COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas
September 2019

CLICK ON TITLE TO JUMP TO ARTICLE

- Note from the Chair by John G. Browning
- Letter from the Editor by Sanjeev Kumar

Featured Articles

- Can Authorities Compel a Suspect to Use His or Her Biometrics to Unlock a Digital Device? By Pierre Grosdidier
- Facebook Faceoffs: Artist Fights Over Social Media Rights and The Need to Address Page Roles in Contract by Gwendolyn Seale and John G. Browning
- Facebook's Libra: What is all the Fuss About? By Ronald Chichester
- Into the Data Breach: The Hit or Miss Patchwork of U.S. Cybersecurity Law by Jeffrey D. Hunt
- Ghosts in the Machine: Algorithmic Bias and the Courts by John G. Browning and Alex Shahrestani
- Expecting a Federal Consumer Data Privacy Law in the US? By Lisa M. Angelo
- Demonetization and Censorship on YouTube: You're Not Gonna Win by Gwendolyn Seale

Op-Eds

- Competency Requirements and Technology: I am a Lawyer, so why do I need to understand or use technology? By Sanjeev Kumar

Short Circuits

- Featuring Tom Kulik, Pierre Grosdidier, and John G. Browning

CircuitBoard

- Featuring John G. Browning

Contents

Message from the Chair 3
By John G. Browning 3

Letter from the Editor 5
By Sanjeev Kumar 5

Featured Articles:-

Can Authorities Compel a Suspect to Use His or Her Biometrics to Unlock a Digital Device? 7
By Pierre Grosdidier 7
About the Author 9

Facebook Faceoffs: Artist Fights Over Social Media Rights and The Need to Address Page Roles in Contract 11
By Gwendolyn Seale and John Browning 11
About the Authors 17

Facebook's Libra: What is all the Fuss About? 19
By Ronald Chichester 19
About the Author 25

Into the Data Breach: The Hit or Miss Patchwork of U.S. Cybersecurity Law 26
By Jeffrey D. Hunt 26
About the Author 30

Ghosts in the Machine: Algorithmic Bias and the Courts 31
By John G. Browning and Alex Shahrestani 31
About the Authors 42

Expecting a Federal Consumer Data Privacy Law in the US? 44
By Lisa M. Angelo 44
About the Author 48

Demonetization and Censorship on YouTube: You're Not Gonna Win 49
By: Gwendolyn Seale 49
About the Author 54

Op-Eds:-

Competency Requirements and Technology: I am a Lawyer – I know the Law, so why do I need to Understand or Use Technology? 55
By Sanjeev Kumar 55
About the Author 56

Short Circuits:-

More Than Meets the Eye? Why Deepfakes Are Trouble Under Existing Copyright & Privacy Laws 57
By Tom Kulik 57
About the Author 60

Instagram Will Get You If You Are Not Mindful 61
By Pierre Grosdidier 61
About the Author 63

Service of Process via Social Media Comes to Texas 64
By John G. Browning 64
About the Author 67

CircuitBoards:-

Legislative Update – Cybersecurity 68
By John G. Browning 68
About the Author 69

How to Join the State Bar of Texas Computer & Technology Section 70

State Bar of Texas Computer & Technology Section Council 72

Chairs of the Computer & Technology Section 72

Message from the Chair

By John G. Browning

Greetings from the Computer & Technology Section! We thank you for being a member, and we hope that you will help us spread the word by urging your colleagues to join as well. Our section has as its mission being a resource to the legal profession in all matters involving technology. With the Supreme Court of Texas' February order amending Rule 1.01 of the Texas Disciplinary Rules of Professional Conduct, Texas became the 36th state to require technological competence—being conversant in the "benefits and risks of relevant technology"—as part of what it means to provide competent representation to clients. Here at the Computer & Technology Section, we are committed to helping Texas lawyers fulfill that duty through the myriad of legal tech education opportunities we offer.

How are we doing this? If you attended the State Bar Annual Meeting in June, our Section sponsored the Adaptable Lawyer track, and provided an array of speakers and materials on cutting edge topics for Texas lawyers ranging from cybersecurity to new sources of digital evidence in the courtroom to tips on apps to make law practice easier and more efficient, as well as a look at how artificial intelligence is impacting our profession. Our members are also regular speakers at Texas Bar CLE events throughout the year on a wide variety of technology-related subjects including ethics. And if you prefer getting your CLE credit in the comfort of your home or office, we have an amazing variety of educational videos—Tech Bytes—available to all Texas lawyers at texasbar.com/tech-resources. Ranging from 5-10 minutes to 45 minute presentations, these videos address areas like encryption, data privacy, ediscovery, and investigations using social media. We are also proud of our commitment to promoting access to justice efforts, and every year we sponsor "With Technology and Justice for All," a one-day CLE course designed to assist legal aid, pro bono, and new lawyers with using technology to enhance their practices.

But, as they say in infomercials, that's not all. Section members continue to enjoy complimentary use of our Texas Bar Legal App, which gives you access to current Texas rules and codes (with links to relevant case law) right at your fingertips. We also publish this members-only newsletter--*Circuits*. Each issue is packed with informative articles about cutting-edge topics, and this issue is no different. From new legislative developments to emerging cases, *Circuits* has it all. You will also see our members' articles on a regular basis in other bar publications, such as the *Texas Bar Journal*.

So let me thank you again for your membership, and for your interest in matters at the intersection of technology and the law. If you would like to become more involved in the Computer & Technology Section, please contact our Section administrator at admin@sbot.org.

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

Letter from the Editor

By Sanjeev Kumar

Welcome to the first issue of *Circuits* for the 2019–20 bar year! I am happy to bring you another issue of *Circuits*, the sections quarterly newsletter, which once again includes several hot articles dealing with technology and law.

There have been multiple reports of authorities searching travelers' electronic footprints on their devices when entering the United States. The fingerprint and facial recognition technology to unlock one's personal device is becoming almost a standard feature on most portable devices, including notebooks, tablets, and smart phones. In the first article of our *Feature Articles*, Pierre Grosdidier (Past Editor and Council Member) gives us a detailed analysis of the legality of governmental agents forcing biometric unlock of a personal device that does not require suspects to divulge their private password for access.

In the next article, Gwendolyn Seale (current Council Member) and John Browning (current Section Chair) give us a glimpse of the battles for control of valuable digital assets associated with Facebook pages that are ensuing and yet to come between band members with soured relationships.

Crypto-currencies like BitCoin and Etherium have seen wild swing in their valuations. The speculative (or real) future of crypto-currencies has resulted in the launch of numerous crypto-currencies and much has been discussed about the interplay between such currencies and regulatory regimes. Ron Chichester (past Section Chair) discusses Facebook's crypto-currency, Libra, and the fuss created by its announcement in his article.

Serious breaches of digital databases have occurred, exposing millions of users' personal information as a direct result of the digitization of more and more data. Such cyberbreaches may result in substantial liabilities for various companies that may be at fault. Guest author Jeffrey D. Hunt gives us a short tour of the wild, wild west of cyber space and the patchwork of cybersecurity laws that may assign liability and/or may be available to an aggrieved party as a remedy.

We have all become aware of the allegations of political biases in social media platforms and fake news. Machine learning and artificial intelligence drive automated decisions in myriad segments in our daily lives, such as employment, mortgages, and healthcare. Section Chair

John Browning and Alex Shahrestani (current Council Member) explore this by focusing on algorithmic bias in the criminal justice context in their article.

Cloud storage, higher connection speeds, and wide adoption of social media applications have resulted in huge amounts of personal data on the cloud and have resulted in extremely accurate profiles for consumers. Most states have enacted consumer data privacy laws, which have created varied requirements for commercial enterprises, even though computer networks do not easily recognize state boundaries. Lisa Angelo (current Council Member) analyzes the patchwork of privacy laws enacted by multiple states and whether there may be a need for or expectation of any federal legislation on the topic in the near future.

The internet has created an avenue for independent artists and contributors to monetize their products through ad-revenue on various platforms, the most well-known being YouTube. Unfortunately, an unfortunate placement of an advertisement alongside socially reprehensible content often results in a wide backlash. Gwendolyn Seale discusses the good and bad consequences of the new monetization policy by Google for YouTube channels.

In our *Op Ed*, Yours Very Truly discusses the technical competency requirements for lawyers in Texas and why we cannot afford to turn a blind eye to technology. Of course, the opinions expressed in the op-ed are entirely mine and not those of the Computer and Technology Section, the State Bar of Texas, and their respective officers.

In our *Short Circuits*, Tom Kulik discusses the ineffectiveness of current copyright laws when it comes to deepfakes; Pierre Grosdidier discusses how someone's digital trail may impact the choice of proper jurisdiction; and John Browning provides an update on developments associated with Service of Process by Social Media in Texas.

