Foundations and Admissibility: Evidence in an Electronic World

Stephen M. Terrell,
Terrell Law Office, LLC,
Indianapolis, IN
terrell@hoosierlawyer.US

I. Overview

Social media and other electronic communications are now an essential part of our daily life. And with that, they have become an essential part of courtroom evidence.

Text messages, Facebook posts and photos, Instagram images, LinkedIn profiles, emails -- all are now part of any lawyer's arsenal of evidence at trial. A Casemaker search of Indiana case law reveals several hundret appellate court decisions involving social media and electronic evidence. These cases cover the spectrum of legal disputes: family law, protective orders, juvenile matters, breach of contract, defamation, child molestation, drug dealing, probation revocation, prostitution, murder -- nearly every type of litigated dispute, both criminal and civil.

Lawyers walking in to courtrooms must be prepared to present and object to social media and electronic evidence.

For a general overview, see Sharon Nelson & John Simek, *The Legal Implications of Social Networking*, 22 Regent U.L.Rev 1 (2009); Edward M. Marsico, Jr., *Social Networking Websites: Are MySpace and Facebook the Fingerprints of the Twenty-First Century*, 19 Widner L.J. 967 (2010); Katherine Minotti, *Evidence: The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.Car.L.Rev. 1057 (2010).

II. Discovery and Sources of Electronic Evidence

Although this presentation does not focus on the issue of discovery, lawyers must keep in mind the extent to which social media and other electronic communications are discoverable, and the sources of that information.

For criminal defense lawyers, the most significant recent case is Riley v. California, 573 U.S. _____ (June 25,2014). In a 9-0 decision, Chief Justice Roberts wrote for a rarely united Supreme Court holding that a search warrant was required for police to search the contents of a cell phone, stating:

> "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."

Perhaps the most complete discussion of discovery and social media by any Indiana court is the decision in *E.E.O.C. v. Simply Storage Management, LLC*, 270 F.R.D. 430 (S.D.Ind. 2010).

In that case, Simply Storage sought broad ranging discovery of social media profiles and postings of the plaintiff employees. Magistrate Lynch noted the surprising lack of legal authority addressing discovery and social media, then set out a broad test that adopted neither of the bright-line tests proposed by the parties. "[D]espite the popularity of SNS (social networking sites) and the frequency with which this issue might be expected to arise, remarkably few published decisions provide guidance on the issues presented here."

The court effectively ordered an item-by-item review of postings and profiles, as well as third-party communications, and production of any that broadly touched on the issues of emotional distress raised by the pleadings.

Magistrate Lynch did issue a warning shot to those who carelessly post their every thought on the Internet and consider their posts on Facebook and other social media to be private. Not so.

"[M]erely locking a profile from public access does not prevent discovery." Magistrate Lynch stated, then further explained:

> [B]road discovery of the claimants' SNS could reveal private information that may embarrass them. . . . [T]he court finds that this concern is outweighed by the fact that the production here would be of information that the claimants have already shared with at least one other person through private messages or a larger number of people through postings. As one judge observed, "Facebook is not used as a means by which account holders carry on monologues with themselves."

Two important notes regarding discovery and electronic information. First, content of electronic communications including social media posts, messages and photos, is not available to private party litigants, even with a subpoena or court order. The federal Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits disclosure of electronic commuications to any non-governmental entity. So even if you subpoena Facebook, you will only be able to obtain identifying information and data, not actual postings.

Second, government authorities can obtain any web-based email as soon as it is opened or marked read - even without a warrant or subpoena. Additionally, any document or data stored in the "Cloud" is available to the government without subpoena or search warrant after six months.

Contrary to the assumptions of most people, email on services such as Gmail, Yahoo and hotmail may be accessed by the government -- and are being accessed by the government -- without subpoena or warrant. This is a product of the federal Communications Privacy Act of 1986, codified at 18 U.S.C. § 2510 et seq., which has since been amended by both the Stored Communications Act (above) and, following 9/11, the Patriot Act.

When this act was created in the mid-1980s, email was simply a gleam on the horizon and no one, not even Bill Gates, was imagining the Cloud and all the data stores there. But it exists now. And federal law says that once it is in the Cloud for 180 days, it is fair game for the federal government to access without warrant or subpoena.

Efforts have been made to amend existing law to require subpoenas for web-based email and data stored in the Cloud. But those efforts have been resisted by the government, both under the Bush Administration and now from the Obama Administration. At this point, the law remains unchanged.

There are many sources of electronic evidence, and more each day. Here is a listing of some of the most frequent sources of social networking and other electronic evidence.

- Text messages. personal messages sent (generally) phone to phone through cell phone providers.

- Email, including business email. This includes office email, email handled by Internet Service Providers, and webmail services like Gmail, Yahoo and hotmail.

- Facebook. With over 1 billion monthly users, if Facebook was a country, it would be the third largest nation on earth behind only China and India. Nearly 500 million people use Facebook's mobile app. Nearly 1 million websites integrate in some way with Facebook, and 55 percent of the top 400 Apps for Iphones / Ipads are linked through Facebook. 25 percent of Facebook users do not bother with any privacy settings.

- LinkedIn. This social networking program geared toward business connections. It has about 74 million users in the United States

- YouTube. There are more than 1 billion unique users visit to YouTube each month. Over 4 billion hours of video are watched each month on YouTube. 72 hours of video are uploaded to YouTube every minute. In 2011, YouTube surpassed 1 trillion views per year.

- Twitter. The world in 140 characters at a time. As of September 2012, there were over 500,000,000 registered Twitter users. In early 2013, more than 400 million tweets were being posted per day, and since its inception, over 163 billion tweets have been posted.

- Instagram. This is a social networking and photo sharing website that has exploded on the Internet. In two years it has gone from startup to 100 million monthly users. Anecdotal evidence is that among younger users, Instagram and Twitter are outpacing Facebook in popularity.

- Pinterest. Latest hot thing in social networking. It is a photo-sharing website largely regarded as the "soccer mom's social network." 80 percent of Pinterest users are women. Average Pinterest user has over $100,000.00 in income.

