Using Social Media as Evidence

Katherine Meger Kelsey, J.D.
February 2019

Indiana Rules of Evidence

Several of the Indiana Rules of Evidence are generally applicable to all types of social media and other technology based evidence. Generally, it is best to think in terms of authentication—providing evidence to show a court that the item is what you are claiming the item to be. If you are able to authenticate a piece of evidence from social media, it should be admissible. This does not require perfect, airtight, undisputable proof of the authenticity of an item of evidence.

Authentication is accomplished through the use of Indiana Evidence Rule 901, which is titled "Authenticating or Identifying Evidence." It provides:

(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) Examples. The following are examples only, not a complete list, of evidence that satisfies the requirement:

(1) Testimony of a Witness with Knowledge. Testimony that an item is what it is claimed to be, by a witness with knowledge.

(2) Nonexpert Opinion About Handwriting. A nonexpert's opinion that handwriting is genuine, based on a familiarity with it that was not acquired for the current litigation.

(3) Comparison by an Expert Witness or the Trier of Fact. A comparison with an authenticated specimen by an expert witness or the trier of fact.

(4) Distinctive Characteristics and the Like. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.

(5) Opinion About a Voice. An opinion identifying a person's voice whether heard firsthand or through mechanical or electronic transmission or recording based on hearing the voice at any time under circumstances that connect it with the alleged speaker.

(6) Evidence About a Telephone Conversation. For a telephone conversation, evidence that a call was made to the number assigned at the time to:

(A) a particular person, if circumstances, including self-identification, show that the person answering was the one called; or

(B) a particular business, if the call was made to a business and the call related to business reasonably transacted over the telephone.

(7) Evidence About Public Records. Evidence that:

(A) a document was recorded or filed in a public office as authorized by law; or
(B) a purported public record or statement is from the office where items of this kind are kept.

(8) Evidence About Ancient Documents or Data Compilations…
(9) Evidence About a Process or System. Evidence describing a process or system and showing that it produces an accurate result.
(10) Methods Provided by a Statute or Rule. Any method of authentication or identification allowed by a statute, by the Supreme Court of this State, or by the Constitution of this State.

Some other rules of evidence to consider when you are seeking to admit evidence from social media networks, or objecting to such evidence, include:

(1) *Rule 106, Remainder of or Related Writing or Recorded Statements*. This Rule provides that if a party introduces all or part of a writing or a recorded statement, the adverse party may require the introduction into evidence of any other part of the writing or recording, or any other writing or recorded statements that should, in the interests of fairness, be considered at the same time.
(2) *Rule 402, General Admissibility of Relevant Evidence*. This Rule provides that generally, relevant evidence is admissible, unless otherwise provided for by the US or Indiana Constitution, an Indiana statute, another evidentiary rule, or any other applicable rule.
(3) *Rule 403, Excluding Relevant Evidence for Prejudice, Confusion, or Other Reasons*. This Rule provides that even if evidence is relevant, it can be excluded by a court if its probative value is substantially outweighed by a danger of unfair prejudice, confusing the issues, undue delay, or needlessly presenting cumulative evidence.
(4) *Rule 404, Character Evidence*. The Rule provides that evidence of a person's character is not admissible to prove that the person acted in the same manner as the person's established character on a particular occasion. But see Matter of J.L.V., Jr., 667 N.E.2d 186 (Ind. Ct. App. 1996), In Re S.L.H.S., 885 N.E.2d 603 (Ind. Ct. App. 2008), and Matter of D.G., 702 N.E.2d 777 (Ind. Ct. App. 1998), all of which determined that parents' character and patterns of behavior towards their children were relevant and at issue, thus permitting the introduction of character evidence.
(5) *Rule 602, Lack of Personal Knowledge*. A witness can only testify on a matter if a sufficient foundation has been laid that the witness has personal knowledge of that matter. This evidence can include the witness's own testimony about his or her personal knowledge.
(6) *Rule 612, Writing or Object Used to Refresh Memory*. A witness can use a writing or an object to refresh his or her memory. If the witness uses a writing or an object, the adverse party is entitled to see it.
(7) *Rule 802, The Rule Against Hearsay,* and *Rule 805, Hearsay Within Hearsay*. These Rules provide that hearsay is not admissible, unless otherwise provided for in the rules or other laws; any amount of hearsay must itself be accounted for by an exception.
(8) *Rule 803, Exceptions to the Rule Against Hearsay*. This Rule provides for many exceptions whereby hearsay would be admissible if the moving party is able to meet certain foundational requirements.
(9) *Rule 1002, Requirement of the Original,* and *Rule 1003, Admissibility of Duplicates*. These Rules provide that while an original writing, recording, or photograph is required,

> a duplicate is admissible, just the same as an original, unless a genuine question is raised about the original's authenticity, or the circumstances make it unfair to admit the duplicate.

