warrants
- Methods for searching through records
- Admitting it: authenticating, foundation, avoiding hearsay objections, who do you need?
- Case law

Identifying cases involving Social Media

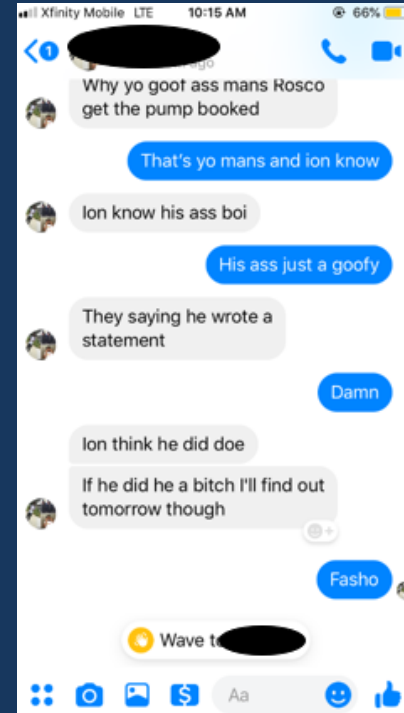
- Used to plan the crime
 - Messages between co-offenders
- Used during commission of crime:
 - Disorderly Conduct – school threats
 - Robbery – used to set up meeting
- Used after the fact:
 - Investigation by police found posts regarding
 - Intimidation of witnesses via social media
- Used to corroborate
 - Posts showing clothing or location

Wanna hit a stain?



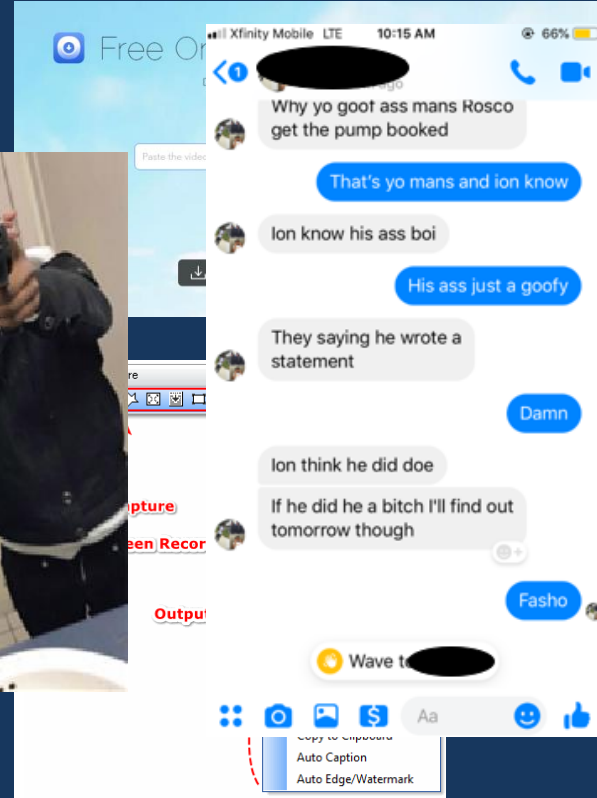
How do we get it?

- Screen Capture



How do we get it?

- Screen Capture
- Video Downloader



How do we get it?

- Screen Capture
- Video Downloads
- Phone Extraction



Copy to Clipboard
Auto Caption
Auto Edge/Watermark

How do we get it?