Finally, in *CircuitBoards*, John Browning provides a legislative update on cybersecurity.

Many thanks to all the contributors for this rich issue and for helping us keep this publication on schedule. Thank you also to Antony P. Ng for his review of and assistance with this issue's articles. We hope that you enjoy reading *Circuits*, and welcome any comments that you may have: please send them to our section administrator at admin@sbot.org.

Kind Regards,
Sanjeev Kumar, Editor

Can Authorities Compel a Suspect to Use His or Her Biometrics to Unlock a Digital Device?

By Pierre Grosdidier

Can authorities compel a suspect to provide a fingerprint, or a facial or iris scan, to unlock the suspect's protected digital device?[1] This question is increasingly important to law enforcement officials given the growing pervasiveness of biometrically protected smart devices. If the answer is no, a suspected child pornographer might place himself beyond prosecution by protecting his stash of contraband with a biometric. Courts are split.

Whereas the Fourth Amendment governs authorities' ability to seize and search a digital device, the Fifth Amendment's protection prohibiting self-incrimination controls their ability to compel the device's owner to surrender access. The Fifth Amendment protects an individual if he or she can show that the following three conditions are met: (1) compulsion, (2) a testimonial communication or act, and (3) incrimination.[2] Authorities usually seek to access confiscated devices when they expect to find child pornography. The elements of compulsion and incrimination are easily satisfied in these cases because authorities seek to coerce a suspect to provide a biometric that grants access to potentially highly compromising evidence. The question then whittles down to whether the act of communicating a biometric is "testimonial."[3]

The testimonial aspect of the act of production is different from the substance of the production. The Fifth Amendment does not protect the latter.[4] But, courts have long recognized that the *act* of producing something may be sufficiently testimonial to "trigger Fifth Amendment protection when the production explicitly or implicitly conveys some statement of

---

[1] The question of whether authorities can compel a suspect to surrender a passcode will be addressed in the next issue of *Circuits*. The answer is, generally, no, because it is a testimonial act. *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1352 (11th Cir. 2012).

[2] *United States v. Authement*, 607 F.2d 1129, 1131 (5th Cir. 1979) (per curiam).

[3] *See*, *e.g.*, *In re Search of a Residence in Oakland, Ca.*, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019).

[4] *In re Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, No. 1:19-mj-10441, 2019 WL 2082709, --- F. Supp. 3d ---, at *3 (D. Idaho May 8, 2019) (citing *Johnson v. United States*, 228 U.S. 457, 458 (1913)).

fact."[5] What triggers the Fifth Amendment is whether the act of production requires the individual "to use 'the contents of his own mind'."[6] Conversely, compelling a suspect to perform a mere physical act, like opening a safe with a key, submitting to a line-up, or providing a voice or handwriting exemplar, a blood sample, or fingerprints, is not testimonial.[7]

At least one district court has held that the act of compelling a suspect to provide biometrics to unlock a digital device is testimonial. In *In re Search of a Residence in Oakland, Cal.* the court denied a warrant that sought the right to compel persons found at a search location to provide their biometrics to unlock confiscated devices.[8] The court held that if a person cannot be forced to provide a passcode because the act is testimonial, the same logic necessarily applied to a biometric. The court also refused to equate a fingerprint taken for identification purposes with one taken to unlock a phone that contains "a database of someone's most private information." It held that the act of pressing a finger to unlock a phone testified to the person's control over, or connection with, the phone's contents and was, therefore, protected.[9]

Other courts have held that compelling a suspect to provide his or her biometrics to unlock digital devices does not offend the Fifth Amendment. These courts reason that the government merely compels a physical act that does not require the suspect to use his mind.[10] In *In re Search Warrant Application for [redacted text]*, the district judge reversed a magistrate judge who had upheld the Fifth Amendment defense.[11] The district judge held that requiring residents of a home to unlock digital devices with their fingerprints did "not qualify as a testimonial communication." The act of pressing a fingerprint was merely physical and not communicative; it could even be done while the suspect slept. The judge rejected the argument that the ability to unlock a device created the inference that the suspect possessed and controlled the device. The issue is whether the act is testimonial, not whether it is

---

5 *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1342.

6 *Id.* at 1345.

7 *Id.* and n.24. Requiring the production of a safe's *combination* is testimonial. *In re Search of [Redacted] Wash., D.C.*, 317 F. Supp. 3d 523, 535 (D.D.C. 2018) (mem. op.).

8 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019).

9 *Id*. at 1016 (citation omitted).

10 *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d at 800, 804 (N.D. Ill. 2017) (Chang, D.J.) (mem. op.).

11 *Id*. at 801. For the case below, *see In re Search of the Single-Family Home and Attached Garage Located at [redacted]*, No. 17-M-85, 2017 WL 4563870 (N.D. Ill. Feb. 21, 2107) (Finnegan, M.J.) (citing *In re Application for a Search Warrant*). These three cases' history is somewhat confusing because judge Chang's opinion does not cite magistrate judge Weisman's opinion and order, and the latter is not flagged with negative history in Westlaw.

incriminating because of its consequences.[12] For example, taking fingerprints can be highly incriminating but, that does not make the practice unconstitutional.

Likewise, in *In re Search of [Redacted] Wash., D.C.*, the court held that compelling the use of a subject's biometric was closer to "the surrender of a safe's key than its combination," because no thoughts are required on the suspect's part.[13] Any thought-like decryption to gain entry into the device is performed by the device and its software, not by the suspect. The court also could make no "principled distinction" between drawing blood for blood-alcohol content, which is not testimonial, and taking biometric features.[14] For these reasons, the court granted a search warrant authorizing the government to unlock the suspect's devices with his biometrics.[15]

Two state courts have issued opinions upholding authorities' right to use suspects' biometrics to unlock their digital devices. In *State v. Diamond*, the Minnesota Supreme Court held that producing a fingerprint was a physical act closer to displaying a body in a lineup than producing documents (which can be a protected act because it requires a thought process).[16] Additionally, the use of biometrics did not reveal the contents of the suspect's mind. Similarly, a Virginia trial court held in *Commonwealth v. Baust* that compelling a fingerprint to unlock a smart phone was like providing a key and required no mental effort on the part of the suspect.[17]

About the Author

Pierre Grosdidier is Senior Assistant City Attorney at the City of 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

---

[12] *Id.* at 805.

[13] 317 F. Supp. 3d at 535-36.

[14] *Id.* at 537.

[15] *See also In re Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, No. 1:19-mj-10441, 2019 WL 3401990, --- F. Supp. 3d ---, at *3 (D. Idaho July 26, 2019) (same).

[16] 905 N.W.2d 870, 875 (Minn. 2018) (citing *United States v. Hubbell*, 530 U.S. 27, 42-43 (2000) (subpoena for documents)).

[17] 89 Va. Cir. 267, 2014 WL 10355635, *4 (Oct. 28, 2014) (not reported in S.E.2d).

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. He was the Section's Webmaster and Circuits eJournal Co-Editor for 2018–19.

Facebook Faceoffs: Artist Fights Over Social Media Rights and The Need to Address Page Roles in Contract

By Gwendolyn Seale and John Browning

In today's world, one of the leading measures of an artist's popularity is signified by the quantity of his/her "likes" or "followers" on various social media platforms. Social media has so transformed our way of life – to the point that an entirely new occupational field has emerged, the "social media manager," becoming a fast-growing career, ranked within the top 50 of the best jobs in America according to CNN.[1] Employment recruiting site Glassdoor reports that social media managers are, on average, paid over $55,000 a year for Facebooking, Tweeting, Instagramming and Snapchatting.[2] Social media presence has even become a critical factor in establishing the strength of an artist's trademark; according to the Sixth Circuit, Facebook likes, Twitter followers and YouTube views provide important evidence for commercial strength of a mark.[3]

Social media's effects are readily apparent within the music industry. The disadvantages are obvious—artists now are forced to cultivate an impressive online presence, potentially distracting them from their craft and passion – making art, or as one acclaimed DJ and music producer describes this new phenomenon in relation to artists, "the unfortunate social media sidehustle."[4] However, social media's permeation into the entertainment industry does have its benefits – it allows an artist's fans to be able to have a closer look into the lives of the people whom they most admire. Consider, for example, Jonathan Bennett, better known as his stage persona, "Chance the Rapper." Chance branded himself and engaged with his social media audience utilizing unconventional methods –streaming all of his music for free on his social media accounts, putting together promotions and give-a-ways, and interacting with fans by

---

[1] Beth Braverman, *Best Jobs In America: 42 Social Media Manager*, CNN (May 9, 2017), http://money.cnn.com/gallery/pf/2017/01/05/best-jobs-2017/42.html.

[2] *Social Media Manager Salaries*, Glassdoor (October 16, 2017), https://www.glassdoor.com/Salaries/social-media-manager-salary-SRCH_KO0,20.htm.