This is not an exhaustive list of evidentiary rules which may apply to admitting a piece of social media evidence. However, these rules are those which do come up frequently in the course of admitting and objecting to a piece of social media evidence.

Authentication Tips

"Authentication of an exhibit can be established by either 'direct or circumstantial evidence.'" Strunk v. State, 44 N.E.3d 1 (Ind. Ct. App. 2015), citing Newman v. State, 675 N.E.2d 1109, 1111 (Ind. Ct. App. 1996). Testimony is an acceptable method of providing this evidence for authentication; having a witness with knowledge about the item of evidence testify, and have the witness's testimony demonstrate that the item of evidence is what you claim it to be, is therefore sufficient. Testimony that can lead to authentication of an item of evidence can include testimony about distinctive characteristics of the item of evidence, such as "appearance, contents, substance [and] internal patterns". Id. Any inconclusiveness about regarding an exhibit's connection regarding the exhibit's connection with the events at issue goes to the exhibit's weight, not its admissibility. Pavlovich v. State, 6 N.E.3d 969, 976 (Ind. Ct. App. 2014).

For purposes of these materials, the term "post" will refer to any kind of statement made by a person to his or her general followers on a social media network. This includes Facebook posts, tweets on Twitter, posts of pictures and accompanying captions on Instagram, etc.

The first method of authenticating a social media post is a fairly simple one. Take screen shots of the post which clearly indicate who is making the post, and taking screen shots of the profile of the person who made the post. Call the person you are alleging to be the owner of the social media account to the witness stand, and ask them to admit that post is his own, or that the profile is his own, or both. If the person admits both, then you have accomplished your goal of authentication. If the person admits one but denies the other, by extension, you may then authenticate that this post is his own post, made by him.

Another method of authenticating a social media post involves another witness besides the account holder. Take screen shots of the post which clearly indicate who is making the post, and taking screen shots of the profile of the person who made the post. Call the witness you are using to authenticate the posts. This witness could authenticate the social media posts by indicating that he recognizes the person from her profile picture, and that he has previously communicated with this person through her social media account.

A social media account holder's profile picture may not be his own picture, but instead, may be a caricature, an image of thing or animal, or an image of a fictional thing or person. It is still quite possible to authenticate a social media post, even if the account holder is using such an online avatar. Take screen shots of the post which clearly indicate who is making the post, and taking screen shots of the profile of the person who made the post. The witness authenticating the account and the post can indicate that she knows that this is the person's account, because she

knows that this online avatar represents him. She may know this because of a personal connection between the person and avatar image, or because she is a friend or follower of this person, and has previously communicated with the person through his social media account.

Authentication of a social media page by a witness can be further bolstered by testimony that the witness has observed the "mutual friends" or followers list, and that this list contains several people who the witness can also identify, indicating that they are in the same circle of friends. For example, in Strunk v. State, 44 N.E.3d 1 (Ind. Ct. App. 2015), the witness was able to note that she and the defendant had two mutual friends, one of which was the witness's own mother. The witness may also add to authentication by testifying that the account contains postings which indicate interests of, affiliations with, and facts about the alleged account holder that the witness knows to be accurate. See Wilson v. State, 30 N.E.3d 1264, 1267-8 (Ind. Ct. App. 2015) (holding that tweets were authenticated in part because the tweets from the account indicated an affiliation with groups to which the defendant belonged).

Other things which lend themselves towards authenticating social media posts as belonging to a specific person are: (1) evidence that the social media profile or posting contains information that only the alleged owner of the account would know; (2) evidence that the person you are alleging is owner of the social media account has a certain style of talking, writing, or distinctive grammar or spelling mistakes, and that this social media account contains those certain styles of distinctive manners and mistakes; and (3) the posts on the social media account contain multiple pictures of the alleged owner, either by himself or with others.

You must be sure that you also have the witness testify that the exhibit which you are offering, a screen shot of the post, the profile, or the homepage of the account, is the same one that she knows to belong to person in question.