- MySpace. Once the dominant social networking site, it is now regarded as outdated by most except for music-related users.

- WayBackMachine.org. Stores old versions of websites so that one can see what websites looked like on previous dates.

- "The Cloud." The biggest change in computer technology over the past several years appears to be "the Cloud." Spurred in part by the Ipad and tablet computing, more and more data is stored and manipulated "in the Cloud." The data no longer resides on an office computer or even a laptop. Rather, it is stored in the 'ether-sphere', maintained by third party providers in a nameless location, accessed only when needed through Internet connections.

III. General Rules of Evidentiary Foundations and Admissibility of Electronic Evidence

There are no special rules for the foundation and admissibility of social media and other electronic evidence. As with nearly all evidence, the fundamental test for establishing the necessary foundation is set out in Evidence Rule 901.

Under Rule 901, the proponent of the exhibit must present "evidence sufficient to support a finding that the matter in question is what its proponent claims."

When offered simply to prove what appeared on a website, testimony may be rather simple. A print out of a website or post may be identified by a witness, who testifies that the print out accurately depicts the website, text message or social media post that the witness observed. This is similar to the method used for authenticating a photograph.

But the issue becomes more difficult when the proponent seeks to attribute the exhibit to the defendant. Courts seem to take a totality of the circumstances when the effort is made to attribute web content to a specific person - such as attributing statements on Facebook to the defendant.

This can be done in three basic ways.

First is through the testimony of the person who made the entry. This is the easiest method when one has a cooperative witness. But all too often the purported author is either uncooperative or unavailable.

Second is the testimony of experts linking the post or message to the defendant through computer forensics. This can be done by obtaining information on IP Addresses and other technical information that can be analyzed by an forensic computer expert. This may entail examining the metadata in posted documents, examining computers and hard drives, or obtaining business records from internet service providers, cell phone carriers, or directly from social media websites such as Facebook.

Two rules can become particularly important in using expert testimony regarding electronic evidence. Indiana judges are being instructed about the interplay between these two rules and the admissibility of the underlying basis of expert opinions.

Rule 703 provides that experts may testify as to opinions based upon otherwise inadmissible evidence if "it is of the type reasonably relied upon by experts in the field." (Evid. Rule 703). In this way, a lawyer may have an expert testify as to his opinion linking a party to a particular Internet message or post even though the necessary foundation for admissibility of the documents upon which he relied had not been established. See *Mills v. Berrios*, 851 N.E.2d 1066 (Ind.App. 2006); *Prewitt v. State*, 819 N.E.2d 393 (Ind.App. 2004)

This does not automatically mean that the underlying documents or data relied upon by the expert are admissible. Nothing in Rule 703 makes the otherwise inadmissible documents or data admissible simply because the expert relied upon them.

Rule 705 provides that the expert may be compelled on cross-examination to disclose the underlying data or facts upon which he relied, even though it would be otherwise inadmissible. It appears that only on cross-examination does the underlying "inadmissible" data relied upon by the witness become admissible as the cross-examiner challenges the basis of the expert's opinion. The lack of supporting facts and data goes to the weight of the evidence, not its admissibility. See *Vaughn v. Daniels Co. Inc.*, 777 N.E.2d 1110 (Ind.App. 2002)

A second less technical, and often less expensive method of establishing a foundation for social media evidence, is to analyze the circumstances and content of the posting. Pursuant to Evidence Rule 904(b)(4), authentication may be made by distinctive characteristics in a document such as ""appearance, contents, substance, internal patterns, or other instinctive characteristics, taken in conjunction with circumstances."

Circumstances that support admissibility may be shown on a simple printout of a webpage, or other related circumstances. This may include username, photo and other identification information shown on the profile page, whether access is password protected, whether the person shared (or did not share) his password with others; whether the content shows a continuity that is consistent with the user posting the information in question; whether the posting contains information available only to the user.

The Maryland case of *Griffin v. State* 995 A.2d 791 (Md.App. 2010), cert granted, 4 A.3d 513 (2010) provides an example of how non-expert testimony can be found sufficient to admit social media. A posting from the MySpace page of the defendant's girlfriend was offered as corroborating evidence that the prosecution's witness was threatened by the defendant.

The MySpace post stated: "Free Boozy! Just remember snitches get stitches! U know who you are!"

The officer who printed off the MySpace page testified that he went to the girlfriend's MySpace page, which included her photograph and personal identification information. The MySpace page contained information that the officer knew correctly identified the girlfriend, including that she lived with the defendant and had two children. It also referred to "Boozy," which the police knew from interviewing the girlfriend, was her "pet" name for him. On cross the officer admitted that he did not personally know that the girlfriend posted the statement, nor did he know when the statement was posted.

The defendant objected on the basis that the prosecution did not sufficiently authenticate the offered MySpace page. The court overruled the objection, and the appellate court affirmed. The court noted the generally liberal standard applied for admissibility, and that the circumstances sufficiently authenticated that the exhibit was what it purported to be.

However, there is not unanimous agreement on this approach. In *State v. Eleck*, 23 A.3d 818 (Conn.App. 2011), the Connecticut Court of Appeals denied admission of a Facebook page offered by a criminal defendant to impeach the testimony of a key prosecution witness, finding that merely identifying the printout of the page with the identification information present on the page was not an adequate foundation.

In that case, the witness testified that her Facebook account had been hacked, her password changed, and that she had no access to her Facebook page during the time period when the message sought to be admitted was posted. But the Court's decision was not based on the claim of hacking, but rather on the lack of sufficient testimony to establish necessary authentication.

In denying admissibility to the Facebook page printout, the Court stated:

> "Because an electronic communication, such as a Facebook message, an e-mail or a cell phone text message, could be generated by someone other than the named sender. This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended. Additionally, passwords and website security are subject to compromise by hackers. Consequently, proving only that a message came from a particular account,

> without further authenticating evidence, has been held to be inadequate proof of authorship."

The Connecticut court recognized that this was a growing area in which no consensus has yet evolved. The court expressed its view that a "one size fits all" approach may not work, and that the circumstances needed to establish authenticity may vary as to each separate electronic media.