[3] *Kibler v. Hall*, No. 15-2516 7-8 (6th Cir. 2016). https://law.justia.com/cases/federal/appellate-courts/ca6/15-2516/15-2516-2016-12-13.html

[4] Wolfgang Gartner, *Hashtag Blessed: Music's Unfortunate Social Media Side Hustle*, Medium (February 23, 2015), https://medium.com/cuepoint/hashtag-blessed-music-s-unfortunate-social-media-side-hustle-f5c95102758b.

producing secret shows that people could only discover if they "followed" him on Twitter.[5] These social media marketing gimmicks enabled him to cultivate an enormous following to the point that he is the first and only artist to ever be nominated for and win a Grammy without ever having sold an album.[6] And while it is interesting and entertaining to discuss the positive and negative impacts of social media on the music industry, instead, this article takes aim in a different direction—focusing on an important area in the realm of social media and the music industry that has long been neglected—the ownership of artist's social media accounts and the peril musicians face if they neglect to address social media profile ownership within a written agreement. This article addresses these issues primarily as they relate within the scope of Facebook's "Page" platform.

First, let us take a look into how Facebook's "Page" platform works and clarify some common misconceptions. Facebook refers to an individual's account as a "personal profile," while it refers to a business or product's account as a "Page."[7] If someone wants to create a Page for a band, one would click a little arrow at the top right hand corner of the webpage, and choose the "create a Page button," fill out the requisite information, such as whether the person is an artist, a band, or a public figure, and accept the terms of use.[8] Instantly, a "Page" is formed.[9] The person who created the Page is referred to as an "admin." This admin has the ability to publish content for everyone to see, can add other members to run the Page, and assign or change those members' roles.[10] These other members may be added as other admins or have other roles (see below).[11] Usually, within the context of bands, the member who created the Page will add the other members as admins, so that each person has the opportunity to post content, whether it is photos, information for upcoming shows, or music releases. Eventually,

---

[5] Ogden Payne, *Three Marketing Takeaways From Chance The Rapper's 'Coloring Book' Roll-Out*, Forbes (May 30, 2016), https://www.forbes.com/sites/ogdenpayne/2016/05/30/three-marketing-takeaways-from-chance-the-rappers-coloring-book-roll-out/#27ff493de5e1.

[6] See Id; Abagail Hess, *How this Grammy-winning artist made it big while giving his work away for free*, CNBC (February 17, 2017), https://www.cnbc.com/2017/02/13/grammy-winning-artist-made-it-big-while-giving-his-work-away-for-free.html.

[7] Aliza Sherman, *Facebook Pages, Groups and Profiles Explained*, Gigaom (January 19, 2010), https://gigaom.com/2010/01/19/facebook-pages-groups-and-profiles-explained/.

[8] Facebook Help Center, How Do I Create A Page?, https://www.facebook.com/help/104002523024878/.

[9] *Id*.

[10] Facebook Help Center, What are the different Page roles and what can they do? (October 21, 2017), https://www.facebook.com/help/289207354498410?helpref=about_content.

[11] *Id*. Graph taken from the webpage.

in a band's career, they may add managers, booking agents, or social media managers to help run their Page, and often times these additional parties will have admin control over the Page, too. It can be advantageous for a band to have a number of people helping to cultivate their social media presence – however, frequently, it presents conflicts, or as I like to call them "Facebook faceoffs" when each individual's role, as it pertains to the operation of the Page, is not clearly established and defined.

The table below outlines the 5 admin roles (across) and what they're able to do (down):

	Manager	Content Creator	Moderator	Advertiser	Insights Analyst
Manage Admin Roles	✓				
Edit the Page and Add Apps	✓	✓			
Create Posts as the Page	✓	✓			
Respond to and Delete Comments	✓	✓	✓		
Send Messages as the Page	✓	✓	✓		
Create Ads	✓	✓	✓	✓	
View Insights	✓	✓	✓	✓	✓

Over the past few years, various bands have been plagued with disasters when an admin for a Page has added or removed other admins from the Page. An aggrieved band member who has admin access to the band's Facebook Page has the ability to hijack the Page and remove the other members, keeping them from being able to have access to or control over the Page. This can be severely damaging for a band as the other members are unable to engage with the band's followers, potentially causing the band to lose the audience they worked so hard to create. There are instances in which the aggrieved band member who removed the other band members as admins believed that such action was justifiable given the fact that he/she created the account and hence, further believes him/her to be entitled to Page ownership. Additionally, the creator of the Page may feel that because of the skill utilized in bringing more followers to the Page, there is an assumption of entitlement to keeping the Page. One often sees these and similar scenarios played out when examining Facebook's Help Page and in other online forums, and neither Facebook nor any other social media platform provides any clear guidance or

suggestions as to how to resolve these Facebook faceoffs.[12] Facebook does allow members to report a page, which can result in admins losing their Page privileges. However, according to online forums, reporting a page only proves effective in cases of hacking or stolen intellectual property.[13] Some sources have stated that individuals may contact Facebook regarding these problems, however it will likely be to no avail – Facebook has no helpline, so people are left to send Facebook an email, of which they receive thousands daily.[14]

There have only been a few publicized instances of band members fighting over and getting locked out of their social media profiles, however, we have seen some similar cases in an employment law context.[15] Frequently, employees of a company will create business accounts for Facebook, Twitter, Instagram or LinkedIn and upon departure, the employee will "take the accounts," disabling the company from accessing them.[16] Companies have combated this problem by constructing social media contracts with their employees or at the very least, including provisions in their employment agreements that address ownership of social media Pages.[17] Additionally, we have also seen a case involving social media Page ownership in a television context.[18] Stacey Mattocks, an insurance agent who created a fan Facebook Page for the canceled CW show, "The Game," cultivated an enormous audience for the Page, which led

---

[12] See Facebook Business>Advertiser Help>Help Community, https://www.facebook.com/help/community/question/?id=10151380489978383; https://www.facebook.com/business/help/community/question/?id=10212858445001377; See also Emily Garman, *How to recover or claim a Facebook page that belongs to you, but someone else owns or controls, The Social Animal* (June 29, 2012), https://www.thesocialanimal.com/social-media/how-to-recover-or-claim-a-facebook-page-that-belongs-to-you-but-someone-else-owns-or-controls.

[13] Facebook Help Center, How do we get control of our corporate Facebook page?, https://www.facebook.com/help/community/question/?id=10153592085034630.

[14] Emily Garman, *How to recover or claim a Facebook page that belongs to you, but someone else owns or controls, The Social Animal* (June 29, 2012), https://www.thesocialanimal.com/social-media/how-to-recover-or-claim-a-facebook-page-that-belongs-to-you-but-someone-else-owns-or-controls.

[15] Keshia M. Tiemann, *LinkedIn Lockout: Social Media Ownership Wars Wage On*, The National Law Review (May 2, 2013), https://www.natlawreview.com/article/linkedin-lockout-social-media-ownership-wars-wage.

[16] Lisa McGrath, *Avoiding disputes over the ownership of social media accounts*, Idaho Business Review (November 18,2013), http://idahobusinessreview.com/2013/11/18/avoiding-disputes-over-the-ownership-of-social-media-accounts/.

[17] *Id.*

[18] See generally, *Stacey Mattocks v. Black Entertainment Television*, CASE NO. 13-61582 (S.D. Fl. Aug. 20. 2014). https://www.scribd.com/document/237340678/Mattocks-Bet.

BET to revive the show.[19] By the time BET aired the show, the Page had 750,000 "likes," at which point BET offered Mattocks a job to work as a social media freelancer.[20] Mattocks declined and disagreements between the two parties ensued – the account was at one point deactivated by Facebook and later restored.[21] Eventually, Mattocks signed a letter agreement with BET to work as a social media freelancer and the agreement clarified access and admin rights with regards to the Page.[22] Shortly after, the parties' relationship fell apart and Mattocks diminished BET's Page role to a lesser role, at which point BET responded with a cease and desist letter to Mattocks.[23] Mattocks thereafter sued BET, claiming conversion, tortuous interference, breach of contract, along with other claims.[24] The Court ruled against Mattocks, stating that she could not establish a property interest in the "likes" for the Page.[25] Mattocks appealed, and eventually, both parties settled.[26]

As noted previously, there is only one case that discusses band disputes over a Facebook Page which comes as an unpublished decision out of the Fifth Circuit last year, *Emerald City Mgmt. v Kahn*.[27] This case involved an appeal of a preliminary injunction by Kahn, in which he was ordered to transfer the Facebook Page for a cover band, "Downtown Fever" to Emerald City Management.[28] Kahn, while in college, formed a band called "Downtown Fever" which grew in popularity around the country.[29] Emerald City Management contacted Kahn, asking him to move to Dallas and to craft a new Downtown Fever band and become Emerald City Management's Director of Operations.[30] Soon after Kahn joined the Emerald City Management team, Emerald City, without Kahn's knowledge, registered the trademark, "Downtown Fever" in its name.[31] Kahn eventually left Emerald City, and continued to use the Downtown Fever name

---

[19] Eriq Gardner, *BET Wins Legal War Over Fan's Facebook Page (Exclusive)*, The Hollywood Reporter (August 20, 2014), http://www.hollywoodreporter.com/thr-esq/bet-wins-legal-war-tv-726594.