For other articles which also discuss many of these tips and situations dealing with social media, technology based evidence, and resulting evidentiary issues, see "Authenticating Facebook Posts, Photos, and Other Evidence" by Melanie Reichert, in the Spring 2015 edition of *Family Advocate*; and "Texts Present Unique Challenges in Evidence Preservation and Admission" by Dave Stafford, *Indiana Lawyer* (February 11, 2015). See also "How Google Search History And Facebook Posts Are Putting People In Prison" by Vic Ryckhaert, *Indy Star* (August 13, 2018); "Facebook Defamation Judgment May Set Precedent, Indiana Lawyers Say" by Dave Stafford, *Indiana Lawyer* (February 7, 2018).

Other Technology and Evidentiary Problems

Other electronic forms of communication, while older than social media, still seem to pose issues for attorneys and courts when it comes to their admissibility as evidence. However, the Indiana Rules of Evidence as well as Indiana case law both provide for the admissibility of electronic records, as long as they are properly authenticated. In the context of family law cases, perhaps the most common of these are cell phone records, specifically text messages, and emails.

Once again, we must remember that "[a]uthentication of an exhibit can be established by either 'direct or circumstantial evidence.'" Strunk v. State, 44 N.E.3d 1 (Ind. Ct. App. 2015), citing

Newman v. State, 675 N.E.2d 1109, 1111 (Ind. Ct. App. 1996). This amounts to having a witness with knowledge about the item of evidence testify, and have the witness's testimony demonstrate that the item of evidence is what you claim it to be.

If you can have the person you claim to be the owner of the email address or cell phone actually authenticate the emails or text messages which you wish to enter into evidence, that is easiest and best. To do so, you would present the person with the email or text messages which you wish to enter into evidence. You would point to the email address or telephone number and ask if that is her email address or telephone number. Ask her if she remembers writing the email or text messages, and if she remembers it, admit the item or items into evidence. If she denies writing the email or text messages, or you suspect that she will deny it, it would be prudent to establish authenticity through a few further things. First, establish that it is her phone number or email address through the admission of innocuous items, such as friendly email or text message exchanges. Note any distinguishing characteristics, such as common mistakes, misspellings, grammar, signature blocks, font styles, use of emoticons, tone, word usage, etc. Once you have established these items, use the similarities, plus the admission of the ownership of the phone number of email address to authenticate the item which you are trying to admit.

Remember that authenticating an electronic device is not necessarily authenticating the data contained in the device. In multiple cases, Indiana courts have held that authentication of ownership of a device is not necessarily the same as authentication of the data stored on the device. See Hape v. State, 903 N.E.2d 977, 990-1 (Ind. Ct. App. 2009); Bone v. State, 771 N.E.2d 710, 712 (Ind. Ct. App. 2002).

You should also remember that, in the case of admitting electronic records, especially text messages, it is best to have physical printouts of the text messages. Do not try to offer the cell phone itself into evidence, as that would leave your client without a cell phone. There are several software programs or applications that will perform this for you; some of them include SMS Backup, CopyTrans Contacts, Phone View by ecamm, and iMazing. Applications and software items go out of date and new items become available on unpredictable cycles, so use the internet to research which options would be best for your situation. You do not need to be able to describe with specificity the manner in which such a program moves the data from one location to another. You need only be able to describe the steps your client took. See In Re Paternity of B.B., 1 N.E.3d 151, 155-9 (Ind. Ct. App. 2013)

Text messages and emails can be authenticated by a witness other than the alleged owner of the email address or phone number. A witness can be used to authenticate an email or text through communication with the alleged owner of the phone number or email address about doing a certain activity, and the activity is completed. An example of this would be arranging to meet in person and then actually meeting in person. Emails and texts can also be authenticated by the contents of conversation, if the contents are the continuation of an earlier, in person conversation, and neither the witness nor the person who owns the phone number are expressing any confusion about the conversation, or about with whom they are communicating. For example, a witness and the owner of a particular email address met in person and spoke about purchasing puppies, exchanged email addresses, and then the witness later emailed the other person, carrying on the conversation about the purchase of puppies. If the person owning the

email address does not express confusion about the topic, or from whom they are receiving this email about puppies, this is an indication that it is the same person that the witness met with earlier in person, and that the person is in fact the owner of the email address, and is the sender of the emails. Perhaps the witness has called the phone number, and is able to identify the person's voice through answering the phone, or the voicemail message. Lastly, authentication can be aided though specific facts in text messages or emails. For example, an email or text message exchange may include, in part, a mention that the person attended funeral for her grandmother that weekend. If the person you are alleging owns the email address or phone number attended such a funeral, then that evidence lends itself to authentication.