- Screen Capture
- Video Downloads
- Phone Extraction
- Search Warrant



Mobile Devices

Type SAMSUNG-SGH-I337

Os Android 4.4.2

Updated 2019-04-02 03:40:56 UTC

Advertiser Id ab77fd44-2e1f-447f-8bfe-083514fc080e

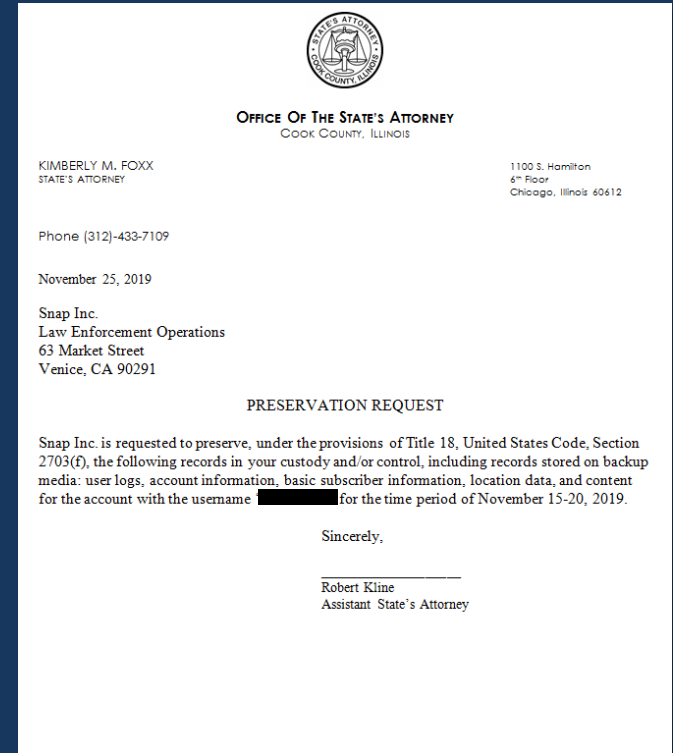
Udid 7c4142f7-cd48-4dca-992a-caf7974d2a29

Why a search warrant?

- Most providers will only supply the most basic information with a subpoena.
 - Subscriber information, billing records
- For detailed records, content, videos/pictures, you'll need a search warrant
 - Stored Communications Act, 18 U.S.C. Sections 2701-2712

Drafting your search warrant

- Preserve your evidence
 - Don't wait for a court order
- Don't reinvent the wheel
- Law enforcement should be drafting the warrant, not you



Drafting your search warrant

- You can review the search warrant and offer corrections
- Follow your office's procedures for search warrants

Now what?

- Once it's been signed, get a copy of the search warrant in PDF format
- Either you or your law enforcement agent should submit the warrant to the proper company



LAW ENFORCEMENT

Technology Investigations Resource Guide ©

GUIDELINES FOR SEIZING
DIGITAL DEVICES

HOSTAGE NEGOTIATIONS
REQUEST CONTROL OF
TARGET PHONE

AMBER ALERT
Best Practices



CURRENT EDITION:
2021
VERSION 1.0



THE GUIDE IS PROVIDED TO
AUTHORIZED LAW ENFORCEMENT
WITH HOSTING SUPPORT FROM
HAWK ANALYTICS



Law Enforcement Technology Investigations Resource Guide ©



THIS GUIDE IS MAINTAINED AND PROVIDED AS A FREE RESOURCE TO ASSIST US LAW ENFORCEMENT AGENCIES

Send updates, corrections, suggestions or comments to:

TechnologyResourceGuide@outlook.com

<https://support.hawkanalytics.com/>

Colin Fagan, CFE

Detective Sergeant - Digital Evidence Forensic Examiner (ret) / President Emeritus - Oregon Remains Investigators Association



LAW ENFORCEMENT TECHNOLOGY INVESTIGATIONS RESOURCE GUIDE ©

Cellular providers, Social Media, Finance, Content Provider LE Guides, Example Forms and more...



EXAMPLE DOCUMENTS – CONSENT TO SEARCH, PRESERVATION, RETENTION, SUBPOENAS, AFFIDAVITS & SEARCH WARRANTS

EXAMPLE DOCUMENT RESOURCES ARE CONTINUALLY REVISED & UPDATED

Although many of these example documents are Oregon examples, they have been crafted in a downloadable Word document format allowing users to copy and paste the most current and best example technical language into their own jurisdictional format.

Unfortunately, there are no *“one size fits all”* affidavits and search warrants for digital evidence and provider content. It is up to each user to adapt what is offered here to use for their own unique case needs and circumstances.

