SOCIAL MEDIA, SMART DEVICES, AND THEIR USE FOR TRIAL STRATEGIES

TEJ R. PARANJPE
Paranjpe & Mahadass, LLP

State Bar of Texas
33rd ANNUAL
ADVANCED PERSONAL INJURY
San Antonio - July 26-28, 2017
Dallas – August 2-4, 2017
Houston – September 6-8, 2017

CHAPTER 20

TEJ R. PARANJPE

P&M LAW
Paranjpe & Mahadass LLP
3701 Kirby Drive, Suite 530
Houston, TX 77098
832-667-7700
TParanjpe@pandmllp.com

EDUCATION

Widener University School of Law, Wilmington, DE
Juris Doctor, May 2009

University of Sussex, Brighton, UK
Bachelor of Film, Cinema, and Video Studies, May 2006

The University of Texas at Austin, Austin, TX
Bachelor of Arts, in Government and Film, May 2006

EXPERIENCE

Paranjpe & Mahadass LLP, Houston, TX
*Managing Partne*r. September 2012 – Present

- Manages litigation docket
- Represented clients in state and federal courts
- Designed, maintained, and adjusted firm's office operations and procedures

Mentlewski Paranjpe Law Group, Houston, TX
Partner. April 2010 – September 2012

- Assisted clients in legal issues including those involving corporate, commercial, securities and consumer law, sports, and entertainment
- Planned and developed firm's operating systems

Sullo & Sullo LLP, Houston, TX
Attorney. May 2010 – August 2012

- Led negotiations with Assistant District Attorneys regarding plea deals for defendant clients
- Served as lead defense counsel for over 100 trials to jury verdict

Pennsylvania Criminal Defense Clinic, Chester County, PA
Certified Legal Intern. 2009

- Represented indigent defendants in preliminary hearings, investigations, negotiations, trial preparations, and Mental Health Court reviews

PROFESSIONAL

Member of the State Bar of Texas, 2010 – Present

MEMBERSHIPS & AWARDS

Rising Star; SuperLawyers
2017

South Asian Bar Association of Houston
Member. 2011 – Present

Board Member. 2012 – Present
President. 2015 – 2016
President-Elect. 2014 – 2015; 2016-2017
Treasurer. 2012 – 2014

Houston Trial Lawyers Association
Member. 2014 – Present

Shunya Theatre
Member. 2013 – Present
Board Member. 2013 – Present
Legal Chair. 2013 – Present

SPEAKING ENGAGEMENTS

Texas Minority Council Program
"Social Media and Discovery"
Houston, TX
October 2015

"Social Media and Ethics"
Austin, TX
October 2014

SABA North America Convention
"So Much Fraud, So Little Time"
Houston, TX
May 2016

TABLE OF CONTENTS

SOCIAL MEDIA, SMART DEVICES, AND THEIR USE FOR TRIAL STRATEGIES

"Social media is reducing social barriers. It connects people on the strength of human values, not identities…"

-- Narendra Modi (Current Prime Minister of India)

"It has become appallingly obvious that our technology has exceeded our humanity…the human spirit must prevail over technology…"

-- Albert Einstein (Scientist)

I. INTRODUCTION

Interactions with technology have long resulted in a dichotomous view of its helpfulness and uses. In today's age, technology is not only used to provide significant insight into data and analytics, for everyday common uses, but it also provides a medium for all of society to reach out and interact socially and publicly without barriers. Social Media, in the form of Facebook, Twitter, Instagram, Snapchat, Vine, and hundreds of other platforms, permits users to directly link with friends and strangers about what is on their mind, what they are doing, and where they even are geographically at any point in time. Opportunities and dangers come alike. Smart devices, whether they are mobile technology and wearable devices like iPhones, Apple Watches, and Fitbits, or stationary products like the Amazon Echo, Google Voice, Nest Thermostats, provide a window for the user into usable statistics and immediately available data and connectivity.

From a legal perspective and a legal landscape, social media provides litigation attorneys, on either side of a case, an ample amount of evidence and insight into the parties involved. This article will delve into the background of how evidence like this is admissible, how to adequately seek its discovery, and how to properly use it during the course of litigation, all the way through trial. The article will also seek to provide some pitfalls of using social media and extremely important actions or omissions to avoid, such as inadvertent (or intentional) spoliation. Further, social media has opened new case theories, both civilly and criminally, as well as new legislation targeting dangerous issues such as cyberbullying and revenge porn.

This article will also delve into new strategies of using smart devices as evidence in trial. Two of the more prominent cases, which are extremely recent, specifically deal with the Amazon Echo and Fitbit. In regards to the Amazon Echo, the *Bates* murder trial sought to acquire data and records of the suspect's Amazon Echo and various other smart devices, in hopes of finding evidence to convict Bates.[1] The second case, involving Fitbit, featured the use of Fitbit data to counter rape allegations, and open the door for charges to be brought against the alleged rape victim for false charges of rape.[2] This article will provide a glimpse into how smart devices are being used for trial, the trends the courts are moving in for admissibility of the technology, and insight into how to use technology to your own advantage for trial purposes.

II. SOCIAL MEDIA

A. Statistics

The number of social media users increases every day. As of 2014, Facebook was reporting over 1.1 billion monthly "active" users. When considering the term "active", this data takes into account users that post pictures, comments, share posts, and "like" posts. Of those users, it is estimated over 699 million users post on average at least one time a day and over 350 million photographs are uploaded daily. On average, Facebook users post over 90 pieces of "content" (photographs, status updates, shares of articles, comments, "likes", and "check-ins", for example) per month. In terms of Twitter, since its inception in 2006, there have been over 170 billion "tweets" that have been made.

B. How Social Media is Used in the Context of Litigation

Social media sites are encouraging its users to record, *in writing*, their present impressions and mindsets, and to share with others what they are thinking or doing, and even where they are located at, at any given moment.[3] Social media is used in litigation for three main purposes: (1) to establish facts; (2) to refute facts; and (3) to prove or disprove damages. In establishing facts, social media can be used to get more information on the parties, find out what happened, when it happened, why someone performed a particular action, and even what a particular person's mindset was when the underlying incident occurred.[4] Furthermore, if someone is using mobile technology or a desktop computer, location services software on the device create a GPS tracker-

[1] Holly Howell *Is Evidence Gathered from "Smart" Devices the New Way to Catch Dumb Criminals?* American Journal of Trial Advocacy (January 24 2017)

[2] Nichole Chauriye *Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie* Catholic University Journal of Law and Technology Vol 24 Iss 2 Art. 9 (May 24 2016)

[3] Mariel Goetz *Social Media Evidence in Civil Litigation* Trial Evidence; American Bar Association Section of Litigation (2013).

[4] *Id.*

like signal, which provides the location of the user.[5] For refuting of facts, social media can be used to rebut the state of mind and health of a claimant, for impeachment purposes, or oppositely boost credibility.[6] Finally, social media provides significant weight in regards to damages. How someone posts, what they post, where they are when they post can all be used to prove or disprove a party's physical, emotional, or financial damages.[7]

C. Types of Cases

The use of social media for evidentiary purposes can be used in a plethora of practice areas, including family law, defamation, and personal injury. One relatively new area of law relying heavily on social media is cyber-bullying and revenge porn.

Revenge Porn

Revenge Porn is a fairly new phenomena which is nonconsensual pornography, defined as the distribution of sexually graphic images of individuals without their consent.[8] This includes both images originally obtained without consent (e.g. by using hidden cameras, hacking phones, or recording sexual assaults) as well as images consensually obtained within the context of an intimate relationship. Nonconsensual pornography transforms unwilling individuals into sexual entertainment for strangers. A vengeful ex-partner or opportunistic hacker can upload an explicit image of a victim to a website where thousands of people can view it, and then that image can be shared on and hundreds of other websites by other users.[9] In a matter of days, that image can dominate the first several pages of "hits" on the victim's name in a search engine, as well as be emailed or otherwise exhibited to the victim's family, employers, co-workers, and peers. In 2015, Texas Governor, Greg Abbott, signed Senate Bill 1135, the Relationship Privacy Act which created a new offense under the Texas Penal Code as well as a civil cause of action under the Texas Civil Practices & Remedies Code.[10]

The Texas Civil Practice & Remedies Code added, in September of 2015, §98B. This section specifically provides that "a defendant is liable to the person depicted in the intimate image or video if: (1) the defendant discloses material without depicted person's consent; (2) there was an expectation the material was private; (3) the disclosure causes harm to the depicted person; and (4) disclosure reveals the identity of the depicted person even if that disclosure is made from information from a third party." If the defendant is found liable, the court can award: (1) actual damages; (2) court costs; (3) reasonable attorney's fees; and (4) exemplary damages.[11] What is important to note is the availability of attorney's fees, which is generally not recoverable for tortious conduct causes of actions. However, even though these damages are provided, attorneys need to be wary of these cases and their expenses, unless taking them on for pro bono purposes, as the defendant is likely an individual from whom a judgment would be hard to collect. The cause of action under this section in the Texas Civil Practice & Remedies Code is cumulative with other remedies.[12] Injunctive relief is also available under this section, and can be up to $1,000.00 per willful violation, and $500.00 per unintentional violation.[13] These monetary amounts are per occurrence. Each view is regarded an occurrence. (E.g. if a revenge porn video has 100 views, this could be a total of $50,000.00 - $100,000.00 for all the violations).

The civil cause of action is broadly worded and is intended to be liberally construed and applied in order to achieve its purpose, but exempts internet service providers protected by the CDA's §230.[14] Accordingly, the Relationship Privacy Act grants Texas courts broad jurisdiction over defendants, giving jurisdiction over: (1) defendants who reside in Texas; (2) any defendant if the plaintiff-victim resides in Texas; (3) any defendant if the offending intimate visual material is stored on a server that is located in Texas, or; (4) any defendant if the material is available for view in Texas.[15] There is existing tension with Fifth Circuit case law on the second, third, and fourth of the jurisdictional criteria, however the arguments will be provided more creditability if evidence can show that the defendant targeted the revenge porn towards Texas.[16]

D. The Legal Landscape of Social Media

Social Media has become discoverable because ultimately the federal rules of civil procedure considered social networks and media to be electronically stored information ("ESI"). Under the Federal Rules of Civil Procedure, rules 26a and 34a, all

[5] David Isom *Getting to Where: Location Based Electronic Discovery in Criminal and Civil Litigation* Salt Lake City, Utah (2011).
[6] *Social Media Evidence in Civil Litigation* (2013).
[7] *Id.*
[8] *What is revenge porn?* Cyber Civil Rights Initiative http://www.cybercivilrights.org/faqs.
[9] Bill Montgomery *Fix Arizona's revenge-porn law* AZ Central (July 11 2015).
[10] https://www.legis.state.tx.us/tlodocs/84R/billtext/html/SB01135F.htm.
[11] Tex. Civ. Prac. & Rem. Code §98B.
[12] *Id.*
[13] *Id.*
[14] Tex. Civ. Prac & Rem. Code §98B.007.
[15] *Id. a*t 98B.006.
[16] *Revell v. Lidov* 317 F.3d 467 (5th Cir. 2002).

electronically stored information, not just paper documents, are subject to discovery.[17]

As such, the courts are still struggling to determine the trend on how to rule on and assign protocols to the discovery of social media. There are several issues to determine still, such as: (1) whether special authentication rules should govern social media evidence; (2) what the threshold showing of relevance must be before the discovery of social media data should be allowed, and (3) when the duty to preserve social media arises.

Some state courts suggest that a carte blanche discovery request for social media records is nothing more than a fishing expedition, requiring a threshold showing to be required. The social media sought needs to be "likely to be relevant to the case…often… by pointing to relevant material in the public portion of the user's account."[18] Granting carte blanche discovery of every litigant's social media records is tantamount to a costly, time consuming, fishing expedition which the courts ought not condone[19]. Should the courts condone this sort of discovery process, a slippery slope would be created. As a matter of judicial policy, such a fishing expedition is not a sufficient basis to open the flood gates of meandering thoughts or silly posting to be used to impeach a party in a simple assault or negligence action without any good cause to believe that any incriminating statement was ever made and publicized in the social media.[20]

Federally, however, the courts seem to be more lenient as to the ability to discovery social media evidence. The Federal Rules of Civil Procedure do not require a party to prove the existence of relevant material before requesting it. This approach would improperly shield from discovery the information of Facebook users who do not share any information publicly.[21]

What Exactly Is Discoverable on Social Media?

The rule of thumb when it comes to discoverable content is: "if you are in control of it, it is discoverable". The main component of discovery here is the issue of control over the social media content. The large question underneath all of that is: Who controls social networking information? In Texas, the person that has actual possession or the legal right to obtain documents, is the one who controls.[22] In other jurisdictions, however, a party must produce evidence if it has the practical ability to obtain the documents from another, irrespective of their legal entitlement to the documents.[23] In the 4th circuit, even if a party cannot fulfill their duty to preserve because they do not own or control the evidence, they still have an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence.[24] Regarding social media specifically, there are going to be several parties that have possession, custody, or control: (1) the actual individuals and users that create social networking accounts, establish their profiles and engage in social networking community; (2) corporations that create the content; (3) the internet service providers; (4) content providers; and (5) host services. In considering host services, there is some information, like metadata associated with files, that is only going to be available to the internet service provider and the host servicing company. The problem that is created here is that the creators of the account have no assurance that these companies will be preserving this type of information indefinitely. The only "controller" in the situation of metadata is going to be a hosting company. This sort of party, however, is not going to be the typical party in a dispute. Even further, such companies generally have confidentiality and contractual agreements in place with their customers, which would cause potential breaches.

Still, not everything is going to be discoverable. The mere hope that there might be something of relevance is not enough to justify the discovery. Courts are holding that in the event no threshold showing is required, that discovery should be tailored to specific time frames and subject matters in order to maximize the chance of obtaining discovery. This way, the courts will be less likely to view requests for social media discovery as unwarranted fishing expeditions.[25] A party seeking discovery must establish a factual predicate for the request by identifying relevant

[17] Fed. R. Civ. P. 26 and 34. *Note the advisory committee's notes in the federal rules included that the framers of the rules intended that the term "ESI" be given a broad interpretation. The framers wanted to insure a broad interpretation and thusly even deleted the terms "data compilation" from the rule in order to provide a broad scope of what is labeled as electronically stored information.

[18] *Keller v. Nat'l Famers Union Prop.* 2013 WL 27731 at 11 (D. Mont. Jan 2013).

[19] *Fawcett v. Altiteri* 960 NYS.2d 592, 597 (NY Sup. Ct. 2013).

[20] *Id*.

[21] *Giachetto v. Patchogue-Medford Union Free Sch. Dist.* 2013 WL 2897054, 4-5 note1 (E.D.N.Y 2013).

[22] "evidence may be considered with the possession, custody, or control of a party if the party has actual possession, custody, control or the legal right to obtain the documents on demand. *In re Kuntz* 124 S.W.3d 179, 181 (Tex. 2003).

[23] *Silvestri v. GMC* 271 F.3d 583 (4th Cir. 2001)

[24] *Id.*

[25] *In re Indeco Sales, Inc.* 2014 Tex. App. LEXIS 11859 (Tex. App.—Beaumont 2014, no pet.); *In re Christus Heal Southeast Texas d/b/a Christus St. Elizabeth Hospital* 167 S.W.3d 596 (Tex. App.—Beaumont 2005).

information on the social media accounts that contradict or conflict with [the opposing party's] claims.[26] However, an objection based on expectation of privacy, under the 4th amendment, is not going to be accepted by the courts.[27]

Applicability

Social Media still has to pass the same barriers as all other trial evidence, including relevance and authentication. In using this evidence, litigators should consider the use of lay and expert testimony about a social media user's motivations and behaviors, and whether the expert can help explain helpful or harmful evidence that is admitted. In the admission of social media discovery, two approaches have emerged: (1) the Maryland approach, and (2) the Texas approach. Under the Maryland approach there are three permissible methodologies for authenticating social media evidence; (1) the testimony of the creator; (2) documentation of the internet history or hard drive of the purported creator's computer; or (3) information obtained directly from the social networking site.[28] Unless the proponent can convince the trial judge that the social media post was not falsified or created by another user via one of these methods, the evidence will not be admitted and the jury cannot use it in their factual determination. The Texas approach has recently undergone some changes from the *Tienda* decision where it was provided that a proponent can authenticate social media evidence using any type of evidence so long as he or she can demonstrate to the trial judge that a jury could reasonably find that the proffered evidence is authentic.[29] On April 27, 2017 the 14th Court of Appeals ruled that as long as the social media evidence provides a present sense impression, then it will survive an objection for relevancy and hearsay.[30]

How Courts Should Weigh Social Media Evidence

The Courts are still trying to figure out the level of scrutiny to put social media evidence under, because of the relative ease of manipulation of data on the internet. Federally, out of the Second Circuit, some courts are suggesting a greater scrutiny test needs to be applied.[31] State-wide, there is a general trend occurring

[26] *Del Gallo v. City of New York* 43 Misc.3d 1235(A) at 6 (NY. Sup. Ct. 2014).

[27] "Overly simplistic approaches to social media erode protections of individual privacy and may lead to unfair results in civil litigation. Courts should move away from an overly narrow definition of privacy and should instead view privacy concerns on a spectrum. Privacy issues arise from the sheer scope and quantity of data available in a social media account, and unfettered access to this volume of detailed data, in the aggregate, may itself constitute a valid privacy concern." *In re Indeco Sales, Inc.*

The general rule is that a producing party's legitimate privacy or confidentiality concerns can be dealt with through an appropriate protective order but do not shield social media postings from disclosure. *EEOC v. Simply Storage Mgmt.* 270 FRD 430, 434 (SD Ind. 2010). Under *Romano v. Steelcase, Inc.* a New York state case, a plaintiff suffered an injury and claimed permanent injuries that limited her participation in certain activities and lessened her enjoyment of life. In that case, the defendant sough discovery of nonpublic portions of her Facebook and Myspace pages, claiming it would contradict her claims of injury. Plaintiff attempted to make a privacy objection which the court rejected. They found that the plaintiff could have no reasonable expectation of privacy in her participation of social media sites, because the very purpose of those sites is to share information with others. The sites' terms of use even provide that "private" content may become publicly available. *Romano v. Steelcase, Inc.* 907 N.Y.S.2d 650 (NY Sup. Ct. 2010).

There is a strong argument that storing such information on Facebook and making it accessible to others presents and even stronger case for production, at least as it concerns any privacy objection. It was the plaintiff who by their very own volition, created relevant communications and shared them with others. So, particularly in the instance in where a plaintiff is claiming physical and emotional injuries, permitting a party claiming such substantial damages for loss of enjoyment of life to hide behind the self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial. *Romano* at 655.

[28] *Griffin v. State* 19 A.3d 415 (Md. 2011).

[29] *Tienda v. State* 358 S.W.3d 633 (Tex. Crim. App. 2012).

[30] *Wilkinson v. State* 2017 Tex.App LEXIS 3808 (Tex. App.—Houston [14th Dist.] 2017).

[31] *US v. Vayner* 769 F.3d 125, 131 n. 5 (2nd Cir. 2014). In this case, the defendant was accused of transferring false identification documents. The primary evidence that was submitted by the state was testimony from a witness who said they had received the documents from the defendant through a particular email address and profile page that came from a Russian social networking website. The Russian site conveyed a variation on the defendant's name, a photo of the defendant, and two different places the defendant had allegedly worked at in the past. The district court found the document to be authentic and noted that the information was fair to assume was being provided by the defendant. There were no questions of authenticity of the documentation as to how it was coming off the Internet. The appellate court, the 2nd Circuit, reversed and found that the district court had abused its discretion in admitting the social media profile page. The 2nd Circuit found that the government had presented insufficient evidence that the page was what the government had claimed it to be – the defendant's profile page, as opposed to a random profile page on the internet that the defendant in actuality did not create or control himself. The court ultimately compared the page to a random flyer found on the street that happened to contain the

where courts find testimony from individuals who printed webpages in question to be insufficient to authenticate social media, on its own. "Anyone can put anything on the internet. No website is monitored for accuracy."[32]

From a Defense Attorney Perspective

Courts are allowing defendants to discovery *any* content that reveals Plaintiff's emotions or mental state, or content that refers to events that could reasonably be expected to show Plaintiff in a significant emotion or mental state. This would prove helpful to defendants when looking at what the plaintiff is demanding for any kind of damage: whether it be financial, physical, or mental.

From a Plaintiff's Perspective

Social media evidence is probably the most damaging to a plaintiff's case. There are ways to combat it, however. Emerging social science research is coming out regarding social media, and it may be necessary for plaintiff's attorneys to have experts ready to provide counter-affidavits or counter-opinions. Research exists that states that a litigant's internal sentiments do not necessarily manifest in observable form, and therefore emotionally damages or remorseful litigants would likely not post pictorial evidence of their true feelings on Facebook. Because social norms encourage taking photos of happy moments, individuals are unlikely to capture shameful, regrettable or lonely moments with the camera.[33] The fact that an individual may express some degree of joy, happiness, or sociability on certain occasions sheds little light on the issue of whether he or she is actually suffering emotional distress.[34] Further studies show that many users tend to exaggerate or lie on social media in order to portray themselves in a more favorable light.[35]

Smart Devices in Trial

Smart devices, and digital data in general, are being used more and more for evidentiary purposes through trial. When lacking objective witnesses, the data from these devices that are in our homes and on our person can provide and shine a significant light into a factual situation and scenario. But, the questions that the public, attorneys, and the courts are wrestling with is: to what extent is this data protected for privacy purposes; how much can it be trusted, and to what extent can we use this data before it truly is hearsay? This article and section will provide *some* insight into the different views, but there are ultimately no hard answers. What this article will focus on doing here is taking a look at how smart devices are currently being used in recent cases; discuss the concerns with those uses; and analyze the privacy issues that exist. We will then look at how this sort of data and evidence is admissible into courts, the trends courts are going towards with this sort of evidence, and finally how defendants and plaintiffs are using this data in a litigation context.

Although smart device owners' queries may function like a standard internet search, it is not made in a manner that the public is accustomed to. Something about being at home with the search process set up to feel like a conversation with a physical non-computer or phone seems to detach users from the reality that these conversations are just another form of internet searching. These devices, like the Echo, work by knowing where people are, what they are doing, and keeping logs of this activity in order to get a better understanding of the users' habits and preferences.[36] Although this does not seem as tangible as a Google search or a text message, these activity logs are the ESI that may be found within a device. It is therefore reasonable to believe, as these devices become more prevalent, that if ESI extracted from one of these devices is able to clear evidentiary hurdles, it will be admissible in a court of law.[37]

Smart Devices Being Used in Trial

Alexa and the Murder Trial

On November 22, 2015, Victor Collins was found drowned in his friend, James Andrew Bates', hot tub in Bentonville, Arkansas.[38] According to Bates' affidavit submitted into trial in the *State of Arkansas v. James Andrew Bates* he had slept through the night, after having invited his friends over to watch a college football game, and found Collins face down in the water when he woke up.[39] When the police arrived, they found evidence of a struggle, broken bottles, spots of blood around the hot tub, and the back patio was

---

defendant's Skype address and was purportedly written or authorized by him.

[32] *Moroccanoil Inc. v. Marc Anthony Cosmetics, Inc.* 2014 WL 5786253, at 7 (C.D. Cal. 2014).

[33] Kathryn R. Brown "*The Risks of Taking Facebook at Face Value: Why the Psychology of Social Networking Should Influence the Evidentiary Relevance of Facebook Photographs"* 14 Vand. J. Ent. & Tech. L. 357, 381-82 (2012).

[34] [34] *Giachuetto v. Patchogue-Medford Union Free Sch. Dist.* 2013 WL 2897054, 8 (E.D.N.Y 2013)

[35] Andrew Hough *"Why Women Constantly Lie about Life on Facebook*" Telegraph (London), Mar 12, 2013.

[36] Holly Howell *Is Evidence Gathered from "Smart" Devices the New Way to Catch Dumb Criminals?*

[37] *Id*.

[38] Andrew L. Rossow *Amazon Echo May Be Sending Its Sound Waves Into The Court Room As Our First 'Smart Witness'* The Huffington Post (Dec. 30, 2016).

[39] *Id*.

wet.[40] Bates had a number of smart devices in his home, ranging from an Amazon Echo, to a Nest Thermostat, and even a smart water meter. The smart water meter provided data to the police that between 1:00AM and 3:00AM over 140 gallons of water had been used.[41] This data was enough to provide probable cause to the police and arrest Bates. The interrogations, and statement from a witness there that evening, provided that there was music streaming from the Amazon Echo that night. The prosecutors then wanted to see if the Echo recorded anything and if they could ultimately hear sounds of a fight or scuffle. Amazon was subpoenaed for its records.[42] The Amazon Echo is always on, and it works passively, always listening with its seven integrated microphones.[43] However, there is no active recording until the trigger word, "Alexa" or "Amazon", is said. At that point, data is then recorded for 20 seconds before the trigger word was heard and for 20 seconds after the user has stopped speaking.[44]

The case is ongoing, and the police have seized the Echo from Bates' home. They are hoping to find any searches that Bates may have performed that would correspond to the events of the evening, in an effort to see if they could paint a better picture of what happened that night.[45] The question is whether sounds were recorded, or if the Echo had been connected to Bates' alarm or lights – at what point any other connected devices were turned on, off, and used.[46]

The Fitbit disproves Rape Allegations?

In March 2015, Jeannine Risley claimed that an intruder had raped her in her sleep.[47] That night, when police arrived, they found overturned furniture, a knife, and a bottle of vodka.[48] Risley informed the police that an unknown man had pulled her out of bed, attacked her in a bathroom and then raped her at knifepoint.[49] She stated she had been sleeping and the was woken up around midnight and sexually assaulted by a man in his 30s wearing boots.[50] At first, she claimed she had been wearing her Fitbit band at the time of the attack, then later claimed she lost it during the assault[51]. The police found the device in the hallway next to the bathroom, and after examining it, the data retrieved from the device indicated she may have been walking around at the time of the attack.[52] The Commonwealth of Pennsylvania charged Risley for perjury and stated that the Fitbit proved she lied because it shows she had been awake and walking around the entire night and not sleeping, as she claimed.[53]

E. Concerns with using Smart Device Data for Litigation

There is concern that whether any given piece of ESI is admissible, or not,: (1) it is irresponsible for prosecutors to present evidence of a smart device user's changing of a habit or behavior as character evidence and (2) this would be a dangerous precedent because prosecutors and police could then simply "guess wrong".[54] The Federal Rules of Evidence have not changed or been amended to reflect the realities of the digital age, so there is currently no clear legal standard that governs law enforcement access to these smart devices.

Privacy

While these smart device manufacturers all have privacy policies, many of their policies seem to allow the corporations to share their users' data with third parties, if they so choose. Information could be collected by companies like Fitbit and Apple that is so detailed that it could enable companies to do everything from accurately guessing your credit rating to pricing an insurance premium[55]. The CIA has even gained notice of this, and have found the potential use of identifying an individual with 100% certainty based solely on their gait or how they walk.[56] Wearable

[40] Christopher Mele *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concern* The New York Times (Dec. 28, 2016).
[41] Amy B. Wang *Can Alexa Help Solve a Murder? Police Think So –But Amazon Won't Give Up Her Data* The Washington Post, note 24 (Dec 28, 2016).
[42] Amazon is not fully cooperating with the records request, and has filed briefs asserting first amendment protections to the information, likening this issue to when the FBI demanded Apple to turn over locked information from the San Bernadino killers' iPhones. CITE MORE.
[43] Jake Swearingen *Can an Amazon Echo Testify Against You?* New York Magazine (Dec 27 2016).
[44] *Id.*
[45] Ashley Carman *Police Want an Echo's Data to Prove a Murder Case, but How Much Does it Really Know?* The Verge (Dec. 27 2016).
[46] Billy Steele *Police Seek Amazon Echo Data in Murder Case* Engadget (Dec 27, 2016).
[47] Myles Snyder *Police: Woman's Fitness Watch Disproved Rape Report* ABC News (July 19 2015).
[48] Brett Hambright *Woman Staged 'rape' Scene with Knife, Vodka, Called 9-1-1, Police say* LancasterOnline (June 19, 2015).
[49] Snyder *supra* 47.
[50] Hambright *supra* 48.
[51] *Id.*
[52] *Id.*
[53] Snyder *supra* 47.
[54] *Lorraine v. Markel Am. Ins.* 247 F.R.D. 534 (D.MD. 2007); and Jill Bleed *Alex a Witness to Murder? Prosecutors Seek Amazon Echo Data* Yahoo Tech (Dec 29 2016).
[55] Justin Sedor *Fitbit, Nike & Jawbone Could Soon Be Selling Your Fitness Data* Refinery 29 (Jan 31 2014).
[56] *Id.*; and Chauriye *supra* 2

technology provides capability of functioning as a personal GPS. This sort of transparency in someone's personal activity can possibly violate their privacy rights as well as a Fifth Amendment right against compelled self-incrimination. Previous data, if the user hasn't opted out of default settings on their wearable devices, has resulted in disclosures like sexual activity, where a person has been, how long they have been active, and even possible health information.[57] For example, Fitbit's privacy policy merely provides that if they are requested to provide user info, they only have to do their "best" to inform the owner of the information request.[58]

FDA regulations currently do not apply to wearable technology.[59] However, these devices are sometimes recommended by physicians, and thus these wearable technology could then be considered a form of medical application that ought to fall under the FDA's purview.[60] If a wearable is subject to regulations, then it would be considered a medical device and any disclosure of information could then be a HIPAA violation. Thus far, however, HIPAA privacy rules haven't been applied to most information obtained by wearable technology because companies, like Fitbit, are not bound by the same confidentiality requirements as physicians.[61] Therefore, the data could "theoretically be made available for sale to marketers and released under subpoena in legal cases with fewer restraints".[62]

The debut of the Apple Watch in the fall of 2014 was a watershed moment not only in the tech industry, but also in the areas of privacy and health law.[63] The technology embedded in the watch and its competing devices effectively shifted health care from the physical to the remote, and in the process created a mechanism for the online collection of highly sensitive health information.[64]

The other side of the coin to all of this is, can there really be an issue of privacy with the court, if the user buys or wears the technology knowing that their information is shareable?

Flaws in technology

Even if all of this data from the wearable technology and smart devices is admissible in court, it is not guaranteed to be accurate or helpful. Fitbit, for example, can register the wearer as taking several steps, when in actuality the person was just driving their vehicle.[65] Fitbit admits that "Fitbit does not represent, warrant, or guarantee that its tracker can deliver the accuracy or sophistication of medical devices or clinical sleep monitoring equipment"[66] Fitbit does claim that the user can adjust settings to lower sensitivity levels which would solve most problems regarding inaccurate recordings.[67] However, if the wearer does not have the time to constantly monitor the accuracy of the recordings, which most people do not, then a Fitbit could continue to record inaccurate data[68]. A 2012 study showed that there was a high intra-device reliability and that the specificity of Fitbit to correctly and accurately identify the wearer's actions was poor.[69] However, despite the flaws, the wearable technology can at the base provide whether there was movement and even location. In the application to the *Risley* case, the Fitbit data showed that the watch was, at the least, moving around the apartment at certain times.

F. The Legal Landscape

Discovery and Admissibility

Physical items at the scene can pose a safety threat and have destruction possibilities that aren't present with digital evidence. Once you get in the digital works, you have the framers' concern of general warrants and the writ of assistance. Digital evidence may be obtained from any piece of technology that processes information that could be used in a criminal way. At its core, information that is stored electronically is said to be digital because it has been broken down into digits; binary units of ones (1) and zeroes (0), that are saved and retrieved using a set of instructions called software or code.[70] Digital evidence, therein, is divided in three separate categories: (1) internet based; (2) stand-alone computers and devices; or (3) mobile devices. Mobile devices have further been defined by Congress as a device that (A) is designed to be carried on the person of the user or to be

[57] Kashmir Hill *Fitbit Moves Quickly After Users' Sex Stats Exposed* Forbes (July 5 2011).
[58] *Privacy Policy* Fitbit http://fitbit.link/25itdKy
[59] Churiye *supra* 2; Karen H. Bromberg & Duance C. Cranston *Wearable Technology: Taking Privacy Issues to Heart* N.Y.L.J. 1, 2 (Mar 2 2015).
[60] Churiye *supra* 2, Colin Lecher *The FDA Doesn't Want to Regulate Wearables and Device Makers Want to Keep it That Way* The Verge (June 24, 2015).
[61] Ariana Eunjung Cha *Wearable Gadgets Portend Vast Health, Research and Privacy Consequences* Washington Post (May 17 2015).
[62] *Id.*
[63] Bromberg & Cranston *supra* 58.
[64] *Id.*
[65] Churiye *supra* 2; *Flex Counts Steps While Driving?* Reddit (Aug 5, 2014).
[66] Jeff Zalesin *Fitbit Buyers Step Up False Ad Claims Over Sleep-tracking* Law 360 (Aug 21 2015).
[67] *How Accurate is My Flex?* Fitbit http://fitbit.link/1VfThjs .
[68] Churiye *supra* 2.
[69] Hawley E. Montgomery-Downs et. al. *Movement Towards a Novel Activity Minoring Device* 16 Sleep & Breathing 913, 913-914 (2012).
[70] *National Forensic Sci. Tech. Ctr.* A Simplified Guide to Digital Evidence 1. (2009).

reasonably portable; (B) provides computing and communications functionality; and (C) is capable of providing access to commercial mobile service or commercial mobile data service.[71]

The discovery of this evidence is going to be very much in line with how to discover social media evidence, as noted earlier in this article. The admissibility will follow more of a federal standard, as this data is specifically regarded as digital data, and therefore is ESI. The admissibility of ESI is laid out in *Lorraine v. Markel Insurance*: (1) is the data relevant under Federal Rules of Evidence (FRE) 401; Is the data authentic under FRE 901; (3) is the data hearsay or subject to an exception under FRE 801-807; (4) is the form of data original or a duplicate under FRE 1001-1008; and (5) is the probative value of the data substantially outweighed by danger of unfair prejudice under FRE 403.[72]. From a criminal context, state courts have established that in order to obtain a warrant for smart devices and their data, the judge must be able to decide that given all of the circumstances set forth, there is a fair probability that contraband or evidence of a crime will be found in a particular place.[73] Further, the tests for relevancy and probative value mirror those set out in a federal standard.[74]

In a civil context, the production of ESI allows an objection to a discovery request if no form was specified or the party did not state the intended use.[75] Therefore, if a wearable smart device's ESI about a person is requested from opposing counsel, they would have to specify the reason for why they need the date or what they would intend to do with it.[76] For each item or category, the response must then either state that inspection and related activities will be permitted as requested, or state with specificity the grounds and reasons for objecting to the request.[77] If a specific form is not requested, then production must be done in the form the information is ordinarily maintained.[78] Since most smart device technology is stored on an owner's computer, printouts from one computer would be considered the form in which data would be ordinarily maintained. [79] When a specific form has not been identified, a specific but not over-intrusive form would have to be set as the form of delivery, or a screenshot of the evidence.[80]

However, using the standards set out by legislation, wearable technology and its data can fall within discoverable evidence. A Fitbit and Apple Watch are designed to be carried on the user, and both have the ability of either receiving texts or calls (Apple Watch) and are extensions of the mobile devices. The Amazon Echo, arguably, can fall underneath the congressional definition of a standalone device. For any of the devices, however, expert testimony will likely hold a significant amount of weight in the mind of a jury to supplement the evidence.

Trends in Court and with Attorneys

In 2014, a Canadian law firm represented a woman that was hurt in an accident. In order to represent the extent of her injuries, the attorneys used her Fitbit to measure her activity levels after the accident. The attorneys planned to use physical activity data from their client's Fitbit tracker at trial to show that her lifestyle had been severely impacted by her injuries. The results showed that because of her accident, her activity level was less than that of an average woman of her age and profession.[81]

Similarly, a case out of San Francisco involved attorneys obtaining data from a smart device technology, Strava. Strava tracks a person's runs, rides, and cross training and can then be uploaded to a person's phone in order to log all of their workouts. In this case, an individual was using the Strava app while he was cycling near Berkeley. The Strava app featured different challenges and goals in competition with other digital users. Apparently, in an effort to reclaim a "King of the Mountain" badge, the cyclist was on a particular route, gaining speed going down-hill, when he had an accident with a vehicle, resulting in his death. The Strava evidence was key in understanding the potential motivations behind the cyclist's actions in order to figure out whether any contributory fault went to the cyclist.[82]

This type of evidence can seemingly be used, in a civil case, from either a plaintiff or a defense side. Plaintiff attorneys can use this evidence to bolster proof of their client's injury, the damage, the future injury, and the loss of relative normalcy. Alternatively, and dangerously for plaintiff lawyers, is the use of this information by defense counsel. If defense counsel becomes aware of a client's use of smart devices for physical activity, it can open the door for significant query and analysis of true injury.

---

[71] H.R. 199 §343, 114th Congress (2015).
[72] *Lorraine v. Markel Am. Ins.* 241 F.R.D. 534 (D. Md 2007).
[73] *Commonwealth v. Hawkins* 701 A.2d 492, 507 (Pa. 1997).
[74] *Id.*
[75] Fed. R. Civ. P. 34b(2)(D).
[76] *Id.*
[77] Fed. R. Civ. P. 34b(2)(B).
[78] Fed R. Civ. P. 34b(2)(E)(ii).
[79] *Fitbug Ltd. v. Fitbit, Inc.* 78 F.Supp. 3d 1180, 1184 (N.D. Cal. 2015).
[80] *Id.;* and Churiye *supra* 2.
[81] Parmy Olson *Fitbit Data No Being Used in the Courtroom* FORBES (Nov 16, 2014).
[82] Kashmir Hill *A Quantified Self-Fatality? Family Says Cyclist's Death is Fault of Ride-Tracking Company Strava* FORBES (Jun 20, 2012).

III. CONCLUSION

The constant stream and new wave of technology and the expanse of social media can only grow over time. While the courts are struggling with these trending issues, we are seeing legislation and decisions start to provide some legal guidance into how the discovery of their evidence and admissibility will be dealt. As we are seeing new civil and criminal statutes be implemented in Texas, in response to growing social media concerns, we are bound to see changes to rules of evidence and considerations (or non-considerations) of privacy arguments when it comes to smart technology. As technology expands and social media becomes more accessible, access to information and data will only get easier. It will be difficult for this sort of evidence to be suppressed or withheld as time passes. Our roles as litigators will get even more complex as evidence of confirmation or rejection of legal claims becomes more abundant. Throughout this process, however, it will remain important to avoid issues with spoliation, and continue to rely on expert testimony to support our positions. One thing is certain, the exponential expansion of social media and the innovation of new technology is only going to increase, so it's vital the legal community and evidentiary rules keep pace.