Evidence and testimony regarding photographs can be admitted into evidence, even if the photographs are not admitted or are not available. In In Re J.V., 875 N.E.2d 395 (Ind. Ct. App. 2007), the Court held that admitting testimony about photographs, rather than the photographs themselves, was not an abuse of discretion in that it was consistent with the exception to the best evidence rule of evidence which allows for the admission of evidence of the contents of a photograph where the original is lost or destroyed unless the proponent lost or destroyed the original in bad faith. In order to invoke this exception to the best evidence rule, the proponent of the evidence must demonstrate that the original was lost or destroyed by showing that a diligent but unsuccessful search has been made in the place or places where the original was most likely to be found. The Court reviewed the relevant evidence and concluded that it showed the officers made a diligent search for the photos and memory card, and were unable to find them in the place where they were most likely to be found, Parents' residence. Id. at 401-02.

Recorded telephone conversations or videotapes may present issues of authentication and consent. The Indiana Supreme Court has laid out five foundational requirements for the admission of tape recording into evidence: (1) it must be authentic and correct; (2) the testimony in them must be freely and voluntarily made, without any kind of duress; (3) all required warning were given and all necessary acknowledgments and waivers were knowingly and intelligently made; (4) it does not contain matter otherwise not admissible into evidence; and (5) it is clear enough to intelligible and enlightening to the jury or finder of fact. Lamar v. State, 258 N.E.2d 795 (Ind. 1972). Later case law clarified that factors (2) and (3) only apply in the context of a custodial interrogation of an accused person. In civil cases, he following foundational elements are required to admit a tape recording: (1) it must be authentic and correct; (2) it does not contain matter otherwise not admissible into evidence; and (3) it is clear enough to intelligible and enlightening to the jury or finder of fact. Apter v. Ross, 781 N.E.2d 744 (Ind. Ct. App. 2003).

The federal Wiretap Act can be found at 18 U.S.C. § 2510 *et seq*. There is an exception to the federal Wiretap Act pursuant to Schieb v. Grant, 22 F.3d 149 (7th Cir. 1994) and Apter v. Ross, 781 N.E.2d 744 (Ind. Ct. App. 2003), which taken together, provide that since a parent's business is raising their children, parents cannot subject to civil and criminal penalties for recording their minor's phone conversations out of concern for their child's well-being. The determining factor is the parent's concern, not the child's well-being, and thus, the court must consider evidence that relates directly to the parent's concern and not necessarily the child's reactions or well-being.

The Indiana Wiretap Act can be found at IC 35-33.5. Under the Indiana Wiretap Act, a recording of a conversation is not an interception if it is done with the consent of the sender or the receiver of the communication. IC 35-33.5-1-5. Indiana law provides that unless there is another determination by court or by statutory law, parents have the ability to consent on behalf of a minor under any Indiana statute. IC 29-3-3-3(a); see Apter v. Ross, 781 N.E.2d at 756. Thus, a parent has the power to consent on behalf of their minor child to the minor child being recorded on a telephone conversation unless that ability to consent is otherwise limited in another legal proceeding. Id. If the parents share an award of joint legal custody, this is sufficient for either parent to consent to the recording on behalf of the child. Id.

Parents may allege that recording phone conversations interferes with their ability to communicate with their children. The Indiana Parenting Time Guidelines provide that recording a phone conversations may constitute an example of unacceptable interference with communication. In Leisure v. Wheeler, 828 N.E.2d 409 (Ind. Ct. App. 2005), Father recorded telephone conversations between the child and Mother, and Mother alleged that this interfered with her communication with the child. The Court noted that while Father was potentially able to consent on behalf of the minor child to recording telephone conversations, he also had to be motivated by a genuine concern for the welfare of the child. The Court noted that evidence showing that the intent was interference rather than protection of the child could be a factor for a court in making a determination about custody or parenting time. Id. at 415-16.

Preserving Evidence

What if the evidence which you are seeking is not part of the general public sphere of a particular social media network? Perhaps the opposing party in a case has a Facebook account, but has her privacy settings set so that neither you nor your client or your client's friends or relatives can access it. However, your client recalls the opposing party would tell your client that she would conduct drug deals over Facebook. How can you access and use that information?