One of the best discussions of how to lay the foundation for electronic evidence, specifically information found on a cell phone, is set out in Ryan *Worline, v. State*, No. 49A02-1312-CR-1041(Ind.Ct.App., Aug. 28, 2014. Unfortunately this is a memorandum decision. Nevertheless, it sets out a roadmap for professionally and efficiently handling electronic evidence that can be used as a guide by law enforcement and attorneys in both criminal and civil cases.

Worline was convicted of murder. Photos, videos and text messages found on his cell phone were used to establish motive, and were upheld on appeal against a challenge of relevancy. But the important part of the decision is the detailed delineation of the foundation for admissibility established by the police officer who retrieved the information from Worline's phone. Because the details are important, that section of the opinion is set out below at some length.

> Here, the State presented testimony about how Worline's cell phone, an Apple iPhone, was seized from his home. Indianapolis Metropolitan Police Department Officer Brett Seach testified about his examination of Worline's cell phone and how the data, including the text messages, was downloaded from the cell phone. Officer Seach further testified to his extensive training and experience with various methods used to extract data from cell phones. This evidence was sufficient to show that the messages were from Worline's cell phone.
>
> Moreover, the background image on the home screen of Worline's cell phone was a picture of Taylor and Worline. The user generated device name was "ryan2." Tr. p. 601. The email accounts associated with that cell phone were "rdworline@aol.com," "rdworline@yahoo.com," and "rworline@me.com." Id. at 602. Included among the contacts portion of the cell phone was an entry for Taylor, which listed her phone number as ending in 8911. There also was contact information for Worline including (1) a picture of Worline, (2) email addresses rdworline@aol.com and rworline@me.com, (3) a link to Worline's Facebook account, (4) Worline's home address, and (5) a phone number ending in 1772, which was the same

> phone number associated with that iPhone. Additionally, the text messages themselves included information regarding Worline's and Taylor's children that was unique enough to establish Worline as the author of the messages. See Pavlovich, 6 N.E.3d at 979 (circumstantial evidence, including familiarity with and detailed knowledge about unique matters, was sufficient to authenticate authorship of text and email messages). . . . Taken all together, this evidence is more than sufficient to authenticate that Worline authored the text messages

Unpublished slip opinion at pp. 9-10.

IV. Alteration and Tampering

There is a concern among many about the possibility of altering electronic evidence. With the most rudimentary photo or text editing program, someone with even modest skills can remove a signature from a document, delete a paragraph from an email, or place opposing counsel on the grassy knoll in Dallas on November 22, 1963.

But in general courts seem to be admitting electronic evidence and allowing questions of alterations and accuracy to be addressed on cross-examination. See, J. Murphy and A. Fontecilla, *Social Media Evidence in Criminal Proceedings: An Uncertain Frontier,* Georgetown Law School Advance E-Discovery Institute (2012).

A leading case addressing this issue is *United States v. Safavian,* 435 F.Supp 2d 36 (D.D.C. 2006). This prosecution grew out of the Jack Abramoff influence peddling scandal in Washington, D.C. By pretrail motion the defendant sought to exclude emails on the grounds of the ease in which such electronic evidence may be altered. The District Court denied the motion. In doing so, the Court explained:

> [Email] may be altered, this trait is not specific to e-mail evidence. It can be true of any piece of documentary evidence, such as a letter, a contract or an invoice. Indeed, fraud trials frequently center on altered paper documentation, which, through the use of techniques such as photocopies, white-out, or wholesale forgery, easily can be altered. The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents).

> We live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world. The defendant is free to raise this issue with the jury and put on evidence that e-mails are capable of being altered before they are passed on. Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done. *The mere possibility of alteration is not sufficient to exclude electronic evidence as a matter of course; rather, there must be evidence of actual tampering.* (Emphasis added)

V. Admissibility and The "Other" Applicable Rules of Evidence

Lawyers dealing with social media and other electronic evidence must keep in mind that authentication is only one aspect of admissibility. Authentication is just the first hurdle. Just because a Facebook posting is properly authenticated does not mean it is admissible. Is it an admission? Is it a proper business record? Is it hearsay? Does its prejudicial impact outweigh its probative value?

This was well summarized in the leading case of *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D.Md. 2007), an insurance dispute over whether damage to a ship was caused by a lightning strike. In an oft-cited decision, Chief Magistrate Grimm noted that in modern litigation a great deal of effort and money is often spent on gathering electronic evidence. Yet despite this, there is a paucity of guidance on the admissibility of this electronic evidence.

Magistrate Grimm undertook an extensive analysis of the foundations and admissibility of electronic evidence that is now often cited by courts facing these issues. In doing so, he noted that electronic evidence "comes in multiple evidentiary 'flavors,' including e-mail, website ESI (electronically stored information), internet postings, digital photographs, and computer-generated documents and data files."

He then lumped all electronic evidence under the umbrella term of ESI, and addressed the extent of the evidentiary rules applicable to determining admissibility of electronic evidence. He wrote:

> "Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible.
>
> Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI relevant as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it authentic as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it hearsay as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an original or duplicate under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance."

The following is just a sample of the ways in which electronic evidence may be offered:

- An admission, *United States v. Safavian*, 425 F.Supp. 2d 36 (D.D.C. 2006), rev'd on other grounds, 528 F.3d 957 (D.C.Cir. 2008).

- Business record, *United States v. Ferber*, 966 F.Supp 90 (D.Mass 1997)

- Statement of present state of mind, *United States v. Joe*, 8 F.3d 1488 (10th Cir. 1993)

- Proof of motive or intent, *Brill v. Lante Corp*, 119 F.3d 1266 (4th Cir 1997).