EXAMPLE FORMS: CONSENT
TO SEARCH DIGITAL DEVICES

EXAMPLE
PRESERVATION REQUESTS

EXAMPLE FORMS: CONSENT TO
ASSUME ON-LINE ACCOUNT
CONTROL

EXAMPLE
SUBPOENAS

OTHER FORMS
& INFO

EXAMPLE AFFIDAVITS
& SEARCH WARRANTS

RECORDS RETENTION
SCHEDULES

OTHER EXAMPLES
STATE | FEDERAL

<https://support.hawkanalytics.com/>

Law Enforcement Technology Investigations Resource Guide

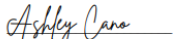
- Can be obtained by going to:
<https://support.hawkanalytics.com/>
 - Click “Request Access” and submit your name, agency, work email

Now what?

Certificate of Authenticity of Domestic Records of Regularly Conducted Activity

I, Ashley Cano, certify:

1. I am employed by Facebook, Inc. ("Facebook"), headquartered in Menlo Park, California. I am a duly authorized custodian of records for Facebook and am qualified to certify Facebook's domestic records of regularly conducted activity.
2. I have reviewed the records produced by Facebook in this matter in response to the Search Warrant received on March 20, 2019. The records include search results for Basic Subscriber Information, IP Address Logs, Messages, Photos, Transactional Information, Videos, Other Content and records for the account with identifier 100027863745883.
3. The records provided are an exact copy of the records that were made and kept by the automated systems of Facebook in the course of regularly conducted activity as a regular practice of Facebook. The records were saved in electronic format after searching Facebook's automated systems in accordance with the above-specified legal process. The records were made at or near the time the information was transmitted by the Facebook user.
4. I declare under penalty of perjury that the foregoing certification is true and correct to the best of my knowledge.



Ashley Cano
Custodian of Records

Date: November 14, 2019

- Once you get your results, make sure there is a certification along with the results

Copy/Tender/Review

- Use “control F” to search for keywords/names/dates





C

- Search in E

Snapchat Account Information	
username	email

- Some Snap

- Home
- Timeline
- Analyzed Data
- File Systems
- Insights
- Tags
- Reports

Extractions: 1

Legacy

Snapchat Snapchat Warrant Return

Extraction start date/time

Extraction end date/time

C:\Users\robert.kline\Downloads\Snapch...

Case Information

Examiner name: Parnitzke 55 Location: PHPD

Content

Data

- Device Events: 17
- Device Locations: 1813
- User Accounts: 1

Data Files

- Text: 5
- Videos: 4

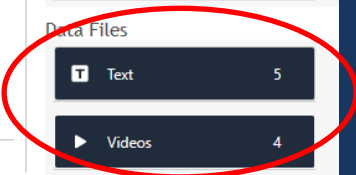
Malware scanner

Malware scan performed: No

W

	status

readers



Copy/Tender/Review

- Print out or flag important quotes/messages/photos/dates
- Create stills for emphasis



Sure, I got the evidence. Now, how am I gonna admit it?



iMessage



Authenticating

- Federal Rules of Evidence 901(a)
 - “To satisfy the requirement of authenticating or identifying an item *** the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.”
 - In other words: It is what we say it is

It is what we say it is

- Absolute proof IS NOT REQUIRED.
- Considering the evidence as a whole, if the court determines that the evidence supports a finding by a reasonable finder of fact, viewing the evidence most favorable to the proponent, that it is more probable than not that the matter is what the proponent says it is, the evidence will be admitted. *Graham, Clearly and Graham's Handbook of Illinois Evidence* §901.1, at 803 (8th ed. 2004)
- **Reasonable Probability Standard** – may use direct or circumstantial evidence to prove this. Once that's done, any issues will go to weight, not admissibility.
- Some states only require *prima facie* showing.

It is what we say it is

- Easiest way is self-authentication (i.e. The Business Record Rule)
 - Fed R. Evid. 902(11)
 - Written certification from custodian or qualified person that it:
 - (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of these matters;
 - (B) was kept in the course of the regularly conducted activity; and
 - (C) was made by the regularly conducted activity as a regular practice.
- But....

It is what we say it is

- Make sure you can attribute it to the defendant
 - Business records can easily authenticate it, but you still have to tie it to the defendant
 - Examples:
 - Device recovered from defendant
 - Defendant identified in videos/pictures
 - References to information only
defendant would have knowledge of



It is what we say it is

- Testimony of Witness With Knowledge - 901(b)(1)
 - Testimony that a matter is what it is claimed to be.
 - Ex: Text message from defendant
 - Recipient testifies about receiving message from a particular number and how they know the sender is the defendant
 - Prior communications with defendant / observing defendant draft it / particular language/content that only defendant has knowledge of
 - *In re Marriage of Larocque*, 2018 IL App (2d) 160973
 - Ex: Video of the crime
 - Prior to testifying, show them the video on a disc. Ask if it “truly and accurately depicts” the incident
 - Victim or witness testifies about the incident. Show them disc and have them identify it as truly and accurately depicting the crime.

It is what we say it is

- Ex: Social Media Officer or Detective downloads video from YouTube which shows offender celebrating his crime
 - Law Enforcement Agent can testify how they viewed the video, identification of the defendant, and how they obtained their copy
 - See *U.S. v. Washington*, 2017 U.S. Dist LEXIS 136220;
 - Get into specifics about when it was posted, when it was viewed

Hearsay Issues



Now that you've authenticated it, make sure you don't have any hearsay issues

If it is a statement by the defendant, it is by definition not hearsay, so long as it's being offered against a party and it's their own statement

- Can't be a statement by co-offender (unless it's a charged conspiracy) or you seek to admit it as an admission of a co-conspirator (Fed. Rule of Evidence 801(d)(2)(E)) in that the statement was made in *furtherance* of a criminal conspiracy.

Hearsay Issues

Problem: How do we admit statements by the victim TO the offender?

Answer: Explanation Exception, aka we are not offering it for the truth of the matter asserted, rather to give context to the offender's statement.

Thread (2132137423474598)

Current 2019-03-18 01:46:52 UTC

Participants Gbuddy Lilslick (100027863745883)
[REDACTED] (100000350837679)

Author [REDACTED] (100000350837679)
Sent 2019-03-13 20:31:32 UTC
Body Wya

Author [REDACTED] (100000350837679)
Sent 2019-03-13 20:30:13 UTC
Body By the mailbox

Author [REDACTED] (100000350837679)
Sent 2019-03-13 20:29:53 UTC
Body Same spot as last time

Author Gbuddy Lilslick (100027863745883)
Sent 2019-03-13 20:29:15 UTC
Body Where u want me ta meet

Author [REDACTED] (100000350837679)
Sent 2019-03-13 20:28:42 UTC
Body Coming around the block

Author Gbuddy Lilslick (100027863745883)

Case Law

- *People v. Kent*, 2017 IL App (2d) 140917
 - V was shot and killed in his driveway by his ex-GF's new boyfriend.
 - Day after the murder, a detective noticed a Facebook profile "Lorenzo Luckii Santos" which showed a picture resembling D and said "its my way or the highway...leave em dead n his driveway."
 - Detective testified to using a fake profile to monitor social media for criminal investigations. He found the post and printed it out. There was no testimony as to when it was posted, but he testified it was deleted that same day.
 - Prosecution argued it was tantamount to a confession to the crime
 - Appellate Court found it was error to admit – there was no direct or circumstantial evidence to show that defendant created the post.
 - Detailed analysis of other cases and what could be done to authenticate.

Case Law

- *People v. Kent*, 2017 IL App (2d) 140917 (cont'd)
 - Provided a non-exhaustive list of factors to consider whether something has been authenticated:
 - Sender admits authorship
 - Sender is seen writing the communication
 - Business records of provider show the communication originated from the sender's device under circumstances where it's reasonable to conclude that only the sender would have had access to the device
 - Communication contains information that only the sender could be expected to know
 - Sender responds to an exchange in such a way as to indicate circumstantially that they were the author of the communication

Case Law (cont'd)

People v. Harper, 2017 IL App (4th) 150045

- D convicted of murder – at trial, People admitted multiple text messages sent to D:
 - "I heard you had something to do with a white boy getting killed today."
 - "I heard a white boy got killed in the hood and you and some of your guys did it. That's the word on the streets"
- People established foundation to introduce calls/texts made by defendant through business records exception.
- Incoming text messages were inadmissible hearsay. Even if they identified the sender, can't admit "word on the streets"

Case Law (cont'd)

Atkins v. Commonwealth, 800 S.E.2d 827 (Va. App. 2017)

- D convicted of three counts of breaking and entering along with three counts of grand larceny.
 - When defendant was arrested during a traffic stop, his phone was recovered.
 - The phone was analyzed by police and, at trial, 20 text messages and a screen shot of a tweet were admitted
 - Messages were sent from the phone
- D argued that prosecution failed to establish that *he* authored the messages
- Appellate Court held standard was preponderance and that evidence did support a finding that he made the statements since:
 - He told police the passcode, he said it was his phone, his email address was on the phone, and there was a photograph of an item from his bedroom on the phone.

Case Law (cont'd)

People v. Ziemba, 2018 IL App (2d) 170048

- D convicted of involuntary sexual servitude of minor, travelling to meet minor, and grooming after backpage sting operation where D travelled to a Holiday Inn and was greeted by the police. Cell phone was recovered from D and was dumped via Cellebrite
- Text messages between D and the officer were admitted
 - Officer testified to responding to texts via laptop and advising D to “knock on door” and then saw the D knock on the hotel room door. Phone number of D’s phone matched number Officer was texting with.
- Court found that there was direct and circumstantial evidence which tied D to phone and messages
- “The proponent need prove only a rational basis upon which the fact finder can conclude that the document did in fact belong to or was authored by the party alleged.”

Case Law (cont'd)

People v. Brand, 2021 IL 125945

- D convicted of Agg Domestic Battery, Home Invasion, PSMV
- After the crime, the offender sent the victim 2 Facebook messages under name "Masetti Meech"
 - First message: detailing where she could find her car
 - Second message: threatening her family - "Your son not going to see 16«
 - A photo of the second message was entered, the first message had been deleted so its contents were testified to by the victim
- Admission of messages upheld; People established authentication of the messages via circumstantial evidence
 - Victim testified defendant routinely communicated with her via that screenname while they dated and the messages contained intimate information only the defendant would know

Case Law (cont'd)

People v. Curry, 2020 IL App (2d) 180148

- Offender convicted of criminal sexual assault
- Trial court ruled that the Facebook messages could be admitted as self-authenticating; content was subject to authentication by victim
- Victim testified that she'd been friends with defendant for years and routinely communicated via FB. She testified to receiving messages from his account after the incident asking her to say that her report was false (while he was in custody!).
- Detective testified to obtaining a search warrant for defendant's account and receiving messages from his account and a letter of authenticity from Facebook
- Appellate Court held they were properly admitted and that circumstantial evidence demonstrated authenticity:
 - Used nickname that defendant used for victim
 - Were sent almost immediately after the incident
 - Provided details only someone familiar with the incident would know

Case Law (cont'd)

United States v. Barber, 937 F.3d 965 (7th Cir. 2019)

- Defendant convicted of breaking into a hunting shop and stealing 15 firearms – at trial Facebook conversations about the robbery were admitted.
- Defense claimed that the prosecution had provided no proof that Facebook account belonged to him
 - ATF agent testified about finding the profile, that many "friends" were known friends, there were pictures of defendant, and it was linked to his cell number.
 - Friend of defendant testified at trial and identified pictures of defendant as well as messages they used to coordinate meet-ups.
- Court of Appeals affirmed – the testimony was "more than enough" for jury to conclude that account belonged to him

Case Law (cont'd)

United States v. Ramirez, 658 Fed. Appx. 949 (11th Cir 2016)

- Defendant convicted of a number of drug offenses
- At trial, used photographs of text messages purportedly sent by defendant to a co-conspirator/witness
- Defense argued the photographs of the text messages weren't authenticated and that there should have been forensic work on the witness' cell phone
- Appellate Court upheld admission: 1) witness identified the photos as being of texts between her and the defendant; 2) investigator testified that the subscriber information for the number listed the defendant.
- Further, found there was no "best evidence" rule violated here because government did not act in bad faith and testimony supported authenticity

Case Law (cont'd)

Tienda v. State, 358 S.W.3d 633 (Texas 2012)

- D convicted of murder – during sentencing, State admitted printouts of 3 separate MySpace profiles
- W testified to finding the profiles and providing them to prosecutors. Admitted multiple messages and pictures of D
- Court affirmed stating there was sufficient circumstantial evidence to establish that they were created/maintained by D.
 - Nickname, email address in D's name, pictures resemble D, messages included language only he would know – EM status and references to V

Case Law (cont'd)

State v. Mrza, 302 Neb. 931 (2019)

- Appeal after D convicted of 1st degree sexual assault
- The night after the incident, D initiated a text conversation with V via Snapchat; V indicated that D had been her “friend” on Snapchat and she knew his username.
- V testified she knew she was talking with him via Snapchat because it was with his same username. During the conversation, D apologized for his acts. Printed copies of the Snapchat messages were admitted at trial.
- Supreme Court of Nebraska agreed with State that authentication requires “evidence sufficient to support a finding that the matter in question is what its proponent claims”
- Added further, “proponent of evidence is not required to conclusively prove the genuineness of the evidence or to rule out all possibilities inconsistent with authenticity”

Case Law (cont'd)

Pugh v. State, 270 So. 3d 949 (Ct of Appeals, Miss. 2018)

- D convicted of conspiracy to commit sexual battery and sexual battery of an incapacitated person after taking part in the assault of an intoxicated woman.
- Portions of the incident were captured on Snapchat by one of the offenders.
- Witness testified to receiving it from co-D and providing it to police. Co-D testified for the prosecution and admitted to having sex with the victim. Testified about seeing flashlight which he later learned was someone filming it.
- Court of Appeals said this sufficiently authenticated the video for admission.
- “[W]e find the State produced sufficient evidence to support a finding that the Snapchat video admitted into evidence at trial was what the State claimed it was—that is, a Snapchat video from [an offender] depicting the alleged sexual battery of [the victim].” *Id* at 957.

Case Law (cont'd)

Lamb v. State, 246 So.3d 400 (Fla. 4th DCA 2018)

- D convicted of carjacking among other charges
- At trial, prosecution admitted a Facebook video of defendant sitting in the stolen car and wearing the victim's watch
- Digital forensic examiner testified as to how he found the video and downloaded it. Detective and Victim testified regarding identifying defendant and the items
- Appellate Court found it was properly authenticated:
 - Police testimony about how it was obtained
 - Distinctive characteristics and content testified to by victim and detective
- Defense also made discovery violation claiming that the examiner was an undisclosed expert
- Court concluded that they were not an expert because they did not give an opinion, rather they testified in the form of facts – they could testify about Facebook without it becoming an expert opinion

Case Law (cont'd)

Commonwealth v. Carrasquillo, 489 Mass. 107 (2022)

- Supreme Court of Massachusetts took on case where trial court allowed evidence that the defendant shared via SnapChat with an officer using a fake account.
- Officer sent a friend request to the defendant using a fake account, the defendant accepted it, and thus the officer could view content posted by the defendant's account. The defendant later posted a video of an individual holding a firearm. The officer recorded the video.
- Defense argued that the police use of a fake account violated the defendant's privacy
- interests
- Supreme Court ruled that while sharing social media diminishes the individual's privacy interests, it does not per se defeat them.
- Court upheld the admission of the evidence because defendant did not know what his privacy settings for the account were AND he diminished his expectation of privacy by accepting the officer's "friend" request despite not knowing the account.



What about
my
jurisdiction?

- 10th Circuit: *U.S. v. Arnold*, 696 Fed. Appx. 903 (10th Cir 2017)
- 11th Circuit: *U.S. v. Ramirez*, 658 Fed.Appx. 949 (11th Cir 2016)
- Connecticut: *State v. Manuel T.*, 337 Conn. 429 (2020)
- Georgia: *Pierce v. State*, 302 Ga. 389 (2017)
- New York: *People v. Franzese*, 154 A.D.3d 706 (2017)
- Ohio: *State v. Roseberry*, 197 Ohio App. 3d 256 (2011)
- Pennsylvania: *Commonwealth v. Murray*, 2017 PA Super 363
- Texas: *Tyler v. State*, 2016 Tex. App. LEXIS 680
- West Virginia: *State v. Benny W.*, 242 W.Va. 618 (2019)

Questions?

Robert.Kline@cookcountyil.gov
312-433-7082



iMessage