It's difficult to get information from Facebook, or from other social media networks. For a thorough discussion of this issue, see "Discovery and Preservation of Social Media Evidence" by Margaret DiBianca, *American Bar Association*.[1] Each social media network has its own release of information policy and should be closely followed if you hope for any degree of success in gaining information. For an example, we will look at Facebook. If you are not law enforcement, Facebook will only release basic subscriber information, not content. It will only release basic information is the following conditions exist: the requested information is indispensable; not in the requesting party's possession; if Facebook receives a valid subpoena; from California state court, or a Federal court. Id. If you want content, you will most likely need to rely on the opposing party and the discovery process to obtain this content. Facebook explains:

> 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

[1] Available at https://www.americanbar.org/publications/blt/2014/01/02_dibianca.html

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 account information or account contents using a subpoena?" Available at www.Facebook.com/Help (emphasis added).

This last italicized sentence indicates that if you are not law enforcement, it appears that Facebook will not preserve evidence in the face of a "Notice of Preservation" letter. It's very important that you send this type of letter to opposing counsel, and be as specific as you can be in your requests. Hopefully, this will aid you in obtaining information via normal discovery routes, without such information being deleted.

Examples of Social Media Situations and Evidentiary Issues

Your client, Mother, is still friends with Father, her now ex-husband, on Facebook. The court has ordered that shall be no contact between their child and Father's new girlfriend, who has several substantiated CPS reports against her regarding her own children, as well as a current open CHINS cases regarding her children. Father posted a video posted on his Facebook page yesterday, and Mother viewed the video. It shows the child sitting in the girlfriend's lap, wearing the same clothes that Mother sent the child to Father wearing just yesterday. Before you are able to determine a way to make a copy of the Facebook video, Father deletes it.

Police officers conduct a search of an apartment under emergency circumstances. During the search, they discover a digital camera which contains pictures of the adults in the apartment, as well their children, in various stages of undress and engaged in sexually explicit acts. The police obtain a search warrant, and come back to obtain the camera, but the pictures have been deleted.

Father was alerted by a common friend that Mother has an Instagram account. Father locates the Instagram account, and it is under a handle that seemingly has no connection to Mother's name, and the profile picture does not reflect Mother. There are many pictures of various types of alcohol in bottles, alcohol in glasses in varying stages of consumption, and pills of varying types. These pictures are all captioned with comments about getting drunk, getting high, and enjoying being that way. Father recognizes some of the friends who favorite her posts and comment on her posts. Father recognizes the coffee table in many of the posts as one that he made and finished for Mother, and knows that Mother kept this table when they separated.

Mother and Father had a child together and continued to live together. While they were still together, Father texted Mother's mother, Maternal Grandmother, a link to his Twitter page, and gave her his password in the same text message. Father asked Maternal Grandmother to post a picture of the child for him. Father never changed his password. Maternal Grandmother became concerned about Father's and Mother's erratic behavior and decided to ask for guardianship. Maternal Grandmother logged into his Facebook account. She accessed his private messages, and discovered several conversations where Father offered to both buy and sell pills of varying types, and conversations where he asked for heroin.

Selected Relevant Indiana Case Law

Price v. State, ___ N.E.3d ___ (Ind. Ct. App. 2019) (*citation not yet available*) (February 22, 2019). The Court discussed constitutional implications of the search and seizure of a cell phone when a defendant was possibly deleting data.

Saintignon v. State, ___ N.E.3d ___ (Ind. Ct. App. 2019) (*citation not yet available*) (January 17, 2019). The Court held, *inter alia*, that the probative value of a picture of the defendant with an injury on his arm two days after the victim was murdered outweighed the potential for prejudice. The State had agreed prior to trial that it would not admit evidence of the defendant's membership in the Aryan Brotherhood. At trial, the State offered evidence showing an injury on the defendant's arm, and such injury would make it more probable that the defendant was the killer. However, the picture also included the defendant's tattoo, which was an Aryan Brotherhood tattoo. The Court concluded that since the State presented no evidence or explanation about what the tattoo was, and the injury was highly relevant to the issue at hand, the minimal prejudice, if any, did not render the photograph inadmissible.