[20] *Mattocks supra note 18*, at 2-5.

[21] *Id*.

[22] *Id*.

[23] *Id*.

[24] *Id*. at 1-2.

[25] *Id*. at 14-15.

[26] Kelly Knaub, *BET Settles Fight Over Who Owns Facebook 'Likes',* Law360 (April 26, 2016), https://www.law360.com/articles/788836.

[27] See generally, *Emerald City Management v. Kahn*, No. 15-40446, (5th Cir. 2016). http://www.ca5.uscourts.gov/opinions%5Cunpub%5C15/15-40446.0.pdf.

[28] Id. at 1.

[29] Id at 2-3.

[30] *Id*.

[31] *Id*.

and Facebook Page.[32] Emerald City responded by filing suit for trademark infringement and other business torts, seeking a preliminary injunction and temporary restraining order to stop Kahn from using the Downtown Fever mark and to return control of the Downtown Fever social media accounts to Emerald City.[33] The district court granted the preliminary injunction; however, it did not order Kahn to transfer the Downtown Fever Facebook Page to Emerald City.[34] Kahn thereafter deactivated the Downtown Fever Page so that no one could view the Page.[35] Emerald City responded with another application for injunctive relief, on the basis of the Lanham Act—claiming that by deactivating the account, the Downtown Fever Facebook audience might believe that the band disbanded.[36] The district court removed the matter to the magistrate judge who held a hearing on this issue.[37] Emerald City presented evidence that another employee created the Page and added Kahn as an admin, and that Kahn had "locked out" Emerald City from the account,[38] presumably by removing any of Emerald City's employees as admins. At the conclusion of the hearing, the magistrate judge issued a report to the district court which recommended that Kahn reactivate the Downtown Fever Page so that he could transfer control of the Page to Emerald City and prevent Kahn from accessing or changing the Page,[39] presumably by removing him as an admin. The district court accepted the report without further discussion and ordered Kahn to turn over the Downtown Fever Facebook Page to Emerald City.[40] So, in this appeal, Kahn argued that the preliminary injunction was granted erroneously and that in order to grant a preliminary injunction based on the Lanham Act, the plaintiff must show the "use in commerce" of a mark and that deactivating an account cannot constitute a "use in commerce" of a mark.[41] The Court of Appeals agreed, stating that "neither shutting down a Facebook account nor blocking administrator access to a Facebook account constitutes "a use in commerce" of a trademark," and vacated the preliminary injunction.[42] Unfortunately, neither the district court nor the Fifth Circuit adequately addressed actual ownership of the account.

---

[32] *Id.*
[33] *Id.*
[34] *Id* at 3.
[35] *Id.*
[36] *Id.*
[37] *Id.* at 3–4.
[38] *Id.*
[39] *Id.* at 4.
[40] Id. at 4–5.
[41] Id. at 5.
[42] Id. at 6–7.

Since Facebook does not offer a procedure by which people can successfully dispute admin problems and since courts have provided virtually no assistance on these issues, it is the responsibility of artists and their lawyers to preemptively address such potential disputes through written agreement. If a band has formed a LLC, it is essential to make certain that within their Company Agreement that it delineates each member's role as it pertains to social media accounts. It may even be advisable to have the LLC own the social media profiles, so that if a member leaves or is expelled, he cannot legally take the social media property with him. And if a band does not have a formalized business entity, at the very least, it should have a written partnership agreement, within which there should be a provision inserted that a band member may have admin control over social media Pages for as long as he/she continues to be a member of the band. If a band decides to hire a manager, other agent or a social media manager, one must make certain to include language within those contracts that states that these parties do not own the band's social media accounts. With regards to Facebook, it is important to designate the person as a content creator, as opposed to an admin, so these individuals never have the opportunity to hijack the Page. And by taking these preventative measures, band members can focus on creating art, instead of facing Facebook face-offs.

About the Authors

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.

John 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.

Facebook's Libra: What is all the Fuss About?

By Ronald Chichester

1. Introduction

On May 24, 2019, Facebook announced that it was going to launch a new cryptocurrency called "Libra" that is powered by the "Libra Blockchain."[1] Instead of direct sponsorship, Facebook took a cue from the open source community and created a separate foundation, called the Libra Association.[2] In conjunction with the announcement, Facebook (through the foundation) published the obligatory white paper[3] as well as a developer's guide[4] and a "testnet"[5] that can be used to test code using a for-purpose language called "Move."[6]

The news spread throughout the world, generating wildly differing opinions, from the pessimistic[7] to the euphoric.[8] Some wonder if Libra might be a competitor to fundamental governmental functions.[9] Others thought Libra might be akin to a multi-headed Hydra striking

---

[1] Chan, S. (2019). *Facebook plans to launch crypto-currency*. [online] BBC News. Available at: https://www.bbc.com/news/business-48383460 [Accessed 13 Aug. 2019].

[2] *See*, https://libra.org/en-US/

[3] *Libra White Paper: Blockchain, Association, Reserve*, The Libra Association (2019), https://libra.org/en-US/white-paper/ (last visited Aug 15, 2019). See also, An Introduction to Libra. (2019). [ebook] Libra Association. Available at: https://libra.org/en-US/white-paper/ [Accessed 13 Aug. 2019].

[4] *See,* https://libra.org/en-US/open-source-developers/

[5] *Id*.

[6] MOVE: A LANGUAGE WITH PROGRAMMABLE RESOURCES, The Libra Association, https://developers.libra.org/docs/move-paper (last visited Aug 15, 2019).

[7] Timothy B. Lee, THERE'S A BIG PROBLEM WITH FACEBOOK'S LIBRA CRYPTOCURRENCY, Ars Technica (2019), https://arstechnica.com/tech-policy/2019/07/facebooks-half-baked-cryptocurrency-libra-explained/ (last visited Aug 15, 2019); Binoy Kampmark, FACEBOOK, FUNNY MONEY AND LIBRA, Counter Punch (2019), https://www.counterpunch.org/2019/07/04/facebook-funny-money-and-libra/ (last visited Aug 15, 2019); Adam Levitin, LIBRA AND FINANCIAL INCLUSION CREDIT SLIPS (2019), https://www.creditslips.org/creditslips/2019/07/libra-and-financial-inclusion.html (last visited Aug 15, 2019) ("Libra is a payment system and that is why it will likely fail.")

[8] Huw van Steenis, TO SUCCEED, LIBRA MUST PROVE ITSELF IN THE INDIAN MARKET, Financial Times (2019), https://www.ft.com/content/5c77d442-ad40-11e9-b3e2-4fdf846f48f5?segmentid=acee4131-99c2-09d3-a635-873e61754ec6 (last visited Aug 15, 2019).

[9] *See, e.g.*, Charles Hugh Smith, COULD A CRYPTOCURRENCY BECOME A GLOBAL RESERVE CURRENCY?, Of Two Minds Blog (2019), http://charleshughsmith.blogspot.com/2019/06/could-cryptocurrency-become-global.html (last visited Aug 15, 2019); *See also*, Tyler Durden, "GAME CHANGER" – IS LIBRA THE TROJAN HORSE FOR AN SDR-BACKED REDESIGN OF THE GLOBAL FINANCIAL SYSTEM?, Zero Hedge (2019),

fear in governments, who promptly conducted hearings,[10] made calls for regulation,[11] and filed bills[12] that caused the Libra Association to backtrack on its ambitions (somewhat) and giving rise to some rather plausible conspiracy theories.[13] Another group of critics, citing Facebook's recent privacy scandals,[14] decried the privacy abuses made possible by the standardized identity required by Libra and what surveillance tools Libra would provide to corporations and totalitarian regimes.[15] The mainstream media, always in tune with government, claimed that

---

https://www.zerohedge.com/news/2019-06-27/game-changer-libra-trojan-horse-sdr-backed-redesign-global-financial-system (last visited Aug 15, 2019).

[10] Slashdot, Facebook Backpedals From Its Original Ambitious Vision for Libra (2019), Slashdot, https://tech.slashdot.org/story/19/07/19/2349224/facebook-backpedals-from-its-original-ambitious-vision-for-libra?utm_source=rss1.0mainlinkanon&utm_medium=feed (last visited Aug 15, 2019); and Watch Live: Senate Grills Facebook Crypto Head About "Libra" Digital Currency, Weather Internal (2019), https://weatherinternal.com/watch-live-senate-grills-facebook-crypto-head-about-libra-digital-currency/ (last visited Aug 15, 2019).

[11] Bloomberg, Facebook and bitcoin must face banking rules, says Trump, South China Morning Post (2019), https://www.scmp.com/news/world/united-states-canada/article/3018271/donald-trump-blasts-bitcoin-facebooks-libra-demands (last visited Aug 15, 2019).

[12] New US House Bill Would Ban Big Tech From 'Banking', Fine Facebook's Libra $1 Million Per Day, Zero Hedge (2019), https://www.zerohedge.com/news/2019-07-15/new-us-house-bill-would-ban-big-tech-banking-fine-facebooks-libra-1-million-day (last visited Aug 15, 2019). *See also,* Slashdot, US Lawmakers Consider Ban On Big Tech Companies Launching Cryptocurrencies, Slashdot, https://news.slashdot.org/story/19/07/15/0019215/us-lawmakers-consider-ban-on-big-tech-companies-launching-cryptocurrencies?utm_source=rss1.0mainlinkanon&utm_medium=feed (last visited Aug 15, 2019).

[13] Tyler Duran, Who In The World Is Most Interested In Facebook's Libra (It's Not Who You Think), Zero Hedge (2019), https://www.zerohedge.com/news/2019-07-18/who-world-most-interested-facebooks-libra-its-not-who-you-think (last visited Aug 15, 2019). *See also,* Edward Playfair, Is Libra the West's response to China's payments empire?, Three Body Capital (2019), https://threebody.capital/blog/2019/6/29/is-libra-the-wests-best-response-to-chinas-payments-empire (last visited Aug 15, 2019).

[14] *See, e.g.,* James Sanders, Facebook data privacy scandal: A cheat sheet, TechRepublic (2019), https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/ (last visited Aug 15, 2019).

[15] *See, e.g.,* Bill Black, Facebook's Libra Currency Monetizes Identity and Threatens Privacy, The Real News Network (2019), https://therealnews.com/stories/facebooks-libra-currency-monetizes-identity-and-threatens-privacy (last visited Aug 15, 2019). *See also,* Inside the Congressional Staff Meeting About Libra, The American Prospect (2019), https://prospect.org/article/inside-congressional-staff-meeting-about-libra (last visited Aug 15, 2019).

terrorists might use Libra for nefarious purposes.[16] The technical community, on the other hand, was overjoyed with all the new (free and not-so-free) goodies bestowed upon them.[17]

Speculation went on for weeks. I deliberately let time pass before finishing this article (much to the consternation of my editors). So in the intervening period, have we found ourselves closer to a consensus? Not necessarily. Libra has been bent somewhat, but not broken. The mainstream media has moved on, which either means that the serious work of development has begun, or that the serious work of development will *never* begin. Time will tell.

2. What is Libra?

According to the Libra Foundation:

> "The Libra Blockchain is a decentralized, programmable database designed to support a low-volatility cryptocurrency that will have the ability to serve as an efficient medium of exchange for billions of people around the world. We present a proposal for the Libra protocol, which implements the Libra Blockchain and aims to create a financial infrastructure that can foster innovation, lower barriers to entry, and improve access to financial services. To validate the design of the Libra protocol, we have built an open-source prototype implementation — *Libra Core* — in anticipation of a global collaborative effort to advance this new ecosystem."[18] (emphasis supplied.)

The Libra Association is made up of a set of corporations called partners.[19]

---

[16] Kate Rooney, MNUCHIN: US HAS 'VERY SERIOUS CONCERNS' THAT FACEBOOK'S LIBRA COULD BE MISUSED BY TERRORISTS, CNBC (2019), https://www.cnbc.com/2019/07/15/treasury-secretary-mnuchin-will-hold-a-news-conference-on-cryptocurrencies-at-2-pm-et.html (last visited Aug 15, 2019).

[17] Binoy Kampmark, FACEBOOK, FUNNY MONEY AND LIBRA, Counter Punch (2019), https://www.counterpunch.org/2019/07/04/facebook-funny-money-and-libra/ (last visited Aug 15, 2019) ("Facebook's Libra cryptocurrency generated more than a smattering of interest last month when its early-access code made its way to GitHub. By the end of the month, it had been "saved" by some 10,000 users, while a 1,000 clones of the codebase were also generated, very much in a playful effort to test its reliability.")

[18] https://developers.libra.org/docs/the-libra-blockchain-paper

[19] https://libra.org/en-US/partners/

Figure 1: Some of the Libra Association Partners. Image from the Libra Association website.

The partners provide the financial and technical backing for the Libra Blockchain and its attendant infrastructure. In short, Libra is a cryptocurrency and smart contract platform that allows someone to buy or sell things with nearly zero transaction fees — worldwide, by leveraging the user-base of Facebook[20] and its subsidiaries such as WhatsApp.[21] This puts Libra squarely in competition with credit card companies such as Visa and MasterCard — which charge hefty usage fees on each transaction — as well as with banks dealing predominantly with national currencies. Interestingly, some of those very same organizations are partners in

[20] https://www.facebook.com/

[21] https://www.whatsapp.com/

the Libra Association. Facebook's financial and technical backing has catapulted the Libra Blockchain to the forefront of programmable blockchains such as frontrunner Ethereum.[22]

3. Why the Fuss?

Because of the size of Facebook's international user-base (estimated at 2.4 billion[23]) and, because Facebook intends for Libra to be based on a variety of hard assets, users should feel confident in the integrity of this cryptocurrency. However, according to the Libra Association documents, the "money in the reserve will come from two sources: commitments by members and users of Libra."[24] Moreover,

> "The association will pay out incentives in Libra coin to Founding Members to encourage adoption by users, merchants, and developers. On the user side, for new Libra coins to be created, there must be an equivalent purchase of Libra for fiat and transfer of that fiat to the reserve. Hence, the reserve will grow as users' demand for Libra increases. In short, on both the investor and user side, there is only one way to create more Libra — by purchasing more Libra for fiat and growing the reserve."[25]

In other words, Libra is not going to be backed by hard assets. Rather, it will be backed by a basket of fiat currencies, and thus itself is an example of a derivative fiat currency.

Finances aside, another major issue with the Libra Blockchain is its *design*. The design of a blockchain belies indelibly the intent of its creators. Blockchains implement a "trust paradigm."[26] Bitcoin[27] is an example of a publicly-available, decentralized, permission-less blockchain based on open source software.[28] In other words, anyone who has access to the Internet can download the software and run it on their own hardware (thereby becoming a "node" in that parlance) – without seeking someone's permission. In addition, the Bitcoin protocol does not require knowing the identity of the individuals conducting transactions in Bitcoin.

---

[22] https://www.ethereum.org/

[23] *See, e.g.,* J. Clement, FACEBOOK USERS WORLDWIDE 2019, Statista (2019), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited Aug 15, 2019).

[24] https://libra.org/en-US/about-currency-reserve/#the_reserve

[25] *Id.*

[26] *See, e.g.,* Kevin Werbach, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (2018).

[27] https://www.bitcoin.org

[28] The bitcoin software is available at https://github.com/bitcoin/bitcoin

In contrast to the Bitcoin example, "[t]he Libra protocol allows a set of replicas — referred to as validators — from different authorities to jointly maintain a database of programmable resources."[29] The software underlying the Libra Blockchain may be free, but the *implementation* of that software requires permission from an authority, namely a Partner with the Libra Foundation. Furthermore, the identity of the individual using Libra will be absent from the transaction ledger, but will be ascertainable via the user's account information with the respective Partner.[30] By restricting the number and location of the replicas (nodes), the Libra Association regulates the infrastructure underlying the Libra Blockchain, and thus regulates access to the Libra Blockchain only to individuals known via their accounts associated with the respective Libra Association Partners.

4. Conclusion

Libra is not a cryptocurrency in the way that most individuals would consider. Unlike Bitcoin, Libra will be centralized among a pre-selected set of Partners. Libra will not provide its users with anonymity, and the Libra Association has made it clear that it will cooperate with law enforcement agencies should the need arise to track the enablers of a transaction. "In simple terms, Libra is just a new brand for old products: Digital gift cards and pre-paid debit cards"[31] — with less anonymity, and the value of which will fluctuate differently from that of any particular national (fiat) currency. Perhaps the greatest compliment bestowed upon Libra, however, came from the current Governor of the Bank of England, Mr. Mark Carney, who suggested that a Libra-*like* currency (but not Libra itself) should be used to eliminate the dominance of the U.S. dollar as the world reserve currency.[32]

---

[29] *See* Compliance & Consumer Protection: Libra, LIBRA.ORG, https://libra.org/en-US/compliance-consumer-protection/#overview (last visited Aug 15, 2019).

[30] *Id.*

[31] Thomas Knapp, FACEBOOK'S LIBRA ISN'T A "CRYPTOCURRENCY", Counter Punch (2019), https://www.counterpunch.org/2019/06/24/facebooks-libra-isnt-a-cryptocurrency-2/ (last visited Aug 15, 2019).

[32] Brian Swint, CARNEY URGES LIBRA-LIKE RESERVE CURRENCY TO END U.S. DOLLAR DOMINANCE, Bloomberg (Aug. 23, 2019), https://www.bnnbloomberg.ca/carney-urges-libra-like-reserve-currency-to-end-dollar-dominance-1.1306107 (last visited Sept 3, 2019).

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.

Into the Data Breach: The Hit or Miss Patchwork of U.S. Cybersecurity Law

By Jeffrey D. Hunt

"*Data breach exposes personal data of millions*" has been a common news headline since 2005. Even as I write this article in mid-August, the lead story on CNN.com is *"Ransomware Attacks Cripple Cities Across America."* These high-profile events receive robust media coverage, but the responsible hackers are seldom brought to justice. Even then, the hackers facing prison are judgment-proof. The staggering financial losses fall to corporations and their insurers, and unfortunate individual consumer victims may suffer identity theft. What are best practices for companies to manage risks? Who faces real exposure and is most likely to be pursued by government enforcement actions and civil lawsuits? Does anyone face criminal liability? How should one advise directors and officers of corporations that may be hacking targets? Is compliance with data breach notification laws in various states sufficient to protect the interests of the company? How about protection and claims of consumers?

Data security and data breaches form part of the general subject of "cybersecurity." Attacks to take down services, systems and websites lay within the cybersecurity realm. Ransomware attacks that lock out system owners and users are other significant crimes in this area. Hacking electricity grids and other infrastructure to interrupt control is an emerging threat. The umbrella term "cybersecurity" refers to security efforts, and breaches, for systems that handle and store data. Unauthorized access typically results in improper use, disclosure, copying, or destruction of the protected data, or improper control of networks, computers or IoT devices. The data may be personal information, business information, or governmental information. Despite the rise of numerous threats, no integrated federal statutory scheme exists to govern cybersecurity practices and liability. Private causes of action are limited. A series of negative headlines reporting that major companies have delayed reporting mass breaches of consumer data have prompted more than 20 states to enact laws in various forms, requiring timely notification of some data breaches. Although a number of notification bills have been introduced in Congress, no legislation has been enacted at the federal level, either to require timely notification of data breaches or establishing a uniform federal law governing cybersecurity. A hodgepodge of laws is finding application to different aspects of cybersecurity. This article reviews laws on the subject from the perspective of advising business clients in Texas.

Companies doing business in Texas face potential criminal and civil liabilities, *when their systems are breached by hackers*, if they fail to comply with statutory requirements to notify

persons impacted by the breach in a timely manner. More than twenty-five (25) states, including Texas, have enacted security breach notification laws. *See*, Tex. Bus. & Com. Code 521.002, 521.053. The Texas statute broadly applies to any entity that conducts business in Texas, and owns or licenses computerized data including sensitive personal information (PI). A security breach occurs where the security, confidentiality or integrity of sensitive PI maintained by such an entity is compromised, or is believed to have been compromised, by acquisition of data by an unauthorized person. In the event of a security breach, the entity suffering breach is obligated to provide timely notification (within 60 days from discovery) to affected persons, whether residents of Texas or non-residents. Where 10,000 or more persons are impacted, the entity also must notify credit reporting agencies. Failure to comply may give rise to harsh penalties or fines. The Texas Attorney General is tasked with enforcement of the notification statute, and may seek injunctive relief and substantial penalties up to $250,000 against the business that suffered the breach. The Texas statute does not provide a private cause of action for affected persons. Texas law was strengthened by amendment, so that from January 1, 2020 entities suffering breach also must notify the Texas Attorney General, when 250 people in Texas are impacted. Where a Texas company conducts business in other states and suffers a data breach, compliance with different notification laws of those states also may be required. Compliance with the Texas statute will be deemed sufficient to satisfy some of the other states.

Two sources of civil remedies should be considered where Texas businesses seek to recover from hackers for system breaches. One is a state civil law, the Texas *Harmful Access by Computer Act,* Tx Civ Prac & Rem § 143.001 *et seq*. (HACA). The HACA provides a civil cause of action for certain breaches of a parallel state criminal law titled *Breach of Computer Security,* Tex. Penal Code Chap. 33, Sec. 33.02 (BCS). The second source is the granddaddy of Federal cybersecurity laws, the *Computer Fraud and Abuse Act of 1984* (CFAA) 18 U.S.C. §1030, discussed below, which creates both criminal and civil liability but is notorious for its' complexity.

The Texas HACA has been used successfully by plaintiff businesses against hackers, who may have been either outsiders or insiders to the victimized business. Civil liability arises under *HACA* where a defendant has breached the BCS criminal statute, and her criminal violation is knowing or intentional. The BCS criminal statute is breached by a person knowingly accessing a computer without effective consent of the owner. The offense typically is a misdemeanor (default) but ranges to a felony where a pattern of violations exists, or where the computer belongs to government or relates to critical infrastructure. The BCS also is breached by

knowingly accessing a computer with intent to obtain a stored file, data or proprietary information to defraud or do harm, or to alter, damage, or delete property, either without effective consent of the owner, or where the computer belongs to government or business and in violation of a conspicuous prohibition or express contractual agreement.

The existence or non-existence of "effective consent" is a recurring question in cases under the BCS and HACA. For example, effective consent did not exist for automated scraping of information from the Southwest Airlines website by an airfare information service, because the website Terms of Use prohibited such activity. *Southwest Airlines Co. v. Farechase, Inc.,* 381 F.Supp.2d 435, 442-32 (N.D. Tex. 2004). Another issue subject to dispute is the occurrence or non-occurrence of injury to person or property, as required for civil liability to arise under *HACA*. See, *TrueBeginnings, LLC v. Spark Network Services, Inc.*, 631 F.Supp.2d 849 (N.D. Tex. 2009). Former employees accessing valuable business data without authorization is frequently pursued under HACA.

The *Computer Fraud and Abuse Act of 1984* (CFAA) 18 U.S.C. §1030, as broadened by amendments over the years, is the primary Federal cybersecurity law. The CFAA broadly prohibits intentionally accessing a protected computer without authorization, or in excess of authorization. The CFAA effectively criminalizes hacking, denial of service (DDoS) attacks, delivery of malware, identity theft, and electronic theft or espionage such as trafficking in stolen passwords. In addition to imposing criminal penalties, the CFAA also creates private causes of action that have been employed by companies pursuing former employees for theft of trade secrets.

Authorities have brought criminal cases under the CFAA for a range of activities. In *United States v. Collins et al.,* (ND Cal. 2011) hackers associated with the Anonymous hactivist collective were charged for their efforts to shut down PayPal in protest of Paypal's decision to end payment processing for Wikileaks. A group of individuals labeled the PayPal 14 settled with the Department of Justice (DOJ), pleading guilty to misdemeanors and each owing a substantial fine.

Another criminal case, *United States v. Swartz*, alleged 13 counts under the CFAA against widely-admired MIT Research Fellow and Internet activist Aaron Shwartz, who was accused of downloading virtually an entire catalog of academic research publications in order to provide open access to them, outside a paywall. The case against Shwartz has been extensively criticized as heavy handed in seeking a 35-year prison sentence where the defendant asserted his First Amendment rights, and ended with the defendant's death by suicide. The Shwartz

case led to Congressional hearings and introduction of Aaron's Law intended to amend the CFAA to curtail government aggression against activists, although passage of the amendment failed. The tragic circumstances led to debate and better understanding that the government and prosecutors are in a position to overreach against individuals expressing unpopular views using the CFAA, which was originally intended to punish hacking for criminal purposes such as financial fraud.

Companies have sued third parties, such as former employees, for actions alleged to violate the CFAA. In one case, Craigslist sued upstart competitor 3Taps to stop 3Taps from accessing Craigslist's classified advertisements, without authorization to scrape information from the Craigslist ads. *Craigslist v. 3Taps,* 942 F.Supp. 2nd 962, NDCA 2012) In another case, *Facebook, Inc. v. Power Ventures, Inc*., 844 F.3d 1058 (9th Cir. 2016), the Ninth Circuit affirmed that even with individual authorization and individual Facebook login credentials being provided by Facebook users who sought to utilize Power Ventures' services to scrape and compare their data across multiple social media websites, the CFAA imposed civil liability for evading Facebook's express prohibition against Power Ventures accessing the Facebook website.

Overbroad application of the CFAA, however, is subject to increasing criticism. The American Civil Liberties (ACLU) and Electronic Frontier Foundation (EFF) are leading efforts to reform the CFAA, to prevent prosecutors and companies from seeking to penalize conduct prohibited by private agreements such as website terms of service. Much of the criticism arises from claims brought against researchers using automated tools to access and scrape information from websites, where the website owner has established restrictive, private terms of service in attempts to thwart research performed in this manner. The ACLU is providing representation in a pending case, for a plaintiff suing the Department of Justice, seeking a ruling that the First Amendment grants researchers the right to provide false information to websites, when testing business practices of the website operators for discrimination in violation of civil rights laws. See, *Sandvig v. Barr* (Case No. 1:16-cv-1368, Dist. Delaware). Similar testing in person is an accepted way of proving discrimination, so that criminalizing analogous conduct via the Internet, for the same purpose, would have a chilling effect on speech.

These are the sources of law most likely to be employed in cybersecurity disputes in Texas. Various other statutes may find application. These include Title 18 of the United States Code including Sections 1028 & 1028A criminalizing identity theft; Section 1029 for device fraud such as phishing; Section 2701 (Stored Communications Act) prohibiting theft of stored

communications, such as emails; the Wiretap Act; the CAN-SPAM Act; and the Electronic Communications Privacy Act (ECPA).

About the Author

Jeffrey D. Hunt is partner and co-founder of Hunt Pennnington Kumar & Dula Pllc, in Austin. He practices in the areas of Intellectual Property and Estate Planning. Jeff assists entrepreneurs, tech companies, investors, and inventors with legal strategies for protecting their technologies and brands from unauthorized use and copying. Jeff's clients have included companies in the fields of: financial technology, energy exploration and production, heavy mechanical equipment, software, computing and networks, communications, wireless, video processing, surveillance, medical devices, healthcare, materials science, chemicals, textiles, marine products, water processing, printing, and consumer products. Jeff is licensed to practice law in Texas and before the United States Patent and Trademark Office. He holds degrees in law, business, and engineering from Vanderbilt University.

Ghosts in the Machine: Algorithmic Bias and the Courts

By John G. Browning and Alex Shahrestani

I. INTRODUCTION

When asked if he could foresee a day "when smart machines, driven with artificial intelligence, will assist with courtroom fact-finding or, more controversially even, judicial decision-making," U.S. Supreme Court Chief Justice John Roberts gave a startling response. He said "It's a day that's here and it's putting a significant strain on how the judiciary goes about doing things."[1] And despite how many might reserve the notion of using technology to predict an individual's likelihood to commit crimes for dystopian science fiction movies like Steven Spielberg's *Minority Report*, the simple truth is that it is already here. In many ways, much of our modern lives is already impacted by machine learning—the intelligent algorithms underlying the artificial intelligence revolution that already determines everything from Facebook newsfeeds and Google search results to Netflix viewing and online shopping recommendations. Algorithms can also help determine whether we get approved for a mortgage or a job interview, as well as what penalties we face if we commit a crime.

But while the success and widespread use of intelligent algorithms have led many to adopt a "numbers do not lie" attitude and imbue such machine learning with what researchers Osonde Osoba and William Wesler IV describe as an "aura of objectivity and infallibility,"[2] the truth is that certain algorithms utilizing machine learning tools do mimic human biases. And while the shortcoming of some built-in bias—the lingering "ghost in the machine" unconsciously left by a programmer—may seem trivial when the consequences are limited to online dating matchups, it becomes far weightier when crime and punishment are concerned. Skewed input data, imperfect or false logic, or just the prejudices of their programmers can result in intelligent algorithms responding (and in some cases, amplifying) human biases.

In the justice system, a number of legal challenges to algorithmic bias in various contexts have already taken place. In the employment arena, the Houston public school teachers union challenged the use of proprietary algorithms for school employment practices. Facebook

---

[1] Adam Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, N.Y. TIMES (May 1, 2017), https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html.

[2] Osonde A. Osoba & William Wesler IV, *The Risks of Bias and Errors in Artificial Intelligence*, *in* INTELLIGENCE IN OUR IMAGE (Osoba & Wesler 2017).

settled an Equal Employment Opportunity Commission (EEOC) complaint alleging that Facebook enabled gender and age-based discrimination in hiring practices through the use of the social networking platform's ad-targeting features, which allowed for job postings to be displayed to audiences narrowed by age and gender. Minorities disproportionately impacted by credit and mortgage lending decisions have brought lawsuits alleging algorithmic bias. In the case *K.W. v. Armstrong*, the American Civil Liberties Union (ACLU) of Idaho brought a class action lawsuit on behalf of about 4,000 individuals with developmental and intellectual disabilities challenging the state's use of a "black box" algorithm to make Medicaid benefits determinations.[3]

This article, however, will focus on algorithmic bias in the criminal justice context. We will begin with an introduction to how such machine learning works generally, as well as a look at the types of algorithmic bias. The article will then examine some examples of algorithmic bias, from the "predictive policing" initiatives of cities like Chicago and Oakland, to challenges to algorithmic bias in cases like 2016's *State v. Loomis*. Finally, we will discuss some of the proposed measures to combat algorithmic bias, including federal legislation like the Algorithmic Accountability Act. Overall, as we shall see, an intelligent algorithm is only as good as the data it learns from. Machine learning on inherently biased data cannot help but lead to biased results.

II. HOW MACHINE LEARNING WORKS

When you were a baby, just learning how to talk, you observed thousands of conversations. You noticed that there was a cadence to the sounds being expressed, you noticed that some of those sounds were repeated over and over again, and you learned your first words. After thousands of hours of training, you pumped out a single word. From there, you probably started trying to string together "sentences" in a series of meaningless babbling, with an occasional coherent word thrown in. The sentence did not achieve the desired outcome, and you tried again. Over time and much trial and error, you learned to talk.

Machine learning works in much the same way. A program attempts to achieve an outcome by modeling its outputs against the data you provide it. To carry the analogy forward, you provide the program with thousands of hours of speech recordings for it to listen and model itself

[3] K.W. v. Armstrong, 789 F.3d 962 (9th Cir. 2015). And for a useful look at algorithmic bias in employment law, see McKenzie Raub, *Bots, Bias, and Big Data: Artificial Intelligence, Algorithmic Bias, and Disparate Impact Liability in Hiring Practices*, 71 ARK. L. REV. (2018).

after. The program tries to match cadence with meaning, and it eventually "learns" to synthesize speech.

However, imagine that instead of providing the program with thousands of hours of actual speech recordings, you provided the program with mostly speech recordings, but maybe a quarter of the recordings were of chattering monkeys. As far as the computer is concerned, all of the recordings are equally valid, so it will attempt to model its synthesized speech after the entirety of the recordings, resulting in sentences that include the occasional monkey-based vocalization or "speech" structure. This would be an obvious error to any person listening to the synthesized speech, but the use of machine learning is often to remove the need for an individual to interact with the data: the program is likely to go on and on synthesizing monkey sounds into the outputs long before anyone notices.

This can lead to many problems when the machine learning tool is responsible for important decisions: (1) whom should receive a job interview ; (2) whom should receive loan money ; (3) what stocks to invest in; or (4) whom should be sent to jail. All of those listed use cases to rely on the data fed into it, and the data can be problematic for a few reasons.

III. TYPES OF MACHINE LEARNING BIAS

There are various kinds of machine learning bias; or rather, there are various ways in which machine learning bias manifests itself. As a result there are three avenues by which machine learning bias can occur, and therefore must be addressed.

A. Pre-Existing

Pre-existing machine learning bias is the codification of already-present biases. If a system designer has a real prejudice that he/she wants to implement into a technological solution, that would be an instance of pre-existing machine learning bias. Another such instance would be the inclusion of an implicit bias into the system, something that the system designer is not cognizant of as a cause of discrimination. Pre-existing machine learning bias means a bias that would exist regardless of the machine learning solution, but the machine learning incorporates that bias into its processes.

B. Technical

Technical machine learning bias is the bias that occurs due to the technical limitations of actually presenting the data. If an employer is presented top candidates for a position in a structured order not based on scoring, then candidates are either going to be advantaged or disadvantaged - the first name on a list of top candidates will have a significant advantage

over those at the bottom of the list. Another example could be that the data gathering mechanism is most robust on the most advanced phones on the market, and the others have a reduced data-set. Technical bias problems reflect a serious difficulty in being objective in presenting results.

C. Emergent

Emergent machine learning bias is the development of new biases or new understandings of biases as technology develops. For example, if audiobooks became so popular a method of consuming literature that published books were made obsolete, then the deaf population would be negatively impacted. A different example would be the development of a new trend in society that has not been accounted for in creating processes for sorting big data—such as a demographic survey not reflecting third options for gender identifiers following a changing social awareness around gender identities.

IV. ALGORITHMIC BIAS IN THE COURTS

A. Predicting Risk

Using mathematics to guide decision-making in the criminal justice system is hardly a new phenomenon. As far back as the 1920s, the Illinois parole board used mathematical tabulations that assessed risk by comparing people up for parole to offenders who had already been released. But while the mathematics behind those tools has improved and statisticians can now grapple with far greater data sets using computers, the problem of inherent bias remains — particularly in the use of predictive analytics. For example, in 2016, the independent investigative journalism project ProPublica studied the "risk scores" and assessments of Northpointe, Inc.—the Michigan-based company behind the Correctional Offenders Management Profiling for Alternative Sanctions (COMPAS)—for 7,000 people who were arrested in Broward County, Florida.[4] These scores are used to determine release dates and bail, since they supposedly predict the defendant's likelihood to commit a crime again. In the cases investigated, ProPublica maintains the algorithms wrongly labeled African American defendants as future criminals at a rate nearly twice (43% vs. 23%) that of white defendants (who were far more likely to be labeled as "low risk" than black defendants). ProPublica's study also found that the COMPAS algorithm was 61% predictive of re-arrest, or "somewhat more accurate than a coin flip." In addition, only 20% of the people predicted to commit violent crimes actually went on to do so. Besides just the errors alone, ProPublica found the software

[4] Jeff Larsen et al., *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

to be biased against African Americans, with blacks given what would appear to be an inflated risk score despite the input of facts suggesting the opposite. In one case, an African American woman with four juvenile misdemeanors was given a score of 8, while a white male with 2 armed robberies and an attempted armed robbery was assessed a score of just 3. While ProPublica's thought-provoking finding generated considerable media attention and raised many questions, it could only go so far due to a persistent issue with such algorithms: transparency. Unable to analyze the algorithm itself because its corporate owners refused to release the code, ProPublica could only rely on input and output data.

A study involving the City of Oakland provides another look at algorithmic bias. In 2016, the Human Rights Data Analysis Group investigated PredPol, an algorithm already in use in several states and designed to predict when and where crimes will take place. Its analysis found that rather than accurately predicting crime, the algorithm exacerbated past racially biased policing practices by leading police to target certain neighborhoods. Applying the algorithm to drug offenses in Oakland, California, the study found that officers were repeatedly sent to predominantly black neighborhoods—areas disparately overrepresented in prior arrest data. PredPol responded that this was merely training data, and that in real world applications the software is not used to predict drug crime.

The Chicago Police Department (CPD) has also turned towards a predictive policing initiative in order to reduce gun violence.[5] It is using a technology that takes various, unknown factors into account, runs those factors through an algorithm, and scores people as part of a "heat list." Oftentimes, those on the heat list are then directly contacted by the CPD to notify them that they are on the CPD's radar as people to watch. The people on the heat list are either invited to a community meeting, notified through communications, or are told in person at their homes. The software's variables as well as the maker of the software are completely unknown and unexamined; all that has been revealed is that criminal history, known criminal associates, and whether one has been the victim of a crime are somehow included in the process. Given the serious nature of the consequences of a computer program determining who is most likely to become a criminal, it was inevitable that a lawsuit would emerge in order to determine the underlying processes for the program. The *Chicago Sun-Times* filed a lawsuit in Cook County's Court of Chancery under the Freedom of Information Act to find out the nature of the algorithm, the maker of the algorithm, and the race of each person on the list, among other

---

[5] Andrew Guthrie Ferguson, *The Police are Using Computer Algorithms to Tell If You're a Threat*, TIME (Oct. 3, 2017) http://time.com/4966125/police-departments-algorithms-chicago/.

factors.[6] The CPD refused the initial FOIA request, claiming it would be "unduly burdensome" to provide those details.[7]

B. State of Wisconsin v. Loomis

During the 1990s, the company Northpointe, Inc. worked on the development of COMPAS, an intelligent algorithm designed to assess the risk that a given defendant will commit a crime after release. It uses a number of factors, including a defendant's own responses to a lengthy questionnaire, to generate a recidivism risk score between 1 and 10 by comparing a given defendant's traits to those of known high-risk offenders. It then classifies the risk of recidivism as low risk (1-4), medium risk (5-7), or high risk (8-10). The score is then included as part of a defendant's presentence investigation (PSI) report for the sentencing judge.[8]

In 2012, Wisconsin implemented COMPAS into its state sentencing procedures. In 2013, 35 year-old Eric Loomis was arrested for his involvement in a drive-by shooting in La Crosse, Wisconsin. No one was hurt, but Loomis was driving the getaway vehicle, a stolen car. He pled no contest to two lesser charges—"attempting to flee a traffic officer" and "operating a motor vehicle without the owner's consent." The trial judge sentenced Loomis to 7 years, based in part on a COMPAS score assessing him as a "high risk." Loomis filed a motion for post-conviction relief seeking a new sentencing hearing, arguing that the court's consideration of the COMPAS risk assessment violated his constitutional rights to due process. He further argued that the trial court erred by improperly assuming that the factual bases for the risk assessment were true.

The case went all the way to the Wisconsin Supreme Court, as Loomis challenged the lack of transparency with the algorithm used to sentence him.[9] Loomis argued that while the sentencing judge could view the risk score itself and the inputs affecting it, no one—not even the judge—knew what decisions the software had been programmed to make. Loomis

---

[6] Smith et al. v. Chi. Police Dep't, Case No. 2017-CH-07992 (Cir. Ct. Cook Cty. Chancery Div. June 6, 2017).

[7] A *New York Times* analysis revealed that the likely most significant factors (among known factors) in being a high-risk subject were the number of times one was the *victim* of a violent crime, with the biggest counter-weight being age. Jeff Asher & Rob Arthur, *Inside the Algorithm That Tries to Predict Gun Violence in Chicago*, N.Y. TIMES (June 13, 2017), https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html?_r=1.

[8] Andrew Lee Park, *Injustice Ex Machina Predictive Algorithms in Criminal Sentencing*, U.C.L.A. L. REV. (2019).

[9] State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

contended that Northpointe (and the software company that had written the algorithm, Equivant) should be required to divulge its source code. Because the companies steadfastly refused to do so, citing its proprietary nature and invoking the trade secrets privilege, Loomis asserted that because the scientific validity of the tool could not be determined, his due process rights had been violated. As an expert for Loomis testified, "There's all kinds of information that the court doesn't have," and because too little is known about how the risks are analyzed, "COMPAS should not be used for incarceration decisions."

But the Wisconsin Supreme Court disagreed, stating "[W]e conclude that if used properly, observing the limitations and cautions set forth herein, a circuit court's consideration of a COMPAS risk assessment at sentencing does not violate a defendant's right to due process."[10] The court also considered that because COMPAS uses only publicly available data and data provided by the defendant himself, Loomis could have denied or explained any information that went into the making of the report.[11]

However, the Court also ruled that courts should proceed with caution, and not make an assessment report the sole basis for its sentencing decision. It further held that the use of a COMPAS risk assessment must be subject to certain cautions. Specifically, PSIs accompanying COMPAS assessments must include five written warnings for judges: (1) that the "proprietary nature of COMPAS" prevents the disclosure of how risk scores are calculated; (2) that COMPAS scores are unable to identify specific high-risk individuals because the scores themselves rely on group data; (3) that although COMPAS relies on a national data sample, there has been "no cross-validation study for a Wisconsin population"; (4) that studies have "raised questions" about whether COMPAS scores disproportionately classify minority offenders as having a higher risk of recidivism; and (5) that COMPAS was developed specifically for a different purpose—to assist the Department of Corrections in making post-sentencing determinations.[12]

In a concurring opinion, Justice Shirley Abrahamson expressed concern with "the court's lack of understanding of COMPAS," calling it a "significant problem" and bemoaning the fact that "few answers were available" to the questions that judges had directed to Northpointe as the case wound its way through the courts. Greater explanation was needed, Justice Abrahamson wrote,

---

[10] *Id.*

[11] *Id.* at 761–62.

[12] *Id.* at 769–70.

in part because "the use of risk assessment tools like COMPAS has garnered mixed reviews in the scholarly literature and in popular commentary and analysis."[13]

The *Loomis* opinion, with its urging of caution, its careful distinction that a court may "consider" rather than "rely" on such risk assessments, and its requirement of written disclaimers for PSIs suggests that perhaps enthusiasm over algorithmic risk assessments will be tempered in the future. Only time will tell.

C. Rodriguez and Beyond

The court in *Loomis* justified its decision in part by noting that, since COMPAS uses only publicly available data and data provided by the defendant, Loomis could have denied or explained any information that went into making the report and accordingly could have verified the accuracy of the information used in sentencing. But in another case involving COMPAS, the defendant had a much more challenging task in denying or explaining the information that provided the basis for the report. In 2017, