COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas
March 2020

Table of Contents

Featured Articles

Short Circuits

CircuitBoards

Table of Contents

Feature Articles:-

Short Circuits:-

CircuitBoards:-

Letter from the Chair

By John G. Browning

Welcome to another edition of *Circuits*! The Computer & Technology Section remains one of the fastest growing sections in the State Bar, with over 2,020 active attorneys as of our most recent membership report. Our journal *Circuits* not only continues to bring you the latest in high quality, authoritative looks at cutting-edge topics in technology and the law, it is also making waves nationwide. *Circuits* articles have been reprinted with permission in a number of other publications, including the *Texas Bar Journal* and the *Computer and Internet Lawyer*. And *Circuit*'s fans among the judiciary include a Ninth Circuit justice. Our influence as a Section continues to grow as well, with the election of member Michael Smith of Marshall as the Mid-Section Representative to the State Bar Board of Directors. Congratulations Michael! In December, our annual "With Technology and Justice for All" CLE boasted record attendance.

If you ever needed a reminder about why it's so critical to stay on top of issues at the intersection of law and technology, you don't need to look any further than the headlines. Law firm cybersecurity remains a hot topic, whether you are a solo/small firm practitioner or a Big Law attorney. Before the end of 2019, more than 100 law firms had reported data breach incidents. In some of the most recent episodes of law firms falling prey to ransomware attacks, one law firm saw its attacker post the firm's confidential data and client files online – a nightmarish scenario. Attorneys' tech competence remains a vital issue, now that lawyers are being held to a higher standard. Don't wind up on the "Disciplinary Report" Section of the Texas Bar Journal like the lawyer who inadvertently sent a witness a link to her client's entire Dropbox, instead of one specific document – exposing the client's confidential information, including financial records and bank account information.

Our State Bar Annual Meeting is coming up in June in Dallas. Please try to join us at our annual membership meeting as we vote on a new slate of officers and council members. If you're interested in serving on the Section's Council, please get in touch with us soon. The Annual Meeting will feature some outstanding programming featuring section members, on a broad

range of cutting-edge law and technology subjects, including the popular Adaptable Lawyer Track.

John G. Browning
2019-2020 Chair
Computer & Technology Section
State Bar of Texas

Letter from the Editor

By Sanjeev Kumar

Welcome to the third issue of *Circuits* for the 2019-20 bar year! The pandemic caused by COVID-19 is wreaking havoc all across the globe. The situation will probably get worse before it improves. Please stay safe and take precautions to ride out this storm. The Computer and Technology Section has a lot of tools available to help it's members remain productive remotely in their practice. I hope all of you are taking advantage of some of those tools. We also have a council that is made up of some very accomplished individuals. If we can help in any way, please do not hesitate to contact us through our section administrator at admin@sbot.org.

Considering the shifting landscape of sales from brick and mortar stores to online platforms like Amazon and eBay, we open this issue with a timely article by our Section Chair John Browning and guest writer Grant Dubois discussing and analyzing the liability exposure of eCommerce sites for sale of defective products sold through their platform and websites.

Pierre Grosdidier (Past Editor and Council Member) resumes the topic of border searches from his previous article in the last *Circuits* issue, which discusses the raised bar for probable cause for search of digital content when crossing our borders. This raised bar was based on a recent decision by a district court on the matter.

Next, our former Section Chair Ron Chichester walks us through the intersection of criminal liability associated with revenge porn laws in Texas and artificial intelligence and how our criminal laws may be inadequate or difficult to apply when dealing with the new technological developments. This is a continuation of his article in the previous issue of *Circuits* regarding emerging legal issues due to artificial intelligence (AI) as related to Intellectual Property ownership due to AI.

We feature an article by a young law student and guest writer, Kirsten Kumar, reminding some of us lawyers who have forgotten the lessons learned in law schools. She shares her recently gained knowledge in regard to E-Discovery and how much of a person's social media may be discoverable.

A few years back there were numerous articles written about the texting of congressman Wiener's namesake. The problem was only getting worse and the State of Texas decided to do something about it. We start our *Short Circuits* section with a short article from our Council

Member, Gwendolyn Seale, in which she discusses the new Anti Cyber-Flashing law recently passed by the state legislator in September 2019.

In our next article in *Short Circuits*, yours truly provides an update on the status of the revenge porn law in Texas and what may still be coming. Texas legislators amended the law to overcome at least one ground cited by the 12th Court of Appeals in finding it unconstitutional due to a violation of the First Amendment free speech clause; however, the second ground is yet to be analyzed in the appeal pending the Criminal Court of Appeals.

In the last article in *Short Circuits*, Pierre Grosdidier discusses the limitations of digital border searches.

In our *Circuitboards* section, Council Member William Smith provides an update from Techshow 2020, in which he discusses Deepfakes as related to legal practice and provides an update on his findings related to marketing software and Customer Relationship Management (CRM) for lawyers.

Finally, for the last article of *Circuitboards*, Council Member Alex Shahrestani provides the recipe for creating our own electronic business cards to help automate our law practice.

Many thanks to all the contributors to this new issue and for helping us keep this publication on schedule. Thank you also to Antony P. Ng and Kirsten Kumar for their review of and assistance with this issue's articles. We hope that you enjoy this new edition of *Circuits* and as always, we welcome any comments that you may have. Please send them to our section administrator at admin@sbot.org.

Kind Regards,
Sanjeev Kumar, Editor

FEATURE ARTICLES:-

"Primed" for Liability? Product Liability Exposure for E-Commerce Platforms

By John G. Browning & Grant Dubois

If you have reveled in the sight of returning home and seeing packages from Amazon on your porch, you are hardly alone. In 2019, e-commerce sales accounted for 14.1% of all retail sales worldwide. And of the coveted 16-36 year-old demographic, 59% head to Amazon before any other e-commerce website.[1] By 2018, Amazon's share of the U.S. e-commerce market had reached 49%—more than its top three competitors (i.e., eBay – 6.6%; Apple – 3.9%; and Walmart – 3.7%) *combined*.[2] More than 50% of Amazon's sales come from third-party vendors, which has led to a question now actively being litigated and which threatens to irrevocably alter the landscape of online commerce: can an e-commerce platform be subject to strict product liability? Or, to put it even more bluntly, when a defective product purchased online injures a customer, who is the "seller" for strict liability purposes?

As the U.S. Supreme Court's decision in *South Dakota v. Wayfair, Inc.* demonstrated, courts have recognized the increasing importance of e-commerce and, at least as far as tax revenue is concerned, are more inclined to hold e-commerce giants accountable.[3] But until very recently, the "Good Samaritan" provision of the Communications Decency Act, U.S. Code § 230(c)(2)(A), has largely held sway nationwide when it comes to tort claims. This provision grants immunity to interactive computer service providers that act in good faith to "restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[4] Section 230(c)(2)(B) grants immunity to interactive computer service providers for "any action taken to enable or make available to information

---

1 Rikke Berg Thomsen, *19 E-Commerce Statistics You Can Use to Inform Your Marketing Strategy*, SLEEKNOTE.COM (Nov. 19, 2019), https://sleeknote.com/blog/e-commerce-statistics.

2 Emily Dayton, *10 Fascinating Amazon Statistics Sellers Need to Know in 2020*, BIGCOMMERCE.COM, https://www.bigcommerce.com/blog/amazon-statistics/#executive-summary-what-this-means-for-amazon-sellers (last visited Mar. 1, 2020).

3 S. Dakota v. Wayfair, Inc., 585 U.S. ____, 138 S. Ct. 2080 (2018).

4 47 U.S.C. § 230(c)(2)(A).

content providers or others the technical means to restrict access" to objectionable material under Section 230(c)(2)(A).[5]

Early on, courts were hesitant to impose tort liability on an online marketplace. In 2014, the U.S. Court of Appeals for the Seventh Circuit upheld the dismissal of negligence claims brought against Armslist—a kind of Craigslist for guns—by the family of a woman killed in 2011 by a stalker who purchased a gun from the website.[6] Alex Vesely argued that his sister Jitka was murdered by Demetry Smirnov after he illegally purchased a handgun that he found on Armslist.com, a site that facilitates sales of guns through private owners, through providing owners the opportunity to post classified advertisements. Vesely argued that online entities like Armslist should bear the same burden of screening potential buyers and sellers as brick and mortar stores would. But the court disagreed, holding that no special relationship existed between the parties and that the Oklahoma-based Armslist only enabled "consumers to use a legal service," but did not invite either the purchaser or the seller of the handgun to break the law.[7] As recently as last year, Armslist would again evade liability, when the Wisconsin Supreme Court held that Section 230 barred tort claims against the classified advertising website where an individual purchased what turned out to be a murder weapon from a private seller.[8] According to the court, any such tort claims treated the website as the publisher or speaker of the third-party content, and were therefore barred.

But is Amazon different than a website that merely serves as a conduit for advertising? After all, consider the role that Amazon provides as a marketplace not just for products sold directly by the online giant but those available on Amazon that are sold by third-party sellers as well. In many instances, Amazon performs many of the tasks that a seller, retailer, or distributor would, including:

- marketing, packaging, shipping, and warehousing the product;
- charging the purchaser's account;
- generating and sending receipts;
- imposing a hold on funds paid by buyers;
- placing its logo on shipping boxes and materials;
- guaranteeing timely delivery and condition of the product during transit; and

---

5 *Id.* § 230(c)(2)(B).

6 Vesely v. Armslist LLC, 762 F.3d 661 (7th Cir. 2014).

7 *Id.* at 666.

8 Daniel v. Armslist, LLC, 2019 WI 47 (Wis. Apr. 30, 2019).

- requiring all communications between buyer and seller to go through Amazon's messaging platform

On the other hand, Amazon does not design, manufacture, provide warranties for, create descriptions of, or name itself as the "seller" of the product.

Despite this blurring of traditional boundaries, courts throughout the country remained reluctant to impose strict product liability on Amazon, holding that either it was not a "seller" of a given product or that Section 230 shielded it from liability. In *McDonald v. LG Electronics USA, Inc.*, a rechargeable cellphone battery allegedly exploded in the buyer's pocket, setting him on fire.[9] The court rejected Amazon's Section 230 defense, reasoning that "to the extent that a plaintiff may prove that an interactive computer service played a direct role in tortious conduct—through its involvement in the sale or distribution of the defective product—Section 230 does not immunize defendants from all products liability claims."[10] However, the court went on to dismiss the claims against Amazon on the grounds that it was not the "seller," only a party that facilitated the transaction by enabling a third party (Safetymind) to sell and ship the batteries to the plaintiff.

Similarly, another federal district court in New Jersey declined to impose liability on Amazon as a "seller" in a case involving a defective laptop battery that caught fire, causing a home to burn down with the purchaser's cats inside.[11] And in a case involving a glass coffee pot that shattered, causing nerve damage to the consumer's thumb, a New York federal court also declined to impose product liability on Amazon as a "seller."[12] Other courts have relied less on whether or not Amazon is a "seller" under state product liability law, and instead relied on Section 230's immunizing of websites against civil liability, including product liability claims.[13]

Inevitably, some of Amazon's victories at the trial court level were challenged on appeal. In May 2019, the Fourth Circuit considered a case in which a buyer had purchased an LED battery-operated headlamp on Amazon from a third-party merchant (Dream Light), only to have it malfunction and cause a fire in the ultimate user's home.[14] The home insurer paid the $313,000 loss, and then brought a subrogation suit against Amazon as the purported seller of

---

[9] McDonald v. LG Electronics USA, Inc., 219 F.Supp.3d 533 (D. Md. Nov. 10, 2016).
[10] *Id.* at 537.
[11] Allstate N.J. Ins. Co. v. Amazon.com, Inc., 2018 BL 261762 (D.N.J. July 24, 2018).
[12] Eberhart v. Amazon.com, Inc., 2018 BL 307257 (S.D.N.Y. Aug. 27, 2018).
[13] *See, e.g.*, Hinton v. Amazon.com, Inc., 72 F. Supp. 3d 685, 688–91 (S.D. Miss. 2014).
[14] Erie Ins. Co. v. Amazon.com, Inc., 925 F.3d 135 (4th Cir. 2019).

the headlamp. Although the lower court dismissed the case on Section 230 grounds, the Fourth Circuit disagreed. It rejected the premise that Erie's product liability claims were based on the publication of another's speech, holding that:

> There is no claim made based on the content of speech published by Amazon—such as a claim that Amazon had liability as the publisher of a misrepresentation of the product or of defamatory content. . . . While the Communications Decency Act protects interactive computer service providers from liability as a publisher of speech, it does not protect them from liability as the seller of a defective product.[15]

However, the court went on to rule in Amazon's favor since it was not a "seller" under Maryland law. As the court pointed out, sellers are "owners of personal property who transfer title to purchasers of that property for a price."[16] Amazon, the court observed, never takes title to the goods sold by marketplace vendors, even while it may hold those goods in inventory and perform fulfillment of the order. Instead, the court stated Dream Light did everything from setting the price for sale, designing the product description, paying Amazon for its fulfillment services, to ultimately receiving the purchase price. Amazon, the court held, functioned more like a broker or consignee. As the court opined, "Although Amazon's services were extensive in facilitating the sale, they are no more meaningful to the analysis than are the services provided by UPS Ground, which delivered the headlamp."[17]

Not long after the Fourth Circuit's decision in *Erie*, the Sixth Circuit weighed in. In *Fox v. Amazon.com, Inc.*, the court reconsidered the granting of summary judgement to Amazon in a case involving a Tennessee family of six injured and their home burned down when a defective battery in a hoverboard caused a fire.[18] The item had been bought in November 2015 as a Christmas present, and that same month Amazon conducted an investigation into hoverboard safety. By December, Amazon had decided that it would stop selling hoverboards globally, and on December 12, 2015, it emailed customers an "Important Product Safety Notification" regarding hoverboard orders, warning of the dangers of the product's lithium-ion batteries and providing an option to return the product. The trial court granted summary judgment for Amazon, holding that it wasn't the "seller" of the hoverboard and accordingly bore no product

---

[15] *Id.* at 139–40 (emphasis omitted).
[16] *Id.* at 141.
[17] *Id.* at 142.
[18] Fox v. Amazon.com, Inc., 930 F.3d 415 (6th Cir. 2019).

liability. The Sixth Circuit initially agreed, under the definition of a seller as "any individual . . . regularly engaged in exercising sufficient control over a product in connection with its sale, lease, or bailment, for livelihood or gain."[19] The court disagreed with the Fox family's portrayal of Amazon as a "seller" because it didn't "choose to offer the hoverboard for sale, did not set the price of the hoverboard, and did not make any representations about the safety or specifications of the hoverboard on its marketplace."[20]

However, the court felt that by sending its December 12 email to purchasers, Amazon had voluntarily assumed a duty to warn consumers. Because this raised a fact question about the Fox family's tort claims and whether they could have received and acted in reliance on such a warning, the summary judgment was reversed.

This was just one of several setbacks for Amazon during the summer of 2019. In July 2019, a federal court in Wisconsin considered another subrogation case against the e-commerce giant, this time involving a bathtub faucet adapter purchased by a homeowner from a third-party vendor on Amazon that malfunctioned and flooded the home.[21] State Farm paid the loss and sued Amazon for strict product liability. The trial court denied Amazon's motion for summary judgment, holding that Section 230 immunity did not apply since State Farm was not seeking to impose liability on Amazon merely because it posted some third party content. In addition, it held that unlike states that required a formal transfer of ownership to confer "seller" status under product liability theories, Wisconsin's strict liability laws were not so rigid. Noting that neither the unknown manufacturer of the adapter nor XMJ (the Chinese seller), were amenable to suit in Wisconsin, the court ruled that Wisconsin law would hold Amazon strictly liable. According to the court, Amazon was "a critical component of the chain of distribution, deeply involved in the transaction" and that "holding Amazon liable serves the purpose of the strict liability doctrine that Wisconsin courts embraced in 1967."[22] Moreover, the court held, there were public policy considerations to be weighed. It observed that

> Amazon has transformed retailing in the United States, and in the process it has taken on many roles that had been served by brick-and-mortar stores, shopping malls, and wholesalers and distributors. This has been a boom to consumers, because through Amazon consumers can purchase a vast range of products,

---

[19] *Id.* at 423.

[20] *Id.* at 425.

[21] State Farm Fire & Cas. Co. v. Amazon.com, Inc., 390 F. Supp. 3d 964 (W.D. Wisc. July 23, 2019).

[22] *Id.* at 973.

> supplied by manufacturers and sellers across the globe, that would otherwise not be available to Wisconsin buyers. But what recourse does a Wisconsin buyer have if one of these third-party products is defective and causes injury or damage?[23]

Perhaps bad news comes in threes, because the summer of 2019 also brought a setback for Amazon that garnered national attention for the seismic nature of its decision—the Third Circuit's initial ruling in *Oberdorf v. Amazon.com, Inc.*[24] Oberdorf sued Amazon in 2016 in federal court in Pennsylvania, claiming that she had been blinded in one eye when the retractable dog leash she purchased online snapped and recoiled, striking her in the face. The seller was a Nevada company called The Furry Gang, which shipped the leash directly to Oberdorf; it has not been active on Amazon's site since 2016, and the plaintiff could not locate it. The trial court granted summary judgment for Amazon, holding that it was not subject to strict product liability because Amazon was not a "seller" under Pennsylvania law. It also held that Oberdorf's remaining tort claims were barred by Amazon's immunity under Section 230.[25]

But on appeal, a three-judge panel of the Third Circuit reversed the lower court's dismissal of the product liability claim and also ruled that Oberdorf's claims were not barred by Section 230 except to the extent that they incorporated a "failure to warn" theory. The panel's majority applied a four factor test under Pennsylvania law that took into account such things as whether Amazon was "in a better position than the consumer to prevent the circulation of defective products" and whether it was the "only member of the marketing chain available to the injured plaintiff for redress."[26] The court distinguished other courts' holdings by finding that those rulings depended on interpretations of different states' product liability laws. The court held that under both Pennsylvania product liability law and § 402A of the Restatement (Second) of Torts, Amazon was a "seller." Amazon, the court opined, should not be allowed to evade liability because its business model "enables third party vendors to conceal themselves from the customer, leaving customers injured by defective products with no direct recourse to the third party vendor."[27]

It is not a stretch to say that the two-person majority's reasoning betrays a lack of understanding of some key underlying concepts of e-commerce. Although it reserves the right

---

[23] *Id.* at 974

[24] 930 F.3d 136 (3d Cir. 2019).

[25] Oberdorf v. Amazon.com, Inc., 295 F. Supp. 3d 496 (M.D. Pa. Dec. 21, 2017).

[26] *Oberdorf*, 930 F.3d 136 at 144.

[27] *Id.* at 145.

to remove sellers' listings or terminate marketplace services for any reason, Amazon's Conditions of Use also cautions that customers purchasing from third-party vendors are "purchasing directly from those third parties, not from Amazon" and that Amazon is "not responsible for examining or evaluating . . . the offerings of any of these businesses." Looking at Amazon's "substantial market control" and the existence of an indemnity provision in its vendor contract, the panel felt that Amazon could "distribute the cost of compensating for injuries resulting from defects" by simple "adjustment of rental terms," or taking a bigger share of its vendors' revenues.[28]

Not surprisingly, Amazon sought an *en* banc rehearing. That request was granted, and the panel's ruling was vacated; the *en* banc hearing took place on February 26, 2020. During argument, Chief Judge Brooks Smith noted that a bill pending before the Pennsylvania Senate would redefine a "product seller." And as Amazon (and the legal world) awaits the ruling of the Third Circuit en banc, it faces other product liability challenges. In April, the Ohio Supreme Court is set to hear oral argument in *Stiner v. Amazon.com, Inc.*, a case in which the plaintiffs are seeking to hold Amazon liable for the death of a teenager who purchased caffeine powder through an Amazon vendor.[29]

So what is the risk of business-breaking e-commerce vendor liability in Texas? It would appear to be fairly low, pending any shakeup in interpretations of Section 230 liability or Texas product liability law. As for Section 230's value as a shield for e-commerce vendors like Amazon, one need look no further than the Fifth Circuit's decision in *Doe v. MySpace, Inc.*[30] In that case, plaintiff argued that the online platform was obligated to implement certain safety measures to prevent sexual predators from communicating with minors online. The Fifth Circuit rejected plaintiff's claims, and in interpreting Section 230 regarded such a duty as "merely another way of claiming that MySpace was liable for publishing the [third-party] communications and they speak to MySpace's role as a publisher of online third-party-generated content."[31]

As for state product liability law, the Texas Products Liability Act defines a "seller" as "a person who is engaged in the business of distributing or otherwise placing, for any commercial purpose, in the stream of commerce for use or consumption a product or any component part

---

[28] *Id.* at 144.

[29] Stiner v. Amazon.com, Inc., 129 N.E.3d 461 (Oh. 2019).

[30] 528 F.3d 413 (5th Cir. 2008).

[31] *Id.* at 420.

thereof."[32] And while at first blush this might seem to encompass e-commerce platforms like Amazon's Marketplace, Texas also provides statutory indemnification for a seller, so long as the seller did not alter the product or act in any other negligent or intentional manner independent of simply introducing the product into the stream of commerce.[33] Of course, in a situation where the seller is insolvent or not subject to a Texas court's jurisdiction (much like the Chinese entities behind the bathtub faucet adapter in Wisconsin), Texas' product liability statute includes a caveat. Seller indemnity is not available under such circumstances, and so a deep pocket like Amazon faces potential exposure.

In the meantime, the evolving body of law on potential product liability exposure for online platforms like Amazon presents sobering issues. As multiple federal court decisions proliferate that turn on interpretation of what constitutes a "seller" under multiple and differing state product liability laws, do such results encourage forum shopping and the problems such practices entail? And if the public policy behind product liability law is to promote public safety by allocating injury costs to producers who are thus incentivized to invest in making and marketing safer products, then what public good is served by creating liability for a company like Amazon, an entity that, as one court observed, "lacks control over the product(s) at issue, making it, ultimately, unable to manage the risks posed by the allegedly defective product?"[34] Regardless of the outcome of the *en* banc rehearing in *Oberdorf*, online marketplaces may be well-advised to re-examine their e-commerce practices in general, including their third-party vendor contracts, oversight, and the extent of fulfillment activities. In addition, at a time when both the Department of Justice and large tech companies like Facebook are calling for an overhaul or even repeal of Section 230's broad immunizations against liability, e-commerce companies should gaze out over the landscape of decisions in the area and realize that when it comes to strict liability, such immunity may be broad (for now) but is not limitless.

---

[32] Tex. Civil Practices & Remedies Code, § 82.005, et seq.

[33] *See, e.g.*, Howard v. Lowe's Home Ctrs., LLC, 306 F. Supp. 3d 951 (W.D. Tex. Jan. 26, 2018).

[34] Allstate N.J. Ins. Co. v. Amazon.com, Inc., 2018 BL 261762, at 14 (D.N.J. July 24, 2018).

About the Authors

John G. Browning is an attorney in Dallas who litigates a wide variety of civil litigation in state and federal courts throughout Texas, including commercial disputes, personal injury and wrongful death defense, employment matters, health care, and intellectual property litigation. He is the author of the books The Lawyer's Guide to Social Networking, Understanding Social Media's Impact on the Law, (West 2010); the Social Media and Litigation Practice Guide (West 2014); Legal Ethics and Social Media: A Practitioner's Handbook (ABA Press 2017); and Cases & Materials on Social Media and the Law (forthcoming). Mr. Browning is also a contributing author to seven other books, the author of nearly 35 published law review articles; and the award-winning writer of numerous articles for regional and national legal publications. His work has been cited in nearly 350 law review articles, practice guides in 11 states, and by courts in Texas, California, Maryland, Tennessee, New York, Florida, Illinois, and Puerto Rico. He has been quoted as a leading authority on social media and the law by such publications as The New York Times, The Wall Street Journal, USA Today, Law 360, Time Magazine, The National Law Journal, the ABA Journal, WIRED Magazine and Inside Counsel Magazine, and he is a recurring legal commentator for the NBC, CBS, and FOX news stations in Dallas. He is an adjunct professor at SMU Dedman School of Law and he serves as the Chair of the Computer & Technology Section of the State Bar.

W. Grant DuBois is an attorney at Suzanne Calvert & Associates, Employees of the State Farm Mutual Automobile Insurance Company, and former Assistant District Attorney for the State of Texas. His practice is dedicated to analyzing complex issues for his clients while maintaining his "always ready for trial" approach to litigation. DuBois is dual-licensed in Texas and Arkansas, and enjoys spending time with his young family and analyzing issues evolving from technology and litigation. Any opinions expressed in this article are his alone, and do not necessarily reflect the views of State Farm or any of its officers, employees, agents, subsidiaries, or affiliates.

District Judge Raises the Bar for Digital Border Searches

By Pierre Grosdidier

A Massachusetts district judge has held that digital border searches require reasonable suspicion that the devices contain contraband, whether the search is basic or "advanced."[1] This decision runs directly contrary to *United States v. Touset*, an Eleventh Circuit Court of Appeals decision that addresses this very issue.[2] It also contradicts U.S. Customs and Border Protection ("CBP") policy, which allows basic searches without suspicion of criminal activity and advanced searches with reasonable suspicion of same.[3] But, the court also held that a "cursory search," consisting of a brief look to confirm a device's ownership, operability, and that it contains data, requires no suspicion.[4]

The facts in this case, as reported in the opinion and the pleadings, arguably give pause. The plaintiffs, ten U.S. citizens and one permanent resident, including several with middle eastern-sounding names, had their digital devices searched by CBP officers. Some plaintiffs had their devices searched more than once, and others after having filed suit. One plaintiff objected to having male CBP officers see pictures of her and her daughters without their headscarves, another of having officers read her attorney-client correspondence, and yet another expressed concern for his searched journalistic work product. In some cases, CBP officers seized the devices or retained copies thereof and added editorial comments in their own records. A CBP officer remarked to one plaintiff that a picture present during a prior search was no longer on the device.[5]

---

1 Alasaad v. Nielsen, No. 17-cv-11730, 2019 WL 5899371, at *1 (D. Mass. Nov. 12, 2019). For background reading on this topic, *see* Pierre Grosdidier, *Expect warrantless digital device searches at the border*, CIRCUITS at 16 (Sep. 2018). A basic search is performed manually, whereas an advanced or forensic search is performed with additional software and hardware.

2 890 F.3d 1227, at 1232-33 (11th Cir. 2018) (declining to conclude that any level of suspicion is constitutionally required for digital border searches, whether basic or advanced); *see also United States v. Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019) (holding manual digital border cell phone searches require no reasonable suspicion of criminal activity but forensic searches do). *Cano* is discussed below in this issue of *Circuits*.

3 CBP Directive No. 3340-049A, Border Search of Electronic Devices (Jan. 4, 2018). National security concerns also justify advanced searches; *see also* United States v. Cano, 934 F.3d 1002, 1007 (9th Cir. 2019) (same).

4 Alasaad, 2019 WL 5899371, at *13.

5 *Id.* at *2-3.

The plaintiffs sued and argued, *inter alia*, that the searches, whether basic or advanced, facially violated their Fourth Amendment constitutional rights "against unreasonable searches and seizures." The government, for its part, invoked the border search exception, which, the court reiterated, serves "the sovereign's interest in protecting the 'integrity of the border'" against contraband.[6]

The court held that the border search exception was not limitless and had to comply with the Fourth Amendment's reasonableness touchstone and the balancing of the intrusion into a person's privacy with the intrusion's necessity to promote legitimate government interests. In this case, the privacy interest was the device owner's interest in its contents. And, even though the balancing was heavily tipped in the government's favor at the border, the privacy interest in this case was considerable because searches of digital devices were particularly intrusive given the wealth of personal information that the devices contained.[7]

The court stressed that the border search exception merely applied to routine searches, not non-routine searches, and that the difference between the two turned on the "invasiveness or intrusiveness of the search."[8] The court acknowledged that most courts that have addressed the issue have held that digital border searches have required a showing of reasonable suspicion for at least advanced searches, given their intrusiveness. But, drawing from the reasoning in the U.S. Supreme Court's *Riley v. California* decision, the court concluded that it could find no "meaningful difference between basic and advanced searches" given the extensive amount of personal information that either search could reveal.[9] For this reason, it held that both type of searches were non-routine and required a showing of reasonable suspicion.[10] This showing required officers to "point to specific and articulable facts" that led them to reasonably suspect that a traveler's digital devices contain contraband.[11] Significantly, even though the "specific and articulable facts" test also reflects CBP policy, it is not as high a bar as the U.S. Supreme Court has required for ordinary police stops.[12] In *U.S. v Cortez*, the Court held that reasonable suspicion must be based on a "particularized and objective basis" considering "the totality of the circumstances" for suspecting that a person has been involved

---

6 *Id*. at *7-8 (citing U.S. Supreme Court cases).

7 *Id*. at *8, 11.

8 *Id*. at *10.

9 573 U.S. 373, 393 (2014) (ruling that authorities needed a warrant to search cell phones confiscated pursuant to an arrest given the abundance of highly private information involved).

10 Alasaad, 2019 WL 5899371, at *14.

11 *Id*. at *12, 15.

12 CBP Directive No. 3340-049A, at 5.

in criminal activity.[13] The Court added that "[t]erms like 'articulable reasons' and 'founded suspicion' [to authorize police stops] are not self-defining; they fall short of providing clear guidance dispositive of the myriad factual situations that arise."[14]

The court refuted the government's argument that digital border searches could uncover evidence of crimes or inconsistencies in the traveler's motive to visit the United States. It held that the interdiction of contraband, not the discovery of evidence of contraband, is the primary concern at the border.[15] Evidence of crime is the same at and inside the border and there seemed to be no reason why a search for evidence at the border was "so much stronger" that it justified the application of the border search exception. And, in the absence of metrics showing the success of digital border searches and the prevalence of digital contraband, such as child pornography, the claim that some searches have uncovered criminal evidence was not "a strong counterweight" to the corresponding privacy intrusion.[16] As to the contradictory reasons for traveling to the United States that a digital search might expose, the court observed that the plaintiffs were ten U.S. citizens and a permanent resident who were admissible as a matter of law after they had established their identity and citizenship.[17]

About the Author

Pierre Grosdidier is an attorney in Houston. He belongs to the first group of attorneys board-certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Secretary for 2019–20.

---

[13] 449 U.S. 411, 417–18 (1981).

[14] *Id.* at 417.

[15] Alasaad, 2019 WL 5899371, at *8.

[16] *Id.* at *9.

[17] *Id.* at *10.

Using AI to Avoid Liability for Revenge Porn

By Ronald L. Chichester

Introduction

In 2015, Texas adopted SB 1135,[1] which made the creation and promulgation of revenge porn illegal and imposed both civil and criminal penalties. This article will briefly describe revenge porn and how certain types of AI can be used to escape liability for that crime.

What is Revenge Porn?

A handy description of revenge porn is provided by Houston attorney Brett Podolsky, who summarizes revenge porn as:

> "In effect, revenge porn is categorized as any type of photo or video that is taken of a person in a sexual situation when those photos or videos are posted online without the subject's consent. In many cases, these images are **posted online by the ex-partners of the subject for the purpose of shame, humiliation or intimidation**. In fact, there are several websites that claim to specialize in revenge porn and invite people to post these images freely. Some websites even feature the names, social media pages, residences and jobs of the subjects who are posted there. Several of these websites have been shut down and their owners have been prosecuted."[2]

The effects of revenge porn are potentially devastating for the victim.[3] Indeed, it is the identification of the person depicted in the image/video *as* that person that is so damaging to the victim and the victim's friends and family.

The Texas Anti-Revenge Porn Statutes

On September 1, 2015, Texas SB 1135 became effective, with elements in both the Texas Civil Remedies & Practices Code[4] and the Texas Penal Code.[5] The relevant portion of the Penal Code starts at Section 21.16 and, *inter alia*, includes:

---

1 Texas Senate Bill 1135 (2015). The text of the bill is available at: https://www.capitol.state.tx.us/tlodocs/84R/billtext/pdf/SB01135F.pdf

2 Brett A. Podolsky, *Revenge Porn Laws in Texas* (Mar. 30, 2016), https://brettpodolsky.com/general-law/revenge-porn-laws-in-texas (last visited Feb. 16, 2020).

3 *See, e.g.,* Darieth Chisolm, *How revenge porn turns lives upside down*, TEDxPittsburgh, https://www.ted.com/talks/darieth_chisolm_how_revenge_porn_turns_lives_upside_down (last visited Feb. 18, 2020).

(b) A person commits an offense if:

(1) without the effective consent of the depicted person and with the intent to harm that person, the person discloses visual material depicting another person with the persons intimate parts exposed or engaged in sexual conduct;

(2) at the time of the disclosure, the person knows or has reason to believe that the visual material was obtained by the person or created under circumstances in which the depicted person had a reasonable expectation that the visual material would remain private;

(3) the disclosure of the visual material causes harm to the depicted person; and

(4) the disclosure of the visual material reveals the identity of the depicted person in any manner, including through:

(A) any accompanying or subsequent information or material related to the visual material; or

(B) information or material provided by a third party in response to the disclosure of the visual material.

Current case law regarding revenge porn laws in Texas and other states focuses on the constitutionality of the act under both the First Amendment and Section 230 of the Communications Decency Act.[6] The central focus of the law, however, is the element of "*depicting another person.*" In order for the harm to be done, there must be an identifiable victim. The difficulty for prosecutors, however, will be when the photograph or video is distorted only enough to make it hard for the judge and jury to recognize the victim in the image/video *as* the victim, but still recognizable by the victim and those close to the victim who can make the connection because they have known the victim far more intimately and for

---

4 Tex. Civ. Prac. & Rem. §§ 98B.001, *et. seq.*

5 Tex. Penal Code § 21.16 (2019).

6 *See, e.g.,* Ex Parte Tallion Kyle Taylor, 03-16-00689-CR (Tex. App. 2017) (defendant unsuccessfully argued that the revenge porn statute was unconstitutional, so a warrant that issued from same was invalid); GoDaddy.com, LLC v. Hollie Toups, 09-13-00285-CV (Tex. App. 2014) (Internet Service Provider argued that the revenge porn statute was barred by Section 230 of the Communications Decency Act); Ex Parte: Jordan Jones, 12-17-00346-CV (Tex. App. 2017) (Statement Regarding Oral Argument advocating a First Amendment argument against the constitutionality of Section 21.16); Neal Rauhauser v. James McGibney and ViaView, Inc., 02-14-00215-CV (Tex. App. 2014) (defendant filed a motion to dismiss on the claim that the legal action was in response to his exercise of free speech). Texas is not unique in this regard. California and other states have had similar cases with similar arguments.

far longer. This raises the question: is there software that can generate an image of a *fictitious* person, who thus does not have standing to sue the creator of that image/video?

How AI is Used to Generate Deepfakes

"Deepfakes are synthetic media in which a person in an existing image or video is replaced with someone else's likeness."[7] Deepfakes can include still images and whole movies.[8] For several years, people have taken the photographs of famous (or not-so-famous) individuals and incorporated those faces onto bodies performing sexual acts in an attempt to fool viewers into thinking that those individuals had been performing those acts. Those images are referred to as "fake porn."[9] It was only a matter of time before revenge porn was combined with deepfakes.[10]

Deepfakes are often generated (digitally) with a variety of techniques, the most popular being Generative Adversarial Networks ("GAN"). Two popular GANs are Nvidia's StyleGAN[11] and Deepmind's VQ-VAE-2[12] (by Google). This technology enables individuals to generate a *new* face from a set of other faces. Figure 1 illustrates the use of GANs to generate a face-to-face translation, the technique used make fake porn.

---

7 Wikipedia.org, Deepfake, https://en.wikipedia.org/wiki/Deepfake (last accessed Feb. 19, 2020).

8 *See, e.g., Robert Downey Jr. and Tom Holland in Back to the Future -This is heavy! [deepfake]*, YouTube, https://www.youtube.com/watch?v=8OJnkJqkyio (last visited Feb. 19, 2020).

9 *See, e.g.,* Noelle Martin, *Online predators spread fake porn of me. Here's how I fought back.*, TEDxPerth, https://www.ted.com/talks/noelle_martin_online_predators_spread_fake_porn_of_me_here_s_how_i_fought_back (last visited Feb. 18, 2020).

10 *See, e.g.,* Ian Morris, *Revenge 'Porn' Gets Even More Horrifying with Deepfakes*, Forbes (Feb. 5, 2018), https://www.forbes.com/sites/ianmorris/2018/02/05/fakeapp-allows-anyone-to-make-deepfake-porn-of-anyone/ (last visited Feb. 19, 2020).

11 Nvidia open-sourced the code used to make the StyleGenerator (called "StyleGAN") and posted it on GitHub. You can clone a copy of the source code and run it yourself at: https://github.com/NVlabs/stylegan.

12 *See, e.g., Going Beyond GAN? New DeepMind VAE Model Generates High Fidelity Human Faces*, Medium (June 6, 2019), https://medium.com/syncedreview/going-beyond-gan-new-deepmind-vae-model-generates-high-fidelity-human-faces-b1cc08fa4bbb. "In their NIPS 2017 paper *Neural Discrete Representation Learning,* DeepMind researchers introduced VQ-VAE, or Vector Quantised Variational AutoEncoder, a VAE variant that comprises an encoder that transforms image data into discrete rather than continuous latent variables (representations), and a decoder which reconstructs images from these variables." *Id.*

Figure 1, from a slide in a presentation by Taylor Brown of CoreLogic (February 18, 2020).[13]

GAN-based software can be used to generate completely fake images of people. In addition, and of particular note for this article, GANs can be used to generate a fake image of a person that *resembles* a victim of revenge porn. How close that resemblance is would be up to the person creating and selecting the GAN-generated images.

Figure 2 illustrates the types of images of fake people that can be generated by a GAN-enabled software application.

Figure 2. A set of *non*-real images generated by Nvidia StyleGAN[14]

[13] Taylor Brown, *Generative Models: Or How to Make Fake Pictures*, https://drive.google.com/file/d/1Qzl8wib-DL8kURKmdY-WbD-KJ4SrG6sH/view.

[14] This image was taken from the StyleGAN GitHub page, https://raw.githubusercontent.com/NVlabs/stylegan/master/stylegan-teaser.png (last visited Feb. 19, 2020).

With respect to revenge porn, however, it is not the generation of completely unique faces that is relevant. Rather, the GAN technology can be used to take, as a source, a photograph of a victim that would qualify as revenge porn under the Texas Penal Code, and then modify that picture successively to the point where only those individuals who know the victim well would be able to identify the victim. In other words, the AI-modified image would only be recognizable to the victim and the victim's friends (thus causing the harm) but would contain elements providing sufficient reasonable doubt to cause a jury to acquit the alleged perpetrator.

Worse, this technique can be automated. As Dallas-based attorney Joseph Jacobson observed, another technology (facial recognition[15]) could be used to trigger the GAN-based process to stop at the closest point where facial recognition software fails to verify the person depicted as the victim. Facial recognition has been used with mixed success in criminal trials.[16] However, this would be an instance where facial recognition would be used to *avoid* liability for a crime precisely because evidence from facial recognition software has been admissible and found probative in some cases.[17]

---

[15] Facial recognition is a technology that provides the capability to identify and verify the identity of a person from a photograph or video. Although there are several techniques for performing facial recognition, they all tend to select facial features of a person, and then match those features to the person identified in another photograph or video. *See, e.g.,* Wikipedia.org, Facial recognition system, https://en.wikipedia.org/wiki/Facial_recognition_system (last visited Feb. 19, 2020).

[16] *See, e.g.*, *A first: biometrics used to sentence criminal*, HOMELAND SECURITY NEWS WIRE (Feb. 1, 2011), http://www.homelandsecuritynewswire.com/first-biometrics-used-sentence-criminal (last visited Feb. 20, 2020); *Law Enforcement's Use of Facial Recognition Technology: Statement for the Record*, FEDERAL BUREAU OF INVESTIGATION (Mar. 22, 2017), https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology *But see,* Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, ELECTRONIC FRONTIER FOUNDATION (May 28, 2019), https://www.eff.org/wp/law-enforcement-use-face-recognition (last visited Feb. 20, 2020); Claire Reilly, *Facial-recognition software inaccurate in 98% of cases, report finds: Metropolitan Police in the UK have had sketchy results with crime-fighting tool*, C|NET (May 13, 2018) https://www.cnet.com/news/facial-recognition-software-inaccurate-in-98-of-metropolitan-police-cases-reports/ (last visited Feb. 20, 2020).

[17] See, e.g., Claire Reilly, Facial-recognition software inaccurate in 98% of cases, report finds: Metropolitan Police in the UK have had sketchy results with crime-fighting tool, C|NET (May 13, 2018) https://www.cnet.com/news/facial-recognition-software-inaccurate-in-98-of-metropolitan-police-cases-reports/ (last visited Feb. 20, 2020).

Conclusion

Artificial Intelligence is a technology that can provide many benefits to society. However, as with all technologies, AI can be used for nefarious ends. An AI technology known as Generative Adversarial Networks can be used for both good and bad ends. In particular, GANs can exacerbate problems in the prosecution of revenge porn cases in both civil and criminal courts.

About the Author

Ronald Chichester is a solo attorney in the Dallas area who specializes in computer-related legal areas, including artificial intelligence, blockchains, smart contracts, distributed autonomous organizations, data privacy & regulation, as well as all aspects of intellectual property. Ron is the Chair of the Blockchain and Virtual Currencies Committed of the Business Law Section of the Texas Bar, and is a past chair of both the Business Law Section and the Computer & Technology Section.

E-Discovery: How Much of a Person's Social Media is Discoverable?

By Kirsten Kumar

Introduction

Social media has become increasingly commonplace in our lives, so commonplace that at virtually any moment in time, we have instantaneous access to any number of social networking sites ("SNS"). Between the prevalence of smartphones and the Internet of Things, including wearable technology like smartwatches, we can post a photo of our morning coffee, send a Tweet complaining about traffic, and even go live on Facebook to prove it all within two minutes of our morning commute.

While the far-reaching presence of social media in our daily lives is far from a new topic, it has raised important questions in the E-Discovery world. E-Discovery, or Electronic Discovery, covers the identification, preservation, collection, review, and exchange of electronically stored information for the purpose of using such information as evidence.[1] A lawyer's mind may immediately jump to e-mail and productivity files like Microsoft Office documents when she hears the term "E-Discovery," but relevant, probative digital evidence may also reside in parties' social media accounts. For example, a video uploaded by a plaintiff of her black diamond run from a big ski trip last week would likely have some implications for her suit alleging severe back injury from a car wreck a month ago. Or, a WhatsApp conversation between two board members of a company discussing firing certain employees over the age of 50 would be highly relevant and probative in an employee's ADEA claim. This raises a question: is all SNS content thus discoverable?

What Qualifies As "Social Media"?

In order to determine what SNS content is discoverable, we must first determine what is included in and excluded from the parameters of "social media." What was once concentrated in a few platforms has now grown to encompass text- and photo-populated apps like Facebook, user-uploaded video portals like YouTube, and even platforms of ephemeral data, including web-based chat services like Slack and mobile applications like Snapchat. Social media comes in many forms, often including a combination of text, photos, memes,

---

[1] *The Basics of E-Discovery*, EXTERRO, INC. at 4 (2nd ed. 2018).

infographics, emojis, audio files, and videos.[2] Regardless, all social media has at least one characteristic in common: the sharing of information in either a targeted or broad fashion.[3]

Understanding Social Networking Sites

In the discovery process, counsel must first understand what type of content is sought from any given source. This requires knowledge of what the particular media type is (i.e. messaging platform, platform for sharing photos and videos, etc.) so that the request can be made with enough specificity. A request for all content from a user's Facebook account, for example, will be unlikely to go very far.[4] Further, counsel is unlikely to find favor with the court by claiming she was unfamiliar with the particular social media and thus had no choice but to rely on her client's claim that all relevant content had been produced.[5] Thus, lawyers are expected to reach a certain standard of competency with respect to social media platforms, either through individual study or associating with an expert.

Discovering Social Media Content: Relevance And Proportionality

In order for content from SNS to be discoverable, it must meet the same standard as any other evidence: it must be relevant and proportional to the needs of the case.[6] One district court has described it: "[p]ut simply, social media information is treated just as any other type of information would be in the discovery process."[7]

Similar to other types of discoverable information, requesting parties may not cast so broad a net as to receive access to all content in a user's social media account. Although some users may "over-share" on an SNS, choosing to publish information on one's social media account does not equate choosing to make such information public to the world, especially in the case of accounts where content is only shared with a user's "friends" or "followers."[8] One court has determined that the simple act of publishing information on an SNS or even communicating to

---

2 The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 3 (2019).

3 *Id.*

4 *See* Ye v. Cliff Viessman, Inc., No. 14-cv-01531, 2016 U.S. Dist. LEXIS 28882 (N.D. Ill. Mar. 7, 2016) (finding an E-Discovery request for Facebook archives "overbroad" because the request was not narrowly tailored to a reasonable time period and specific content relevant to the claim).

5 *See* Calvert v. Red Robin Int'l., Inc., No. C 11-03026, 2012 WL 1668980, at *19 (N.D. Cal. May 11, 2012) (declining to issue sanctions against counsel who was "unfamiliar" with the social media platform and instead waiting "to see if similar lapses" occurred in the future).

6 Fed. R. Civ. Pro. 26(b)(1).

7 Locke v. Swift Transp. Co. of Ariz., LLC, No. 5:18-CV-00119-TBR-LLK, 2019 U.S. Dist. LEXIS 17412, at *4-5 (W.D. Ky. Feb. 4, 2019).

8 *Id.* at *6.

another via an SNS does not automatically make such content, without regard to the subject matter, discoverable.[9] However, SNS content is generally "neither privileged nor protected by any right of privacy."[10]

Social media may be treated the same as other requests for discovery procedurally; however, relevance, proportionality, and burden often tend to cause disagreement between parties.[11] In theory, the relevance and proportionality requirements help narrow the scope of searching through large stores of content. In practice, however, it may be difficult to discern just what social media data is relevant and proportional to the needs of the case. Social media content may be relevant to ongoing litigation for the same reason that an email or text message would: many social media platforms allow for direct messaging between parties.[12] Additionally, SNS content may include geolocation data or evidence of a party's physical or mental state following an accident or event giving rise to a claim.[13] Finally, a major factor contributing to relevance of such content is subject matter. While discovery of social media content may still qualify as a "novel and evolving issue under federal law,"[14] some courts have spoken out against "fishing expeditions" into a party's social media account.[15] Rather, the *substance* of the communication determines relevance.[16]

According to the Sedona Conference Working Group, counsel should consider the following issues when initially reviewing social media evidence to request or preserve:

- which social media sources are likely to contain relevant information;
- who has possession, custody, or control of the social media data;
- the date range of discoverable social media content;
- what information is likely to be relevant;
- the value of that information relative to the needs of the case;
- the dynamic nature of the social media and user-generated content;

---

9 *Id.*

10 Davenport v. State Farm Mut. Auto. Ins. Co., No. 3:11-cv-632-J-JBT, 2012 U.S. Dist. LEXIS 20944, at *3 (M.D. Fla. Feb. 21, 2012).

11 The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 8 (2019).

12 Todd Heffner, *Demystifying Social Media Discovery*, The Daily Report, LEGALTECH NEWS (Aug. 30, 2019).

13 *Id.*

14 Locke v. Swift Transp. Co. of Ariz., LLC, No. 5:18-CV-00119-TBR-LLK, 2019 U.S. Dist. LEXIS 17412, at *4 (W.D. Ky. Feb. 4, 2019).

15 *Id.* at *7.

16 *See id.* at *4.

- reasonable preservation and production formats; and
- confidentiality and privacy concerns related to parties and non-parties.[17]

Privacy considerations play an important role in determining whether a party's request for SNS content is proportional to the needs of the case. Two factors implicate privacy concerns: "the importance of the discovery in resolving the issues, and whether the burden . . . of the proposed discovery outweighs its likely benefit."[18] Thus, privacy will often impact the perceived burden of discovery in the case of SNS content.

Discovering Social Media Content: Preservation and Collection

Preservation and collection of SNS content may pose particular issues for litigants. One unique characteristic of social media content is that it is typically dynamic, meaning a user, recipient, application host, or even the technology itself can easily modify or destroy the content.[19] Certain types of social media have additional unique issues. For example, counsel may have trouble identifying the source of anonymous application content or preserving and collecting content from ephemeral messaging applications and live-streamed videos.[20] Further, some content may be encrypted end-to-end.[21] Counsel should weigh such considerations carefully in considering the burden of production on a party and act promptly in instructing clients to preserve relevant social media content early in the litigation.

Discovering Social Media Content: Possession, Collection, and Control

Finally, counsel should be cognizant of the question of "control" in social media discovery. At the time of this article, courts have inconsistently dictated the meaning of "control" in this context.[22] While some have adopted broad definitions, applying a "practical ability" standard, others have adopted a more narrow "legal right" test.[23] Thus, counsel should consult any pertinent case law in her jurisdiction to proceed in an informed manner. Generally, though, the user controls the "vast majority" of the user-generated content from his or her social media account.[24] This same general rule also applies to organizations' SNS content.[25] However, when

---

[17] The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 8 (2019).
[18] Reid v. Ingerman Smith LLP, No. 2012-0307, 2012 WL 6720752, at *1.
[19] The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 3 (2019).
[20] *Id.* at 6.
[21] *Id.*
[22] *Id.* at 14.
[23] *Id.*
[24] The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 14 (2019).
[25] *Id.* at 16.

social media content is stored on an external website, efforts to obtain such evidence may be barred by the Stored Communications Act.[26]

Closing Thoughts

While social media content may not generally be subject to any privilege or privacy protection, it is still subject to ordinary discovery rules and regulations under the Federal Rules of Civil Procedure 26(b) and/or other pertinent jurisdictional rules. Thus, when litigators find themselves faced with the need to request production of content from SNS, they should be prepared to state their request with enough specificity to convince the court that such information will be relevant to the case at hand, likely to lead to further discovery of admissible evidence, and able to be produced without too much burden on the producing party. Further, producing parties should be equally prepared to state with specificity any objection to the production of requested information. Procedurally, SNS content may be no different than other electronic information requested during the discovery process. However, counsel must be prepared to get familiar with the platform, including its data, metadata and production forms, in order to successfully request or object to such content being produced.

About the Author

Kirsten Kumar is a second-year student at the University of Texas School of Law. Prior to law school, she was part of the technology community of Austin and worked in marketing for a local startup that was featured on ABC's Shark Tank. There, she created public-facing messaging, managed content marketing and assisted in producing content for the startup's pitch in SXSW's 2016 Accelerator Pitch Event, which it won.

Kirsten has a background in multimedia journalism, including digital photography, videography, and graphic design and has been published in various media, including lifestyle magazines and KUT Austin radio, an NPR affiliate. In addition to tech and IP, Kirsten has experience in immigration law and an interest in international humanitarian and human rights law, which she hopes to pursue upon completing her law degree.

[26] *Id.* at 23.

Being A Dick May Cost You: The Significance of Texas' New Anti Cyber-Flashing Law

By Gwendolyn Seale

If you are a woman who has participated in the online-dating world within the last decade, chances are you have received an unwanted photograph of male genitalia. According to a research study by Pew, 53 percent of women between the ages of 18-29 have received an unsolicited explicit image from a male;[1] a YouGov survey found that 78 percent of millennial women have received an unsolicited "dick pic."[2] Women receive these pictures through text messages, dating apps, and through social media communications. However, avoiding dating apps or social media does not necessarily guarantee immunity from these explicit pictures. New York subway riders have complained about the rash of inappropriate photographs they have received via AirDrop.[3] AirDrop is an Apple feature in which Mac, iPhone and iPad users can wirelessly send files to each other. With Airdrop, a sender does not need to have a recipient's phone number, be connected to the person on social media, or be accessing the same Wi-Fi network; rather, the sender is able to transmit materials to anyone who has an iPhone in a particular geographic vicinity. And while a recipient can decline such materials, a preview of the materials will show up on the user's phone, ultimately enabling the user to see an obscene photograph.

These troubling statistics have begged the question – if there are criminal penalties for indecent exposure in Texas, then why haven't similar punishments been implemented for flashing people through electronic communications? Until recently, about the only consequence a sender of such explicit material faced was a ban from dating or social media apps – an repercussion without real impact, given how simple it is to create a new account.

---

1 Jane Hu, *A Woman Frustrated by Unsolicited Dick Pics Decided to Make Her Own Filter*, SLATE (Sept. 10, 2019), https://slate.com/technology/2019/09/social-media-unsolicited-dick-pics-filter.html.

2 Yael Bame, *53% of millennial women have received a naked photo from a man*, YOUGOV. (Oct. 9, 2017), https://today.yougov.com/topics/lifestyle/articles-reports/2017/10/09/53-millennial-women-have-received-dick-pic.

3 Claire Valentine, *AirDropping Dick Pics Is the Newest Subway Harassment Trend*, SLATE (Aug. 14, 2017), https://www.papermag.com/airdropping-dick-pics-now-reality-subway-2472847586.html.

Texas proffered a solution to this issue, H.B. 2789, which went into effect in September 2019. This law punishes any person who knowingly transmits visual materials electronically that depicts "any person engaging in sexual conduct or with the person's intimate parts exposed."[4] Additionally, this law prohibits sending visual materials of a male's covered genitals that are "in a discernibly turgid state."[5] According to this law, the intent of the sender does not matter; rather, if the recipient does not request the photo or provide express consent, the sender can be held liable, facing a Class C misdemeanor and up to a $500 fine.

Texas is the first state in the nation to have introduced this specific law, and it has been met with both praise and cynicism. The cynics proffer the common motifs—whether women will follow through with the reporting processes, given the high percentage of those who never report being a victim of sexual assault or rape—or whether the police will follow through on reports even if women pursue reporting such crimes. A more serious problem relates to explicit images sent via AirDrop. While it may not be difficult to identify a sender of a message from a dating app, social media or a text message, identifying a cyber-flasher on AirDrop presents a host of difficulties, as a recipient can only see the "name" of a sender's device, which a sender can change at will.

Besides the practical problems that this law may have difficulties addressing, attorneys have raised legal questions in connection with the law. First Amendment experts have criticized the law for being overbroad and vague, arguing that posting breastfeeding photos, or sending doctors medical-related photographs technically violate this law when applying the law's plain wording to these examples. Such arguments are concerning, considering that the Relationship Privacy Act (the Texas revenge porn law) was declared constitutionally overbroad in April 2018 by the Texas 12th Court of Appeals in Tyler.[6] The Tyler Court of Appeals reasoned that because in today's world, sharing visual materials has become utterly habitual, the Act violated the free speech rights of third-parties by restraining speech more than the Constitution allows.[7] The case is still sitting before the Texas Court of Criminal Appeals; however, the Texas Senate passed a bill last year which attempts to mend the third-parties' right to free speech issue.[8]

---

4 TX H.B. 2789. Full text: https://capitol.texas.gov/tlodocs/86R/billtext/html/HB02789I.htm.

5 *Id.*

6 See John Browning, The Texas Revenge Porn Law: On Life Support After Ex Parte Jones? CIRCUITS (Sept. 2018).

7 *Id.*

8 Chuck Lindell, *Senate approves fix to 'revenge porn' law*, STATESMAN (May 19, 2019), https://www.statesman.com/news/20190519/senate-approves-fix-to-revenge-porn-law.

Despite these practical and legal challenges, this bill, nonetheless, is crucial in this digital age as it now establishes in writing that sending unsolicited explicit photographs is regarded as criminal conduct. While a $500 fine may not seem to provide much deterrence, at least it advances the notion that this conduct is illegal. And hopefully, as more people become aware of the new law pertaining to the unwanted solicitation of explicit digital images, perhaps it will influence some to refrain from this practice. As a member of the millennial statistic identified above, I believe this law is long overdue and is a necessary first step toward the reduction and eventual eradication of unsolicited explicit photographic images.

About the Author

Gwendolyn Seale is a 2016 graduate of SMU Dedman School of Law and practices entertainment law at Mike Tolleson and Associates in Austin, Texas. Her practice consists of drafting and negotiating contracts related to music, film, and sports entertainment, and assisting clients with copyright and trademark matters. In addition to her practice, Gwendolyn has published articles and presented Continuing Legal Education Courses on topics such as Youtube's monetization policies, legal issues surrounding music festivals, and the evidentiary significance of emojis.

Revenge Porn Laws in Texas

By Sanjeev Kumar

In the last decade plus, the proliferation of smart phones and social media platforms has resulted in the evolution of a new breed of warriors, the so called "keyboard warriors." The wide acceptance of these platforms and devices, combined with the easy accessibility of millions of users to these platforms, has enabled such keyboard warriors to have the capabilities of publication at their fingertips. This is in contrast to the prior ecosystem where such capabilities were the domain of a select few, such as news organizations, governmental entities, and media conglomerates.

The absence of any need to physically confront anyone else while using these platforms has almost worked as a superpower serum for some keyboard warriors. This sense of anonymity has provided some with courage that most would not possess in a physical confrontation. The keyboard warriors don't shy away from posting questionable content online that might give them pause before sharing with another face-to-face. This has resulted in public feuds between online users on the Internet and unfounded assertions posted by these keyboard warriors about their so called "enemies." This underlying hatred, combined with a false sense of courage, enables these keyboard warriors to act recklessly in posting, even though such actions would have resulted in ostracization by the community and even civil and/or criminal penalties if conducted outside of the ethereal world of social media platforms and the Internet.

One of the worst nightmares people have faced is the release of sexually explicit photos in public. Often, these are images and videos shared in private that suddenly become public as a result of a breakup, as one ex-partner "gets back at" the other with an intention to hurt and shame the other partner. This is the simplest example of revenge porn, though it might not be limited to just that type of public disclosure. Nude images, compromising videos or other private data may also end up on the Internet due to other motivations. These motivations range from political—as in the case of Dallas-area representative Joe Barton, who was already in his sixties when he shared his nude selfies with women that ended up appearing on Twitter—to revenge for failing to extort money—as in the numerous public cases of hacked celebrity selfies appearing on the Internet or hacked user accounts of the Ashley Madison dating site.

As is stated above, revenge porn is not limited to just ex-sexual partners. In the state of Texas, the definition of revenge porn is the act of intentionally disclosing or distributing visual

imagery of another person engaged in sexual acts or of another person's intimate parts. Thus, a person who engages in such activity may be civilly and criminally liable even if there was no prior sexual partnership with the other person.

In 2015, Texas enacted a law making it a crime to distribute sexually-explicit images of a person without that person's consent.[1] Unlike some of the other state's laws that designated this as a stronger criminal offense of felony, this was originally just a misdemeanor in Texas. Texas amended the law in 2017 to turn the offense into a state jail felony with a maximum punishment of two years in jail and a $10,000 fine.

The law makes it a crime when a person:

- Distributes nude or sexually explicit images or videos of a person;
- Without the depicted person's consent;
- The depicted person had a reasonable expectation of privacy when taking those images/videos; and
- The depicted person suffered harm and the depicted person's identity was revealed.

Furthermore, the law makes it a crime for a person to even threaten such a disclosure with an intent to extort a benefit or knowingly publish such material on a platform or website they own.

Such laws have been challenged on First Amendment grounds in multiple jurisdictions, including in Texas as early as 2015. In May 2018, East Texas' 12th Court of Appeals ruled that the law violated the First Amendment.[2] In this case, the perpetrator's act satisfied the first element of the crime, but it can be argued that the second element was an omission by the perpetrator. The law as written would have been applicable to a middleman forwarding such content without having any intention of harming the depicted person or knowledge that it was posted without consent.

The court concluded that Section 21.16(b) (of the Texas Criminal Code) was an invalid content-based restriction and was also overbroad because it violated the rights of too many third parties by restricting more speech than the Constitution permitted; therefore, its proscription on the disclosure of visual material was unconstitutional and a violation of the First Amendment Free Speech clause.[3] The court found that the state had not devised a narrow

---

[1] Tex. Pen. Code § 21.16 (2015).

[2] Ex Parte Jones, No. 12-17-00346-CR, 2018 WL2228888 (Tex. App.—Tyler, May 26, 2018).

[3] *Id.* at *8.

enough remedy to protect its compelling interest of protecting the citizens from unintended pornography as the law was applicable in an overbroad manner and would criminalize innocent disclosures protected by the First Amendment.

Even though the case is on appeal at the state's highest court, the Texas Court of Criminal Appeals, the state legislature passed an amendment in 2019 to include "intent to harm a person" in the law to narrow the applicability of the law and as a result overcome the 12th Court of Appeals objection. As amended in 2019, the law made it a crime when a person:

- Distributes nude or sexually explicit images or videos of a person;
- *With an intention to harm the depicted person;*
- Without the depicted person's consent;
- The depicted person had a reasonable expectation of privacy when taking those images/videos; and
- The depicted person suffered harm and the depicted person's identity was revealed.[4]

The 12th Court of Appeals also found that the law violated the First Amendment due to its content-based restriction, as the law requires the government to examine what was depicted in the photos or media to determine whether the law was broken; in the court's view, such "content-based" restrictions on photos, speeches, and other forms of expression could not be justified. The current law does not address this second issue which is being considered by the Court of Criminal Appeals and could still undermine the revenge porn law.

About the Author

Sanjeev Kumar is the founder and principal at Hunt Pennington Kumar & Dula PLLC, which provides a wide range of legal services to entrepreneurs and business owners in the areas of business and corporate law, intellectual property and estate planning. Sanjeev brings a vast wealth of experience in the tech industry to the table. Prior to practicing law, Sanjeev co-founded Portal Player, a semiconductor startup, and grew it into a NASDAQ listed company that was responsible for integral portions of the first seven generations of Apple iPods. Sanjeev is a past Computer & Technology Council Member and current Newsletter Editor for the Council. He is a member of the State Bar College of Texas and elected City Councilmember for the City of Lakeway, Texas. He is licensed to practice in Texas as well as registered with USPTO as a Patent Attorney.

[4] Tex. Pen. Code § 21.16 (2019).

Digital Border Searches Have Their Limits Too

By Pierre Grosdidier

Digital border search decisions keep rolling in. In *United States v. Cano*, the Ninth Circuit Court of Appeals held that manual digital border searches of cell phones require no reasonable suspicion of criminal activity but that forensic searches do.[1] Importantly, the court also held that these searches, whether manual or forensic, must be confined to the search for contraband and cannot extend to the search for criminal evidence. The court vacated Cano's conviction because it relied in part on evidence obtained through a warrantless search of his seized cell phone.

Cano was arrested entering the United States with 14 kilos of cocaine in his spare tire. Government agents seized his phone and searched it both manually and forensically without a warrant. Evidence obtained through these searches that was introduced at trial over Cano's objection helped convict him. On appeal, Cano argued, *inter alia*, that the searches breached the Fourth Amendment and that the collected evidence should have been suppressed.[2]

In holding for Cano, the court first restated the rule that border searches exist to enforce immigration laws, not laws in general. Immigration laws seek to identify legitimate travelers crossing the border and ensure that their effects contain no contraband. The court rejected the amicus's argument that the border search exception applies only to physical effects and does not reach the digital data on cell phones because the latter cannot conceal drugs, guns, or smuggled individuals. The court cited child pornography as the "best example" of digital contraband and held that cell phones and their data can be searched at the border.[3]

The court further explained that the search for contraband is different from the search for border-related crime, even if the distinction is a subtle one. It argued that the seizure of child pornography from a traveler at the border is a finding of contraband and evidence of criminal activity (*e.g.*, "possession of child pornography, 18 U.S.C. § 2252A(a)(5)(B), and importation of obscene material, 18 U.S.C. § 1462(a)"). However, such a seizure does not otherwise authorize border officials to investigate the traveler for other sex-related criminal activities. Likewise, the

---

1 934 F.3d 1002, 1007 (9th Cir. 2019). In *United States v. Cotterman*, the court had reached the same result for laptop computers. 709 F.3d 952, 1014 (9th Cir. 2013) (en banc). Because the arguments for this holding are not new, this article focuses only on the permissible scope of digital border searches.

2 *Id.* at 1008–10.

3 *Id.* at 1013–14.

border search exception does not allow border officials to search for evidence of criminal activity located at places other than the border.[4] For these reasons, the court held that the border search exception authorizes warrantless cell phone searches only to find contraband, or in a manner tethered to the search for contraband.[5] And, because border searches are confined to uncovering contraband, border officials may only forensically search cell phones when they reasonably suspect that the phones hide contraband.

As to Cano's case, the court held that officers' first manual searches of his cell phone were clearly authorized without any showing of suspicion. Their rummaging through Cano's text messages—and finding none—fell well within the scope of the search for digital contraband. But, the officers exceeded their authority when they recorded phone numbers in Cano's phone and snapped pictures of text messages that Cano received after his arrest because these actions bore no nexus to digital contraband.[6] Absent a reasonable reason to believe that Cano's phone contained contraband, the forensic search violated the Fourth Amendment and the collected evidence was inadmissible.[7]

About the Author

Pierre Grosdidier is an attorney at Houston. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Secretary for 2019–20.

---

4 *Id.* at 1017–18. The court acknowledged the tension of its holding with *United States v. Kolsuz*, which held that the border search exception includes "*the prevention and disruption of ongoing efforts to export contraband illegally.*" *Id.* at 1017 (citing *United States v. Kolsuz*, 890 F.3d 133, 143 (4th Cir. 2018)).

5 *Id.* at 1018–19.

6 *Id.* at 1019.

7 *Id.* at 1021.

Techshow Takeaways 2020

By William Smith

Each year, the Computer and Technology Section sends attendees to the American Bar Association TECHSHOW, one of the most prominent annual conferences on the integration of technology into legal practice. This year's conference (February 26 – 29, 2020) in Chicago, Illinois provided the opportunity to learn about the latest developments in cybersecurity, privacy, automation, and legal tech. It also provided great networking opportunities with a diverse group of practitioners, technologists, and vendors in attendance. In this issue of *Circuits*, we summarize presentations from the conference that consider the impact of two new software tools on the practice of law.

NOTE: At the time of publication, final session materials had not been made available for download by the ABA. We have provided citations to sources where they are available. Otherwise, we rely on the identified presenters as sources. *Circuits* readers looking for further information are encouraged to contact the author at wdsmithii@gmail.com, as additional detail should be available in the final materials.

DEEPFAKES AND LEGAL PRACTICE: THE LATEST DEVELOPMENTS

Sharon D. Nelson of cybersecurity and forensics provider Sensei Enterprises (https://senseient.com/) and Lincoln Mead of Canon Discovery Services (https://cbps.canon.com/managed-services/discovery-services) gave a timely overview of "deepfakes". "Deepfake" refers to the use of machine learning "Artificial Intelligence" (AI) technology to create convincing fake video and audio of real people. Its prevalence has exploded: an October 2019 report from Deeptrace Labs identified 14,678 deepfake videos representing an 84% increase from December 2018, with 850 identified victims.[1]

Deepfakes are created using generative adversarial networks (GANs). These consist of two algorithmic systems called a generator and a discriminator which go through thousands or more iterations of creating an output designed to imitate a real image. The process attempts to detect if the image is synthetic by comparing it against a human-curated training dataset.

---

[1] Aja Romano, *Deepfakes are a real political threat. For now, though, they're mainly used to degrad* women, Vox (Oct. 7, 2019), https://www.vox.com/2019/10/7/20902215/deepfakes-usage-youtube-2019-deeptrace-research-report.

Based on the errors detected by the discriminator, the generator refines its algorithm to produce a more accurate fake. This process is repeated until an acceptable level of fidelity is reached. An exploration of how this technology actually works is beyond the scope of this article, but it is worth noting a few characteristics of the technology that have significant practical implications. GANs are a popular technique in many "AI" applications, meaning that advances in other areas of machine learning may be applied to improve deepfakes. Their effectiveness is based on having a large dataset of real images of the targeted person. The requisite "raw material" is likely to increase for the foreseeable future as the number of photos, videos, and audio recordings of individuals and public figures captured on the internet grows. Finally, because all deepfake detection methods currently available are also based on machine learning techniques, the presenters envisage an escalating arms race between the creation and detection of deepfakes in the short and medium term.

Applications: Social media and the political use of Deepfakes

Most media coverage of deepfakes has focused on its potential use in politics. The presenters shared a number of examples of the use of synthetic or artificial video to political ends. They noted that the most prominent use thus far—a fake video of House Speaker Nancy Pelosi appearing to drunkenly slur her words during an interview—was in fact a "shallowfake". This is where fake media is created through more traditional digital editing techniques without the use of machine learning.[2] In a different example, director Jordan Peele's deepfake of President Obama, created for educational purposes, was shown to demonstrate the sophistication of deepfake technology.[3]

Social media is the primary vehicle used to spread political disinformation. However, social media platforms have struggled to respond to public pressure to adopt coherent policies on deepfakes. This has also been the case with fake news more generally. Recent examples provided in the session highlighted the approaches of various high-profile platforms. In January, Facebook adopted the policy that it would ban any media if it:

1. "has been edited or synthesized – beyond adjustments for clarity or quality – in ways that aren't apparent to an average person and would likely mislead someone into thinking that a subject of the video said words that they did not actually say" and

---

[2] Jeff Horwitz, *Pelosi Slams Facebook Over Altered* Video, THE WALL STREET JOURNAL (May 29, 2019), https://www.wsj.com/articles/pelosi-slams-facebook-over-altered-video-11559164773.

[3] *You Won't Believe What Obama Says In This Video!*, YOUTUBE (Apr. 17, 2018), https://youtu.be/cQ54GDm1eL0 (last visited Mar. 18, 2020).

2. "is the product of artificial intelligence or machine learning that merges, replaces or superimposes content onto a video, making it appear to be authentic".[4]

The presenters' views were that this policy contains so much wiggle room as to be largely ineffective. Twitter's policy is also fairly subjective, including a requirement that the media be "likely to cause harm" (4 February 2020) to be subject to removal.[5]

Given that social media is the primary vehicle used to spread political disinformation, it is ironic that many social media platforms are actively developing and promoting identical technology for benign uses. In one example, Snapchat launched a "Cameos" feature on December 9, 2019 which allows users to artificially insert their faces in pre-existing videos.[6]

Applications: Fraud, Harassment, and Fabricated Evidence

As significant as the political and cultural implications of deepfakes are, the use of this technology for fraud and its impact on many kinds of evidence are likely to have more immediate ramifications for lawyers. The TECHSHOW presentation illustrated this with two startling examples from the UK.

Economically motivated criminals are often early adopters of new technology (e.g.: ransomware attackers and cryptocurrency). Deepfakes are no exception. In September 2019, reports emerged of a British energy CEO who thought he was on the phone with the boss of his firm's German parent company.[7] Since the CEO recognized the subtle accent and "melody" of his boss's voice, he did not question the instruction to immediately transfer €220,000 EUR to the bank account of a Hungarian supplier. According to the victim, he only became suspicious later when calls came through purporting that the transfer had been reimbursed, which was not the case, and requesting a second transfer. Since no suspects have been identified, the technology used by the attackers is unknown and the victim's account is the only publicly disclosed evidence. This kind of criminal application is likely to become widespread, due to the low cost

---

4 Monika Bickert, *Enforcing Against Manipulated Media,* Facebook (Jan. 6, 2020), https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/ (last visited Mar. 18, 2020).

5 Yoel Roth & Ashita Achuthan, *Building rules in public: Our approach to synthetic and manipulated media*, Twitter (Feb. 4, 2020), https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html (last visited Mar. 18, 2020).

6 *Introducing Cameos*, Snap Inc. (Dec. 9, 2019), https://www.snap.com/en-US/news/post/introducing-cameos (last visited Mar. 18, 2020).

7 *Voice Deepfake Scammed a CEO Out of $243,000*, Ride the Lightning (Sept. 10, 2019), https://ridethelightning.senseient.com/2019/09/voice-deepfake-scammed-a-ceo-out-of-243000.html (last visited Mar. 18, 2020).

of audio deepfake technology, and the high incidence of phishing-based invoice fraud. The presenters recommended that best practice for transfer verification must now be an outgoing phone call placed to a known trusted number, since neither the caller ID data nor the voice on the other end of incoming calls can be considered reliable.

The presenters also described a 2019 UK family law case in which, according to the father's counsel, deepfake audio was entered into evidence for the first time in the United Kingdom. (Please note that the presenters' source list was not available at the time of publication, and so the citation in the footnote below is the most detailed report the author was able to locate. Moreover, because the UK custody proceeding records are sealed, the account of the father's attorney will be difficult to verify.) Reportedly, the mother of the child subject to the proceeding produced a recording of the father making violent threats towards his wife.[8] Byron James, the father's attorney, claims that they were later able to obtain an un-edited version of the actual recording and demonstrate that the mother had used technology to create a fake, synthetic recording. As Mr. James observed, judges are not currently trained to be aware of the possibility of this type of false evidence, and the presenters noted that the same is true of lawyers and jurors.

Another prominent area where deepfake technology is being used maliciously at the individual level is the production of nonconsensual pornography and revenge porn. Deeptrace Labs' research found that the overwhelming majority—96%— of deepfake videos depict women.[9] Those videos often depict synthetic pornography of female celebrities. However, the accessibility of the technology is fueling the creation of fake videos of former romantic partners for blackmail or harassment. One of the presenters reported that their firm was now frequently receiving inquiries from clients who had been the victim of this practice. In mid-2019, an app called "Deepnude" was released which had purportedly been trained on 10,000 images and used deepfake techniques to create a nude version of any image depicting a clothed woman.[10] It was for sale for $99 until its creator removed it. Copies are reportedly

---

8 Patrick Ryan, '*Deepfake' audio evidence used in UK court to discredit Dubai dad*, THE NATIONAL (Feb. 8, 2020), https://www.thenational.ae/uae/courts/deepfake-audio-evidence-used-in-uk-court-to-discredit-dubai-dad-1.975764.

9 Aja Romano, *Deepfakes are a real political threat. For now, though, they're mainly used to degrad* women, VOX (Oct. 7, 2019), https://www.vox.com/2019/10/7/20902215/deepfakes-usage-youtube-2019-deeptrace-research-report.

10 James Vincent, *Copies of AI deepfake app DeepNude are easily accessible online—and always will be*, THE VERGE (July 3, 2019), https://www.theverge.com/2019/7/3/20680708/deepnude-ai-deepfake-app-copies-easily-accessible-available-online.

available on the grey market for $20. However, revenge pornography is one of the few areas where legislatures have made progress on regulating deepfake technology (see below).

Controlling Deepfakes: Regulation

Virginia became the first state to make it a crime to share deepfake revenge pornography when it amended its existing revenge porn statute in July 2019 to include videos involving "a person whose image was used in creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic."[11]

In October 2019, Texas became the first state to criminalize the use of deepfakes in politics, amending the Texas Election Code to make it an offense if a person, "with the intent to injure a candidate or influence the result of an election: (1) creates a deep fake video; and (2) causes the deep fake video to be published or distributed within 30 days of an election."[12] Shortly thereafter, California also passed a law criminalizing the use of deepfakes in campaigning.[13] However, both the Texas and California laws have been criticized for being open to constitutional attack on First Amendment grounds.[14]

The National Defense Authorization Act, signed into law by President Trump on December 20, 2019, contained the first federal measure addressing deepfakes. It required the government to produce a report on foreign weaponization of deepfakes and to inform Congress about deepfake disinformation activities targeting US elections and established a prize for deepfake detection development.[15]

---

[11] Virginia Code § 18.2-386.2(A).

[12] Texas Election Code Title 15 § 255.004(d).

[13] California Elections Code §20010.

[14] *See, e.g.,* Kenneth Artz, *Texas Outlaws 'Deepfakes' but the Legal System May Not Be Able to Stop Them*,TEXAS LAWYER (Oct. 11, 2019), https://www.law.com/texaslawyer/2019/10/11/texas-outlaws-deepfakes-but-the-legal-system-may-not-be-able-to-stop-them/; Kari Paul, *California makes 'deepfake' videos illegal, but law may be hard to enforce*,THE GUARDIAN (Oct. 7, 2019), https://www.theguardian.com/us-news/2019/oct/07/california-makes-deepfake-videos-illegal-but-law-may-be-hard-to-enforce.

[15] Matthew Ferraro et al, *First Federal Legislation on Deepfakes Signed Into Law*, WilmerHale (Dec. 23, 2019), https://www.wilmerhale.com/en/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law.

Since then, legislation has been introduced or is pending in Massachusetts, New York, Maryland, and at the federal level. Security firm Malwarebytes published a blog post in January offering a useful overview of these initiatives.[16]

Controlling Deepfakes: Research and Technology

Efforts to draft and enforce regulations to combat the malicious use of deepfakes are not just complicated by free speech concerns. They are also hampered by the lack of reliable tools to identify deepfake content. The TECHSOW presentation concluded with some examples of research groups in academia and industry that are on the cutting edge of this work, a few of which are highlighted here.

UC Berkeley's School of Information has developed a detection tool based on a person's unique facial quirks.[17] SUNY Albany's Department of Computer Science has assembled a repository of deepfake techniques based on comparing altered videos to the originals, which they are using to create detection tools.[18] The Technical University of Munich created a FaceForensics++ database of deepfake examples by applying four common face manipulation techniques to 1,000 YouTube videos.[19] Google expanded on that project by hiring 28 actors to record a set of baseline videos and then applying publicly available deepfake algorithms to produce 3,000 sample synthetic videos.

The presenters pointed out that many of the detection techniques can probably be defeated by improving the neural networks used for deepfake production. Given that technological arms race, the legal difficulties in regulating political speech, and the borderless nature of the Internet, it is likely that political discourse will continue to be significantly impacted by deepfake synthetic media. The accessibility of deepfake technology means that lawyers who assess the credibility of recorded evidence and advise clients on how to prevent and redress fraud must quickly educate themselves on the subject.

---

[16] David Ruiz, *Deepfakes laws and proposals flood US*, Malwarebytes Labs (Jan. 23, 2020), https://blog.malwarebytes.com/artificial-intelligence/2020/01/deepfakes-laws-and-proposals-flood-us/ (last visited Mar. 18, 2020).

[17] Kara Manke, *Researchers From the I School and Engineering Use Facial Quirks to Unmask 'Deepfakes'*, Berkeley School of Information (Jun. 18, 2019), https://www.ischool.berkeley.edu/news/2019/researchers-i-school-and-engineering-use-facial-quirks-unmask-deepfakes (last visited Mar. 18, 2020).

[18] *Tackling the DeepFake Detection Challenge*, University at Albany (Sept. 20, 2019), https://www.albany.edu/news/92306.php (last visited Mar. 18, 2020).

[19] *Google has released a giant database of deepfakes to help fight deepfakes*, MIT Technology Review (Sept. 25, 2019), https://www.technologyreview.com/f/614426/google-has-released-a-giant-database-of-deepfakes-to-help-fight-deepfakes/ (last visited Mar. 18, 2020).

MARKETING PLANNING AND CRM SOFTWARE FOR LAWYERS

Thursday at TECHSHOW included a session about marketing strategy for lawyers and customer relationship management software products that are custom-made for attorneys. The session was presented by Stephanie Everett of Lawyerist (https://lawyerist.com/) and Chelsey Lambert of Legal Tech Media Group (https://lextechreview.com/).

The session's theme was to move beyond "random acts of marketing", which is the kind of reactive and uncoordinated approach that many lawyers currently employ. Many lawyers expend significant effort in traditional ways of marketing themselves—networking, presenting at conferences, paid advertising, lawyer directories, etc. However, these activities may not produce a high return on that effort, and few firms have the right tools in place to measure that return. Fortunately, as the presenters showed, the current generation of lawyer-specific Customer Relationship Management (CRM) tools offers significant efficiency gains and returns on investment, contrasted with the labor intensive "random acts of marketing" approach.

A More Strategic Approach to Marketing

To market effectively, lawyers need to have a marketing strategy. This should answer the following questions: Who are we going to target? What are we going to say to them? How are we going to reach them?

Lawyers and firms should consider what makes a great client prospect, and what the characteristics of that prospect are. It might be better to focus on a smaller number of more profitable clients or there might be cheaper ways of acquiring and serving a larger number of less profitable clients. Auditing current sources of leads, for example referrals, website visitors, legal directory profiles, in-person networking/business development, and email marketing, can help the firm measure its current efforts and understand where it should improve.

Once it understands the "personas" of its clients, a firm can think about how its sales funnel works. The sales funnel describes the journey that customers go on to move from leads to buyers. The presenters' model describes the stages of awareness, interest, consideration, intent, evaluation, and purchase. For many firms, the website will be a key part of this sales funnel. Research shared in the session shows that when a visitor comes to a website, the marketer has 20 seconds to grab their attention and then 2 minutes to get them to stick around. Once that point is reached, statistically the visitor will most likely view multiple pages. Lawyers should consider what questions come up frequently with clients and what their concerns are to inform what message to deliver to their prospects.

The other key component of the marketing strategy is how the firm will find the prospects it wants in order to deliver the right message to them. Most firms are using many of the channels described above like email, social media, and in-person networking. However, technology offers ways to do much of this more efficiently and to measure the effectiveness and ROI of these efforts. Given that the average cost to acquire an email address is $75, according to the presenters, and how valuable and scarce attorney time is, this greater efficiency is critical to making business development more effective. The CRM industry has solutions that are purpose-built for lawyers and that are easy to use right out of the box. These include **Lawmatics, Clio Grow, Lead Docket, ClientRock, Captorra, and Law Rules**. Readers can find reviews of these products at Chelsey's website, https://lextechreview.com/.

About the Author

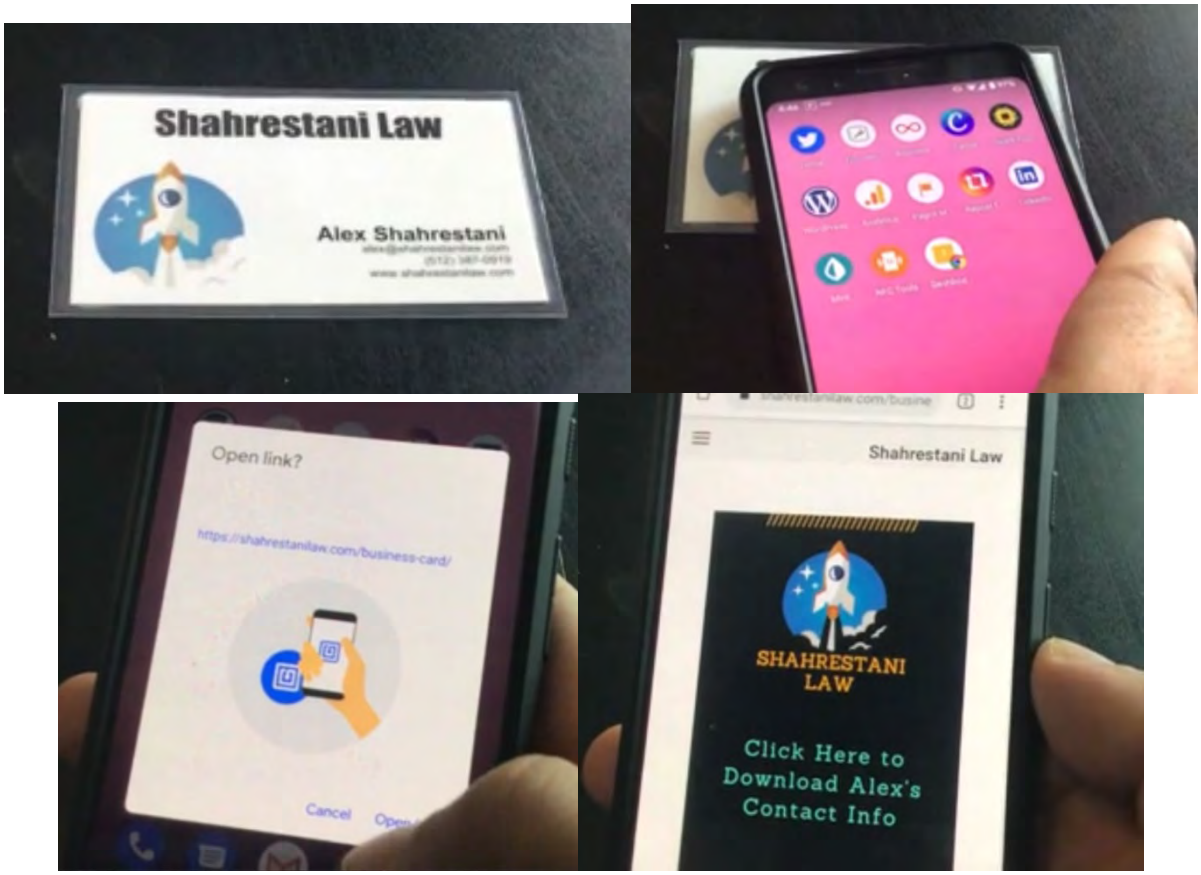
William Smith is Assistant General Counsel of Business Talent Group, LLC (BTG), the leading marketplace that connects independent management consultants, subject matter experts, and executives with global companies to solve their biggest business problems. He leads BTG's data privacy compliance, employment law, and commercial agreements activities. In addition, he closely supports BTG's General Counsel on fundraising transactions, governance and investor matters, and risk management. He is a member of the Council of the Computer and Technology Section of the State Bar of Texas.

Automate My Practice: Make Your Own Digital Business Card

By Alex Shahrestani

If you're anything like me, you've got hundreds of beautifully designed business cards that are uselessly sitting on your desk when you need them the most. It's an extra thing to think about, and it can be hard to remember when you're running out the door during a busy day.

I decided to solve that problem by building myself a personalized digital business card.



It works automatically on about four out of five devices that I come across, and it's a nifty party trick! To get started, you'll need a few things.

- An NFC-enabled smartphone. NFC is standard on most, if not all, new models of smartphones.
- A smartphone app for writing to NFC tags. I used "NFC Tools," but there are others out there.
- One of your business cards.
- An NFC sticker. You can buy packs of NFC stickers on Amazon for around $10.

- A webpage for hosting your contact info.
- Access to lamination services, such as Office Depot (optional).

Step 1: Design Your Contact Info Page

Your contact info page can look however you want it to. However, I would suggest keeping the page simple and informative. Here's mine:

It's a simple image that I embedded with a link to my "Contact Card." You're probably familiar with contact cards, but just in case you're not: a contact card is a file format for storing contact information on a phone. The contact information stored on a contact card includes names, email addresses, phone numbers, websites, social media profiles, and more.

Create a contact for your own business on your phone and add every piece of information you want people to have. I include all contact info, a link to my website, a link to my firm's social media profiles, and the name of my firm. "Share" your contact card to your own email address

to get the file in the correct format, then upload it to a location that is publicly accessible (such as your website).

Now you'll put the image and the link together: create a page on your website to place the image, then embed the link to your contact card in the image. Here's a link to my contact card page.

Step 2: Make Your NFC Tag

Open up your NFC-writing app and find the "Write" option. Your app will probably give you various options on the data you can write to your tag. Options will likely include files, phone numbers, addresses, and various automated tasks, such as automatically logging someone into your WiFi. All you'll need to add is a URL pointing to the page you set up in Step 1.

You technically could just add all of that information from Step 1 directly to the tag instead of the webpage, but there are a couple of reasons not to do that. First, NFC tags can't hold very much information, so you might limit what info you can share with your tag. More importantly, it makes it inconvenient to update the information you share if it ever changes.

Once you've selected the URL, select the "Write to Phone" option and tap the upper back of your phone to the tag. You should get a notification on your screen letting you know if the tag was successfully written. If something goes wrong, you can just tap "Write to Phone" and try again—NFC tags let you write to them as many times as you want.

Test the NFC tag by closing the app on your phone and tapping the back of your phone to the tag again. Your phone should prompt you with a link to open.

Step 3: Wrapping Up

The final step is the most satisfying – attach the sticker to the back of your business card and take it to get laminated. Make sure not to fold the sticker around the edge of the card or the NFC tag will break. In fact, I would bring a few cards with a few stickers affixed to them just in case something goes wrong.

If you don't want to or can't get the cards laminated, consider sticking the NFC tag to something you always have with you, like a water bottle or cell phone, and cover it with a sticker. It will function just as well, and it will be just as convenient.

About the Author

Alex Shahrestani is a startup-tech nerd trapped in an attorney's body. He serves as Vice President of EFF-Austin, CLE Program Coordinator for SXSW, a leadership member of the Computer & Technology Section of the State Bar, a leadership member of Texas Exes Young Alumni- Austin, and the Founder of the Journal of Law and Technology at Texas. His practice focuses on startup and small business issues, and he provides subscription services for his clients. You can find out more about him and how he uses his CS background to inform his practice at shahrestanilaw.com.

How to Join the State Bar of Texas Computer & Technology Section

Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.

Step 1
Go to Texasbar.com and click on "My Bar Page"

Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)

If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.

State Bar of Texas Computer & Technology Section Council

Officers:
John Browning – Dallas – Chair
Shawn Tuma – Plano – Chair-Elect
Elizabeth Rogers – Austin – Treasurer
Pierre Grosdidier – Houston – Secretary
Sammy Ford IV – Houston – Past Chair

Webmaster:
Judge Xavier Rodriguez – San Antonio

Circuits Editor:
Sanjeev Kumar – Austin

Term Expiring 2022:
Lavonne Burke Hopkins – Houston
Gwendolyn Seale – Austin
Alex Shahrestani – Austin
Michelle Mellon-Werch – Austin

Term Expiring 2021:
Chris Downs – Plano
Seth Jaffe – Houston
Judge Emily Miskel – Dallas

Term Expiring 2020:
Lisa Angelo – Houston
Eddie Block – Austin
Kristen Knauf – Dallas
Rick Robertson – Plano

Chairs of the Computer & Technology Section

2018-2019: Sammy Ford IV
2017-2018: Michael Curran
2016-2017: Shannon Warren
2015-2016: Craig Ball
2014-2015: Joseph Jacobson
2013-2014: Antony P. Ng
2012-2013: Thomas Jason Smith
2011-2012: Ralph H. Brock
2010-2011: Grant Matthew Scheiner
2009-2010: Josiah Q. Hamilton
2008-2009: Ronald Lyle Chichester
2007-2008: Mark Ilan Unger
2006-2007: Michael David Peck
2005-2006: Robert A. Ray
2004-2005: James E. Hambleton
2003-2004: Jason Scott Coomer
2002-2003: Curt B. Henderson
2001-2002: Clint Foster Sare
2000-2001: Lisa Lynn Meyerhoff
1999-2000: Patrick D. Mahoney
1998-1999: Tamara L. Kurtz
1997-1998: William L. Lafuze
1996-1997: William Bates Roberts
1995-1996: Al Harrison
1994-1995: Herbert J. Hammond
1993-1994: Robert D. Kimball
1992-1993: Raymond T. Nimmer
1991-1992: Peter S. Vogel
1990-1991: Peter S. Vogel