McCallister v. State, 91 N.E.3d 554 (Ind. 2018). The Court held, among other things, that the trial court did not abuse its discretion in admitting a DVD showing surveillance video from a station camera overlooking the hotel lobby; that the trial court did not abuse its discretion by admitting a recorded phone conversation between the defendant and his girlfriend; that the trial court did not abuse its discretion in admitting several mobile phone records. Regarding the surveillance video, the Court noted the trial court was entitled to admit the video as a "silent witness", meaning it was substantive rather than demonstrative evidence. This required a strong showing of authenticity and competency, including proof the video was not altered. The Court noted the time stamp date, the testimony of the hotel manager about the authenticity of the video, both from the time stamp and from the contents of the video, and the testimony of the manger about the chain of custody of the video. Regarding the recorded jailhouse phone conversation, the Court noted the notices posted that all conversations are recorded, the defendant's waiver of the issue by failing to properly raise it at trial, and the non-incriminating nature of the conversation. Regarding the mobile phone evidence, the Court noted that in one instance, the admitted material was an FBI report of the contents of the phone, including some text messages, and the defendant had not objected to its admission. The Court also noted that the State had presented sufficient foundation and authentication; the detective crossed checked the defendant's phone number with the FBI report, and the report itself showed the defendant's phone number ladled with his initials. The Court deemed this sufficient to provide a foundation for admitting the report, especially since there was no objection. In the other mobile phone instance, the defendant objected to the recording being played, claiming no one had been adequately identified. The Court determined that Ind. Evid. R. 901(a) had been satisfied—there was testimony identifying the individuals' voices from the detective, who was familiar with all three individuals on the phone call.

Wynne v. Burris, 105 N.E.3d 188 (Ind. Ct. App. 2018). The trial court did not abuse its discretion in admitting into evidence recorded telephone conversations from jail between the plaintiff and his girlfriend. Wynne argued that the recordings were illegal and not admissible. The Court noted that the Indiana Wiretap Act at IC 35-31.5-2-176 provides that the recording of a communication with the consent of either the sender or the receiver is not an interception. The Court also cited Edwards v. State, 862 N.E.2d 1254 (Ind. Ct. App. 2007). When calls from jail

are places by a sender, the receiver is given an admonishment at the beginning of the call that it may be recorded. Wynne's girlfriend was admonished that he call was recorded and she still accepted the call; further, Wynne acknowledged that calls were recorded. The Court deemed this to be consent.

Laird v. State, 103 N.E.3d 1171 (Ind. Ct. App. 2018). The Court held that the other-acts evidence about the defendant's internet search history was admissible to show the defendant's plan to molest the child victim. Despite pre-trial motions which attempted to exclude the evidence, the defendant did not raise the object to the evidence during the hearing when the evidence was introduced. Thus, he failed to preserve the matter for appeal. The defendant had claimed that the internet search history was not admissible under Ind. Evid. R. 404(b), which is designed to prevent a jury from making a forbidden inference that prior wrongful conduct suggests present guilt. The State argued that the evidence was admissible under Ind. Evid. R. 404(b)(2), which was to show his plan or preparation to molest the child victim. The Court agreed with the State under the facts of this case, but noted that this exception could not engulf the rule. Furthermore, the defendant placed his intent at issue by claiming anything he did was accidental; the internet history evidence was admissible to show intent rather than accident.

Sparks v. State, 100 N.E.3d 715 (Ind. Ct. App. 2018). The Court held that taking a recording of a defendant from a social media page of a conversation that had already taken place was not a contemporaneous recording of the defendant, and therefore did not violate the federal Wiretap Act. The Court noted that federal courts have routinely concluded that the federal Wiretap Act only applies to "contemporaneous" interceptions of wire, electronic, or spoken communications. This means it applies only to communications which are in transit, and not to communication's which have already been made and are in storage. The facts of case were undisputed, namely, that the Facebook account housed a recording of a conversation which had already taken place and was stored on Facebook. Thus, there was no violation of the federal Wiretapping Act.

Keith v. State, 105 N.E.3d 1147 (Ind. Ct. App. 2018). The Court held that the state present sufficient evidence to show that the defendant was guilty of possession of child pornography. The defendant had argued on appeal that "receiving an image sent by somebody else that is automatically deleted by the application is not possession under Indiana law and that he did not 'intentionally point a web browser to certain websites to view them'". The defendant had encouraged the victim to use Snapchat to send him images of her uncovered breasts and genitalia.

Taylor v. State, 101 N.E.3d 865 (Ind. Ct. App. 2018). The Court held that the trial court did not err in allowing the detective to testify as to what he was able to recover from the defendant's phone using he "Chip-Off" forensic technique. The defendant specifically argued that the detective failed to meet the standard for the admission of expert scientific testimony under Ind. Evid. R. 702. The Rule provides that a witness who is properly qualified as an expert may testify in the form of an opinion if the expert's specialized knowledge will assist the tier of fact in understanding the evidence or making a determination, and that expert scientific testimony is only admissible if the court is satisfied that the expert testimony is based on reliable scientific principles. The party seeking to admit expert scientific testimony bears the burden of establishing both the foundation and the reliability of the scientific principles that are the basis for the expert

testimony. Reliability can be established by judicial notice, or by another sufficient foundation to convince the court that the scientific principles at issue are sound. Court may also consider the following: (1) whether the technique has been or can be empirically tested; (2) whether the technique has been subjected to peer review and publication; (3) the known or potential rate of error, along with the existence and maintenance of standards controlling the technique's operation; and (4) general acceptance within the relevant scientific community. The Court noted that the detective had extremely extensive field training in the area of cell phone forensics, with forty hours specific to the "Chip-Off" technique; that the technique was being peer reviewed and had been in use since approximately 2014; that national institutes have established guidelines regarding the technique; and that the detective had employed this particular technique seventy-one times, sixty-one of which were successful. The Court also opined that the detective's testimony was not scientific in nature, but rather, was technical or specialized knowledge. Since the testimony was about specialized knowledge acquired through training and experience, it fell under Ind. Evid. R. 702(a)'s provision for specialized knowledge, and did not need to be proved reliable by scientific principles under Ind. Evid. R. 702(b).

Strunk v. State, 44 N.E.3d 1 (Ind. Ct. App. 2015). The Court held that the trial court properly admitted the Facebook message from the defendant to the child. After molesting the child in what he claimed was a ritual, the defendant sent a Facebook message to the child, stating "im [sic] sorry about what happened. But if yoi [sic] possibly can we need to finish the ritual. Untill [sic] we do i [sic] must suffer the aftermath of it all. That is what caused the seizures. And it will only get worse from there. So please save me from this suffering. Please I beg of you." At trial, the child testified that: (1) she had previously communicated with the defendant through his Facebook page, as recently as earlier that day; (2) the defendant's Facebook profile picture was that of a wolf; (3) the exhibit being offered was the defendant's Facebook page, because it contained the same profile picture; and (4) she also knew it was the defendant's Facebook page, because it listed two mutual friends between herself and the defendant, one of which was her mother.

Clark v. State, 915 N.E.2d 126, 129-131 (Ind. 2009). The Court held that the trial court did not err in admitting the defendant's posting on his MySpace page into evidence. The defendant first argued that his MySpace posting was inadmissible character evidence under Indiana Evid. R. 404(b). The Court determined that Rule 404(b) did not apply to this particular piece of evidence, a post made by the defendant, which stated:

> Society labels me as an outlaw and criminal and sees more and more everyday how many of the people, while growing up, and those who judge me, are dishonest and dishonorable. Note, in one aspect I'm glad to say I have helped you people in my past who have done something and achieved on the other hand, I'm sad to see so many people who have nowhere. To those people I say, if I can do it and get away. B ... sh.... And with all my obstacles, why the f ... can't you.

The Court opined that this posting was made by the defendant himself, and it contained only statements about himself, not about the defendant's prior deeds or criminal acts. Consequently, Rule 404(b) did not apply, and the evidence was deemed to probative of issues at trial. The Clark Court also determined the MySpace entry was also probative evidence of an issue at trial. The defendant testified that, at most, he was reckless because he was drunk, and repeatedly suggested during his testimony that his state of mind and requisite intent could only have been best called

reckless or irresponsible, and not criminal. The Court opined that "[o]nce [the defendant] took the stand to testify along these lines, it was proper to permit the prosecution to confront [the defendant] with his own seemingly prideful declarations that rebutted his defense."

Wilson v. State, 30 N.E.3d 1264, 1267-8 (Ind. Ct. App. 2015). The Court held that the social media posts made on Twitter, allegedly by the defendant, were sufficiently authenticated. The defendant argued that the Tweets had not been properly authenticated as being authored by him. The Court noted that Federal Rule of Evidence 901(b)(4) was one of the most frequently used means to authenticate electronic data, including text messages and emails. Indiana Evid. R. 901(b)(4) is analogous to this Rule. In deeming the authentication of the Tweets to be sufficient, the Cort noted the following: (1) the witness testified that she frequently communicated with the defendant on Twitter; (2) the defendant had posted pictures of himself and the witness via Twitter; (3) the witness identified the account as the defendant's Twitter account based on her knowledge of the defendant's online handle and the general appearance of the account and profile; (4) there were multiple pictures of just the defendant posted from the account; and (5) the Tweets from the account indicated an affiliation with groups to which the defendant belonged.

Pavlovich v. State, 6 N.E.3d 969, 976-980 (Ind. Ct. App. 2014) transfer denied, 9 N.E.3d 678 (Ind. 2014). The Court held that the defendant's text messages and emails were sufficiently authenticated and were admissible, despite the lack of a direct connection between the defendant and the text messages and emails. The phone company records for the number in question were associated with a different name, and the address was an address in the middle of a highway. Police had not searched any cell phone that the defendant had at the time of his arrest to verify if his phones were associated with the number in question, or whether the defendant had used the phones to communicate with the witness. After going through an analysis of the Indiana Evidence Rules, and cases from other states, the Court determined that the text messages and emails were sufficiently authenticated despite the above noted facts, and were admissible. The Court noted the following: (1) the witness testified that after she and the defendant had arranged an in person meeting through text messages and a phone call from the number; (2) the witness identified the defendant in court as the man who had sex with her at the meeting; (3) the witness was familiar with the defendant's voice from talking to him on the phone, and it was the same voice as the man she met in person; (4) the conversations the witness had with the defendant via text message were continuations of the conversations they had in person; (5) the defendant supplied his email address in these text message conversations; (6) at no point in the email or text messages exchanges did the defendant express any confusion about who was texting or emailing him, the contents of the conversation, or references to conversations the defendant and the witness had in person; (7) when an email indicated that he was staying at specific hotel, a detective was able to confirm that the defendant was registered at that same hotel; and (8) the voicemail message associated with the number was identified by the witness as the defendant's voice.

In Re Paternity of B.B., 1 N.E.3d 151, 155-9 (Ind. Ct. App. 2013). The Court held that the printout of text messages from Father to Mother was sufficiently authenticated and therefore admissible. Father argued that the text messages had not been sufficiently authenticated, that the printout contained text messages that did not logically flow as a conversation would, lacked context, appeared to start in the middle of a thought, that parts of conversations were missing,

and that Mother was unable to discuss the program which she used to produce the text messages. Mother had obtained the text message document by plugging her phone into a computer, which ran the data from the phone through a software program, which transcribed the text messages. Mother was not able to specifically describe any further how the program worked. In deeming the text messages sufficiently authenticated, the Court noted: (1) Father identified the phone number as his, and the other phone number as Mother's; (2) Father indicated that he didn't doubt it was him, and that he remembered some of the conversations; (3) Mother believed that every text from a certain time period was in the document; (4) although Father claimed that parts of the messages were missing and deleted by Mother, he was unable to point to any specific examples; (5) Father did not attempt to introduce his own version of the complete text messages, and he never testified that the text messages that were on his own phone were unavailable to him; and (6) Father's argument was more about the doctrine of completeness rather than the authentication of the text messages.

Hape v. State, 903 N.E.2d 977, 990-1 (Ind. Ct. App. 2009). The Court held that while the physical cell phone had been sufficiently authenticated as the defendant's, the text messages themselves had not been sufficiently authenticated. However, this was not a fundamental error requiring reversal. Authentication of data saved in an electronic device, such as a cell phone or a computer, is a condition precedent to the admission of the data. The Court had determined that a text message stored in a phone is intrinsic to the phone; however, it is possible to offer both the phone and the text message as spate pieces of evidence, for separate purposes. If the State had intentionally offered the text messages into evidence, it would have been for the purpose of the jury's ability to read and use those text messages in making its determination of guilt. As it was, the State only intentionally admitted the cell phone itself, and a jury member was able to turn it on and read text messages during deliberations.

Fry v. State, 885 N.E.2d 742, 745-8 (Ind. Ct. App. 2008), *trans. denied*. The Court held that the trial court did not abuse its discretion in concluding that the cell phone records were admissible. The Court concluded that the contents of the cell phone records, considered in conjunction with the State's third-party discovery requests and the certification from the cell phone companies that the attached records are true and accurate, created a reasonable probability that the cell phone records were what they claimed to be. Absolute proof was not required, only reasonable probability that the item was what it claimed to be.

Bone v. State, 771 N.E.2d 710, 712 (Ind. Ct. App. 2002). The Court determined that testimony before court was sufficient to establish authenticity of exhibits as depicting images contained in defendant's computer. The detective testified that he had seized the defendant's computer, described the process by which he transferred images to the exhibit, and how the images were unaltered in the transfer.