- Self-authenticating evidence. See, *Williams v. Long*, 585 F.Supp 2d 679, 686-88 (D.Md 2006) (collecting cases that postings on government websites are inherently authentic or self-authenticating); See, *Ciampi v. City of Palo Alto*, 790 F.Supp.2d 1077 (N.D.Cal. 2011) (Printouts of newspaper website articles that included dates of publication, page numbers, and web addresses)

VI. Indiana Cases and Electronic Evidence

A Casemaker search reveals several hundred appellate cases that mention various social media. In most of these cases, the reference is in passing. But even those passing reference show the growing use of electronic evidence at trial. Only in a limited number of cases has a ruling on electronic evidence been made an issue on appeal.

One may speculate that some of the lack of challenges to electronic evidence may be due to the uncertainty lawyers may have to challenging the foundation and admissibility of electronic evidence. But that remains speculation. What is not speculation is that in more and more cases, emails, Facebook profiles, text messages, and photos posted on the Internet are becoming more common and more important in presenting cases before Indiana courts.

What follows is a summary of the Indiana cases that have addressed the issue of social media and electronic evidence, followed by brief summaries of cases (most unpublished) which show the broad range of of cases in which social media and electronic evidence is being used.

1. The Computer as Silent Witness - Laying a Foundation

***Bones v. State*,** 771 N.E.2d 710 (Ind.Ct.App. 2002). Bones took his computer to repair shop. When technician was checking it out after making repairs, he found images of child pornography. Technician called police, who after initial inspection obtained a warrant and had computer examined by state police officer trained in computers. When the warrant was served on Bones, his wife blurted out: "He promised me he wouldn't do that again!"

Bones challenged the admission of a CD and hard-copy images of the computer files and photos that were admitted at trial. The Court of Appeals relied upon Evid. Rule 901 which states that "the requirement of authentication . . . is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The Court held the images were sufficiently authenticated by the investigating detective who testified (1) about the nature and extent of his computer training, (2) that he removed the hard drive, made an image of it and "right protected" it on the floppy disks (now obsolete); (3) identified and described the software used in the process; (4) described how he generated the images offered from the files on Bone's computer; and (5) that the images exactly and accurately depicted the images on Bone's computer.

2. Text Messages On Phone Must Be Separately Authenticated

***Hape v. State*, 903 N.E.2d 977 (Ind.App. 2009).** Cell phone was admitted into evidence. During deliberations, the jury accessed text messages that were unknown to either prosecution or defense. Court held that the jury's view of the text messages was harmless, but stated that text messages are not made admissible simply by admission of the cell phone. The messages themselves are subject to separate authentication before their admission into evidence.

The Court of Appeals held that proper authentication is a condition precedent to the admission of evidence, citing *Bartlett v. State*, 711 N.E.2d 497, 502 (Ind. 1999). The Court summarized that "Writings and recordings must be authenticated pursuant to Indiana Evidence Rule 901(a) before being admitted. See *Bone v. State*, 771 N.E.2d 710, 716 (Ind.Ct.App. 2002) (reviewing whether data from defendant's computer was sufficiently authenticated)."

This applies to text messages that must likewise be authenticated. In addressing the specific issue of authenticating text messages, the Court stated:

> "The proponent of a piece of evidence has to decide the purpose for which the evidence is offered. Even though we have determined that a text message stored in a cellular telephone is intrinsic to the telephone, a proponent may offer the substance of the text message for an evidentiary purpose unique from the purpose served by the telephone itself. Rather, in such cases, the text message must be separately authenticated pursuant to Indiana Evidence Rule 901(a). See also *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 546 (D.Md.2007) (observing that federal courts have recognized Federal Rule of Evidence 901(b)(4) as a means to authenticate electronic data, including text messages); *Dickens v. State*, 175 Md.App. 231, 927 A.2d 32, 37 (2007) (reviewing whether text messages saved on a cellular telephone were properly authenticated); *State v. Taylor*, 178 N.C.App. 395, 632 S.E.2d 218, 230-31 (2006) (reviewing whether the State properly authenticated text messages).

3. MySpace Profile Page Admitted Regarding State of Mind

***Clark v. State*, 915 N.E.2d 126 (Ind. 2009)**. Conviction for brutal murder of child was affirmed. Court admitted Defendant's profile statement from his My Space account to counter the Defendant's defense that he was intoxicated and reckless, but did not have necessary intent for murder.

Clark's MySpace profile stated:

"Society labels me as an outlaw and criminal . . . To those people I say, if I can do it and get away. Bull sh** And with all my obstacles, why the f**k can't you."

The Defendant challenged the admission as improper evidence of prior bad acts under Evidence Rule 404 (b). The Court upheld admission of the MySpace page on the basis that the evidence was only of the Defendant's words and not prior acts. Further, the statements were relevant, as the Defendant himself had put the matter of his intent at issue by his own testimony.

4. Juvenile Delinquency and Criminalizing MySpace Posting:

A.B. v. State, 885 N.E.2d 1223 (Ind. 2008): A.B., a 14-year-old former student in the Greensburg School System was charged and adjudged a juvenile delinquent for postings on MySpace - postings which the prosecutor claimed and trial judge found would have been a Class B misdemeanor of harassment if committed by an adult.

The six asserted criminal acts consisted of postings about the Greensburg Middle School principal after A.B.'s friend was suspended for posting an online joke about the principal. Three of the items were posted on a private page in MySpace, and three were posted on a public page.

The Court of Appeals reversed on the basis that the statements were protected speech. Without engaging in any First Amendment analysis, the Supreme Court stated that it disagreed with this decision, but affirmed the reversal on other grounds.

The decision provided a glimpse into the world of middle school-aged "children" that is a far cry from the world of *Ozzie and Harriet*, and *Leave It to Beaver*.

Among the statements posted under the heading "F**k Mr. Gobert" were:

> "hey you piece of greencastle s* *t. what the f* *k do you think of me know (sic) that you cant [sic] control me? huh? ha ha ha guess what ill [sic] wear my f* *king piercings all day long and to school and you cant [sic] do s* *t about it.! ha ha f* *king ha! stupid b* *tard!"

and

> " [R.B.] made a harmless joke profile for Mr. Gobert. and [sic] some retarded b* *ch printed it out and took it to the office. [R.B.] is expelled, has to go to court, might have to go to girl [sic] school, and has to take the 8th grade over again! that's [sic] just from the school, her paretns [sic] have grounded her, and took [sic] her computer, she cant [sic] be online untill [sic] 2007! GMS is full of over reacting idiots!"

The Indiana Supreme Court in a unanimous opinion reversed the conviction, but did so on different grounds than the Court of Appeals. The opinion is particularly noteworthy for two points. First, the Supreme Court chastised the prosecution for its lack of understanding and lack of evidence about MySpace and how it functioned. Second, the Supreme Court admitted that it took the extraordinary step of going outside the record to determine how MySpace worked.

The Court opened its opinion by stating:

> "As a preliminary matter, we note that the evidence presented at the fact-finding hearing was extremely sparse, uncertain, and equivocal regarding the operation and use of MySpace.com ("MySpace"), which is central to this case. Only two witnesses testified at the fact-finding hearing, the school principal and A.B.'s mother. No expert witnesses were called. Neither of the witnesses provided knowledgeable and reliable details about MySpace. The primary source of information about MySpace came from the testimony of the principal, whose "understanding [came] from talking to students and trying to go figure how to go about researching this." Tr. at 25. The principal testified: "I don't get on MySpace." Tr. at 36. The Commentary to Canon 3B of the Indiana Code of Judicial Conduct advises: "A judge must not independently investigate facts in a case and must consider only the evidence presented." Notwithstanding this directive, in order to facilitate understanding of the facts and application of relevant legal principles, this opinion includes information

> regarding the operation and use of MySpace from identified sources outside the trial record of this case. "

As to the private page posts, the Court held that they could not have been intended to come to the attention of Mr. Gobert since access was limited to those invited to join the page, therefore the evidence lacked a necessary element of the offense.

As to the public pages, the Court held that the evidence did not support that the evidence did not support that there was "no legitimate purpose" for the communication, another necessary element of the "crime."

5. Police cannot search text messages without warrant

***Kirk v. State*, 974 N.E.2d 1059 (Ind.App. 2012).** Police seized a cell phone during pat down of Kirk, who was suspected of drug dealing. After taking the phone from Kirk's pocket, the police officer clicked on text messages and flipped through them, finding several references to selling and buying marijuana.

At trial, the content of the text messages was allowed in evidence. On appeal, the conviction was reversed. The Court of Appeals held that police could not go rummaging through the contents of a seized cell phone without a warrant. The text messages must be subject to a search warrant. Without the warrant, the text messages were product of illegal search and therefore suppressed. Without the text messages, there was insufficient evidence of conspiracy to sell drugs.

Note: there was no discussion of the Electronic Communications Privacy Act, discussed earlier in this paper.

6. Judicial Discipline:

In re Bennington, ____ N.E. 3d _____, 18S00-1412-JD-733 (Ind. 2015), decided February 10, 2015. Muncie City Court Judge Dianna L Bennington was in a contentious relationship with the father of her children. Among other things, when the father posted a photo of himself and his girlfriend on a beach vacation, she posted a response stating: "Must be nice to take such an expensive trip but not pay your bills. Just sayin'." She left the post up for more than an hour before removing it.

The Supreme Court held that "the injudicious comment on J.W.'s Facebook page and public conduct below the standard expected from judges violated Rule 1.2

of the Code of Judicial Conduct." Bennington was removed removed from the bench and permanently prohibited from acting in any judicial capacity.

7. Miscellaneous Unpublished Opinions: The Scope of Using Social Media and Electronic Evidence

Custody / Visitation

B.M. v. M.M., 965 N.E.2d 772 (Ind.App. 2012) (Unpublished memorandum decision). Electronic evidence provided key evidence in changing custody from Mother to Father, and denying Mother's request to move to Texas with the Child.

Stepmother used fictional male identity of "Deezy" to "friend" Mother on both Yahoo and MySpace. During discussions, Mother disclosed numerous instances of outrageous conduct, including: (1) marriage and planned move to Texas because "I figure if I'm married there ain't sh*t they can do about it, u know"; (2) violent relationship with her husband, including beating of the Child -- "he tossed her around like rag doll n treated [her] like a Red Headed Step-Child ... slammed against the wall ... all kinds of sh*t!!" but bragging that Mother "jacked em in his jaw"; (3) drug use -- " Lortabs, Zanax, muscle relaxers . . . just to be able to handle da sh*t."; and (4) sending semi-nude photos by text messages to "Deezy".

Mother was apparently visibly shocked when the Guardian ad Litem advised her that "Deezy" was in fact the child's stepmother. Later at trial she claimed her Yahoo and MySpace accounts had been hacked.

Despite the critical nature of this evidence, there was no discussion of the foundation for admission nor any challenge on the basis that the account actually was hacked.

In re Paternity of M.F., **956 N.E.2d 1157 (Ind.App. 2011).** (Unpublished memorandum decision). Text messages between mother and father regarding visitation arrangements formed key to contempt proceedings. No challenge to admission of evidence.

Termination of Parental Rights:

J.H. v. Indiana Dept. of Child Services, 971 N.E.2d 216 (Ind.App. 2012). (Unpublished Memorandum Decision). Department of Child Services was not required to attempt to contact parents through Facebook in proceedings to terminate parental rights.

Child Abuse:

Hunt v. State, 973 N.E.2d 105 (Ind.App. 2012). Unpublished Memorandum Decision. Court affirmed conviction for battery on a child. Evidence included series of text messages between the defendant and the child's mother, including among them:

"What did [J.M.] do last night? Y did u whoop her butt"

[Reponse:] "Wut?"

"She bit me are you on drugs you forget I told you last night dont text me thanks bitch

" Hey yo bitch, you need to call me. I don't know what's going on but uh, you're really pissing me off because I whooped her ass because she bit me"

Injunction and Misappropriation of Trade Secrets:

Snyder v. Classic Restaurant Services, LLC, 29A02-1207-CT-592 (Ind.Ct.App. April 3, 2013). Snyder, while an employee of Classic, set up a competing business and used email from a fellow employee working in Classic's business office to obtain confidential information about Classic's customers and pricing. Court of Appeals affirmed injunction issued against Snyder preventing him from soliciting or doing business with any of Classic's customers.

Protective Order:

Andrews v. Ivie, 956 N.E.2d 720 (Ind.App. 2011). Facebook photos and text messages supported issuance of protective order. The Facebook evidence was not challenged.

Malone v. State, 870 N.E.2d 32 (Ind.App. 2007) (Unpublished memorandum decision). Text message from protected person to defendant did not serve as sufficient notice of issuance of protective order. There was no challenge to admission of the text message.

Slavin v. State, 972 N.E.2d 419 (Ind.App. 2012) (Unpublished memorandum decision). Defendant's own text messages were sufficient to show Defendant's knowledge of protective order.

Probation revocation:

Fugate v. State, 968 N.E.2d 874 (Ind.App. 2012) (Unpublished Memorandum decision). Defendant's actions in using his cell phone to set up a Facebook profile under a false name showed that he willfully violated the conditions of his probation and sought to conceal his actions. No challenge was made to the Facebook evidence. Revocation of probation was affirmed.

Intimidation:

Eberle v. State, 942 N.E.2d 848 (Ind.App. 2011) Conviction for intimidation, harassment and stalking affirmed, but remanded for sentence modification. Evidence of text messages including photos of erect penis, and texts stating:

"[Y]ou better watch your back";

"you don't know who you're messing with"

" I'm going to f* * * you up, b* * * * * "

Other statements were so vile that even using ellipses could not make them presentable in a public paper. The Defendant admitted to police that he called the victim, and cell phone records confirmed that he made the calls.

Noll v. State,* 950 N.E.2d 32 (Ind.App. 2011).** Text message that "" You will not f with Austin or I will begin mailing packages [of sexually explicit photos]," supported conviction for intimidation.

Sex Offender Registration

***Harris v. State,* (Ind.Ct.App. March 27, 2013) Cause No. 20A04-1204-CR-225.** Holding conviction for accessing Internet as a sex offender violated First Amendment, but upholding conviction for failure to register as a sex offender. My Space was accessed by probation officer and admitted in evidence without issue.

Child Molestation:

***Lynch v. State*, 978 N.E.2d 757 (Ind.App. 2012).** (Unpublished memorandum decision). Conviction for attempted child molestation affirmed. My Space communications between 12 year old and Defendant was found by

victim's mother, who reported it to police. Defendant admitted the MySpace page communications were his.

***Lashaway v. State*, 955 N.E.2d 262 (Ind.App. 2011)** (Unpublished memorandum decision). Text messages between defendant and victim were admitted in evidence in case of conspiracy to commit child molesting. The text message evidence was not challenged.

Scebbi v. State, 957 N.E.2d 219 (Ind.App. 2011) (Unpublished memorandum decision). Defendant used text messages to solicit 14-year-old for sex. Affirmed. No challenge to text message evidence.

Witness Intimidation:

***Bryant v. State*, 977 N.E.2d 31 (Ind.App. 2012)** (Unpublished memorandum decision). The Court of Appeals affirmed admission of text messages that threatened witness in burglary and assault case.

> "The text messages here indicated that they were from phone number 317-447-5310, and E.B. testified that Bryant used this number. E.B. also testified that she received text messages from Bryant, that she saved some of the text messages, and that State's Exhibits 20, 21, 22, 23, 24, and 25, which were photographs of the text messages, accurately showed the content of the text messages that Bryant sent her. Based upon the record, we conclude that the State established a foundation for admission of the text messages pursuant to Ind. Evidence Rule 901, and the court did not abuse its discretion in admitting the text messages."

Prejudice Outweighs Probative Value:

***Lainhart v. State,* 916 N.E.2d 924 (Ind.App. 2009)** (Unpublished memorandum decision) Text message of threats were excluded on basis that probative value of bias was outweighed by unfair prejudice. The Court noted the insufficiency of defense's offer of proof that failed to place the text message itself in the record.

> "We understand the difficulty in printing out messages from cell phones, but defense counsel could have taken a picture of the display or at the very least had the witness read the message aloud in court."

Probable Cause:

***Hurst v. State*, 938 N.E.2d 814 (Ind.App. 2010).** Text message to police from 11-year-old including photo of growing marijuana was sufficient to support probable cause for search warrant.

Unemployment Compensation:

***Plasky v. State*, 914 N.E.2d 866 (Ind.App. 2009).** (Unpublished memorandum decision). Employee fired for sending text message notices on 19 occasions that would not be at work despite being told employer's policy was that he must phone. Held: employee terminated for just cause.

Fritz-Lint v. Review Board of Indiana Department of Workforce Development, _____ N.E. 3d _____, 93A02-1404-EX-243 (Ind.App 2014) (Dec. 11, 2014). Racial "joke" email passed along to two co-workers was sufficient to show discharge for cause, even if Fritz-Lint was not the person who placed a paper copy on an African-American employee's desk. Held: employee terminated for just cause.

Appendix A: Selected Indiana Rules of Evidence

Rule 104. Preliminary Questions

(a) Questions of Admissibility Generally. Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the Court, subject to the provisions of subdivision (b). In making its determination, the Court is not bound by the Rules of Evidence, except those with respect to privileges. Where a determination of admissibility under this paragraph requires resolution of a question of fact, the question shall be resolved by the preponderance of the evidence.

(b) Relevancy Conditioned on Fact. When the relevancy of evidence depends upon the fulfillment of a condition of fact, the Court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition.

(c) Hearing of Jury. Hearings on the admissibility of confessions shall in all cases be conducted out of the presence and hearing of the jury. Hearings on other preliminary matters shall be so conducted when the interests of justice require, or when an accused is a witness and so requests.

(d) Testimony by Accused. The accused does not, by testifying upon a preliminary matter, become subject to cross-examination as to other issues in the case.

(e) Weight and Credibility. This rule does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility.

Rule 703. Bases of Opinion Testimony by Experts

The facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to the expert at or before the hearing. Experts may testify to opinions based on inadmissible evidence, provided that it is of the type reasonably relied upon by experts in the field.

Rule 705. Disclosure of Facts or Data Underlying Expert Opinion

The expert may testify in terms of opinion or inference and give reasons therefor without first testifying to the underlying facts or data, unless the

court requires otherwise. The expert may in any event be required to disclose the underlying facts or data on cross-examination.

Rule 901. Requirement of Authentication or Identification

(a) General Provision. The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

(b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

(1) *Testimony of witness with knowledge.* Testimony of a witness with knowledge that a matter is what it is claimed to be.

(2) *Nonexpert opinion on handwriting.* Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.

(3) *Comparison by trier or expert witness.* Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.

(4) *Distinctive characteristics and the like.* Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

(5) *Voice identification.* Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.

(6) *Telephone conversations.* Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (i) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (ii) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.

(7) *Public records or reports.* Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

(8) *Ancient documents or data compilation.* Evidence that a document or data compilation, in any form, (i) is in such condition as to create no suspicion concerning its authenticity, (ii) was in a place where it, if authentic, would likely be, and (iii) has been in existence 30 years or more at the time it is offered.

(9) *Process or system.* Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.
(10) *Methods provided by statute or rule.* Any method or authentication or identification provided by the Supreme Court of this State or by a statute or as provided by the Constitution of this State.

Appendix B: Obtaining information from Facebook

Information on Civil Subpoenas

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

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

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

If a user cannot access content because he or she disables or deleted his or her account, Facebook will, to the extent possible, restore access to allow the user to collect and produce the account's content. Facebook preserves user content only in response to a valid law enforcement request.

May I obtain any information about a user's account using a civil subpoena?

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

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

Does Facebook notify users prior to responding to subpoenas?

Facebook may notify users before responding to legal process as permitted by law.

When will I receive a response to my civil subpoena?

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

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

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

Information for Law Enforcement Authorities

These operational guidelines are for law enforcement officials seeking records from Facebook. For private party requests, including requests from civil litigants and criminal defendants, visit: facebook.com/help/?page=1057. Users seeking information on their own accounts can access Facebook's "Download Your Information" feature from their account settings. See facebook.com/help/?page=18830. This information may change at any time.

US Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under US law:

A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available.

A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.

A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.

We interpret the national security letter provision as applied to Facebook to require the production of only 2 categories of information: name and length of service.

International Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account. Further information can be found here: facebook.com/about/privacy/other.

Account Preservation

We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of formal legal process. You may expeditiously submit formal preservation requests through the Law Enforcement Online Request System at facebook.com/records, or by email, fax or mail as indicated below.

Emergency Requests

In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay, a law enforcement official may submit a request through the Law Enforcement Online Request System at facebook.com/records. Important note: We will not review or respond to messages sent to this email address by non-law enforcement officials. Users aware of an emergency situation should immediately and directly contact local law enforcement officials.

Child Safety Matters

We report all apparent instances of child exploitation appearing on our site from anywhere in the world to the National Center for Missing and Exploited Children (NCMEC), including content drawn to our attention by government

requests. NCMEC coordinates with the International Center for Missing and Exploited Children and law enforcement authorities from around the world. If a request relates to a child exploitation or safety matter, please specify those circumstances (and include relevant NCMEC report identifiers) in the request to ensure that we are able to address these matters expeditiously and effectively.

Data Retention and Availability

We will search for and disclose data that is specified with particularity in an appropriate form of legal process and which we are reasonably able to locate and retrieve. We do not retain data for law enforcement purposes unless we receive a valid preservation request before a user has deleted that content from our service.

Details about data and account deletion can be found in our Data Use Policy (facebook.com/policy.php), Statement of Rights and Responsibilities (facebook.com/terms.php), and Help Center (facebook.com/help/?faq=224562897555674).

Form of Requests

We will be unable to process overly broad or vague requests. All requests must identify requested records with particularity and include the following:

The name of the issuing authority, badge/ID number of responsible agent, email address from a law-enforcement domain, and direct contact phone number.

The email address, user ID number (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) or username (http://www.facebook.com/username) of the Facebook profile.

User Consent

If a law enforcement official is seeking information about a Facebook 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. For account content, such as messages, photos, videos and wall posts, users can access Facebook's "Download Your Information" feature from their account settings. See facebook.com/help/?page=18830. Users can also view recent IP addresses in their Account Settings under Security Settings/Active Sessions. Users do not have access to historical IP information without legal process.

Notification

Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other process establishing that notice is prohibited. Law enforcement officials may also request nondisclosure if notice would lead to risk of harm. If your data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.
Testimony

Facebook does not provide expert testimony support. In addition, Facebook records are self-authenticating pursuant to law and should not require the testimony of a records custodian. If a special form of certification is required, please attach it to your records request.

Cost Reimbursement

We may seek reimbursement for costs in responding to requests for information as provided by law. These fees apply on a per account basis. We may also charge additional fees for costs incurred in responding to unusual or burdensome requests.

We may waive these fees in matters investigating potential harm to children, Facebook and our users, and emergency requests.

Submission of Requests

Online

Law enforcement officials may use the Law Enforcement Online Request System at facebook.com/records for the submission, tracking and processing of requests.

Please note that a government-issued email address is required to access the Law Enforcement Online Request System. You may also submit requests by email or fax as indicated below.

Email

records@fb.com
Fax

United States: +1 650 472-8007

Mail

United States Mail Address: 1601 Willow Road, Menlo Park CA 94025
Attention: Facebook Security, Law Enforcement Response Team

Law enforcement officials who do not submit requests through the Law Enforcement Online Request System at facebook.com/records should expect longer response times.

Notes

Acceptance of legal process by any of these means is for convenience and does not waive any objections, including lack of jurisdiction or proper service.

We will not respond to correspondence sent by non-law enforcement officials to the addresses above.

Appendix C: Obtaining information from Twitter.

Twitter provides information for Law Enforcement to obtain tweets at https://support.twitter.com/articles/41949-guidelines-for-law-enforcement# However Twitter provides no meaningful information for civil subpoenas. Twitter has shown a propensity to fight subpoenas.

Guidelines for Law Enforcement

These guidelines are intended for law enforcement personnel seeking to request information about Twitter users.

What is Twitter?

Twitter is a real-time information network powered by people all around the world that lets users share and discover what's happening now. Users send 140-character messages through our website and mobile site, client applications, or any variety of third-party applications. For more information, you can also visit https://twitter.com/about.
For the latest on Twitter's features and functions please visit our Help Center.

What User Information Does Twitter Have?

User information is held by Twitter, Inc. in accordance with our Privacy Policy and Terms of Service. We require a subpoena, court order, or other valid legal process to disclose information about our users.
Most Twitter profile information is public, so anyone can see it. A Twitter profile contains a profile photo, header photo, background image, and status updates, called Tweets. In addition, the user has the option to fill out location, a URL, and a short "bio" section about themselves for display on their public profile. Please see our Privacy Policy for more information on the data we collect from users.

Does Twitter Have Access to User Photos or Videos?

Twitter provides photo hosting for some image uploads as well as a user's profile photo, header photo, and account background image; Twitter does not, however, provide hosting for videos, nor is Twitter the sole photo hosting provider for images that may appear on the Twitter service. More information can be found on our photo and video sharing pages.

Data Retention Information

Twitter retains different types of information for different time periods. Given Twitter's real-time nature, some information may only be stored for a very brief period of time. Information on our retention policies can be found in our Privacy Policy.

Preservation requests in accordance with applicable law must be signed, include the username and URL of the Twitter profile in question (e.g., @safety and https://twitter.com/safety), a **valid return email address**, and be sent on law enforcement letterhead. Requests may be sent via the methods described below.

Private Information Requires a Subpoena or Court Order

In accordance with our Privacy Policy and Terms of Service, non-public information about Twitter users is not released except as lawfully required by appropriate legal process such as a subpoena, court order, or other valid legal process.
Some information we store is automatically collected, while other information is provided at the user's discretion. Though we do store this information, it may not be accurate if the user has created a fake or anonymous profile. Twitter doesn't require email verification or identity authentication.

Requests for User Information

Twitter, Inc. is located in San Francisco, California and will only respond in compliance with U.S. law to valid legal process. For example, requests for contents of communication require a U.S. search warrant.

Emergency Requests

Twitter evaluates emergency disclosure requests on a case-by-case basis. If we receive information that gives us a good faith belief that there is an emergency involving the death or serious physical injury to a person, we may provide information necessary to prevent that harm, if we have it.

Requests From Non-U.S. Law Enforcement

U.S. law authorizes Twitter to respond to requests for user information from foreign law enforcement agencies that are issued via U.S. court either by way of a mutual legal assistance treaty or a letter rogatory. It is our policy to respond to such U.S. court ordered requests when properly served.

Will Twitter Notify Users of Requests for Account Information?

Yes. Twitter's policy is to notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order (e.g., an order under 18 U.S.C. § 2705(b)).

What Information Must Be Included?

When requesting user information, your request must include:

- The username and URL of the Twitter profile in question (e.g., @safety and https://twitter.com/safety);
- Details about what specific information is requested and its relationship to your investigation;
    - **Note**: Please ensure that the information you seek is not available from our public API. We are unable to process overly broad or vague requests.
- A **VALID EMAIL ADDRESS** so we may get back in touch with you upon receipt of your legal process.
-

How To Make an Emergency Request

If there is an emergency that involves the danger of death or serious physical injury to a person that Twitter may have information necessary to prevent, you may make an emergency disclosure request by email to lawenforcement@twitter.com (which we continuously monitor) with the subject: **Emergency Disclosure Request**. Please include **all** of the following information:

- Identify the person who is in danger of death or serious physical injury;
- The nature of the emergency (e.g., report of suicide, bomb threat);
- Twitter @username **and** URL (e.g., @safety and https://twitter.com/safety) of the subject account(s)) whose information is necessary to prevent the emergency;

- Any specific Tweets you would like us to review;
- The specific information requested and why that information is necessary to prevent the emergency; **and**
- All other available details or context regarding the particular circumstances.
-

NOTE: Our support system **removes all attachments**, you must include the contents in the body of the message; you will receive an automated response that you **must reply to** in order for us to see your request.
Alternatively, you may fax emergency requests to: 1-415-222-9958 (faxed requests *may* result in a delayed response; for the quickest turnaround, we **strongly suggest** emailing all emergency requests).

General Inquiries

Other general inquiries can be sent via email to: lawenforcement@twitter.com; you will receive an automated response that you must reply to in order for us to see your inquiry.
NOTE: We do **not** accept legal process via email; our support system removes all attachments.

Contact Information

You may fax Twitter, Inc., c/o Trust & Safety, at: 1-415-222-9958.
Our mailing address is:

Twitter, Inc.
c/o Trust & Safety
1355 Market Street
Suite 900
San Francisco, CA 94103
Receipt of correspondence by any of these means is for convenience only and does not waive any objections, including the lack of jurisdiction or proper service.

Only email from law enforcement domains will be accepted. All others will be disregarded. Non-law enforcement requests should be sent through our regular support methods (https://support.twitter.com).

Appendix D: Obtaining information from Google (including YouTube, Google+)

Google has no published guidelines for obtaining information from Google, including YouTube and Google +. Rather, Google takes the position that it will accept subpoenas only issued from the Santa Clara (California) Superior Court, or presumptively from the Federal Court located in the Northern District of California.

A subpoena to Google must be served on:

Google Custodian of Records
1600 Amphitheater Parkway,
Mountain View, CA 94043

NOTE: The Federal Electronic Communications Privacy Act (ECPA) provides that opened email stored remotely - that is, in the "Cloud" – and not on a computer's hard drive – can be accessed by the federal government without a warrant. Google complies with this interpretation of the law.

In 2012, federal and state authorities made 13,753 separate requests for information on 31,072 users. More than half of these requests were without warrants.

Google complied, providing access to data, including the content of emails sent or received through Gmail, as well as the name, Internet address, and telephone number of Gmail, YouTube, and other Google users.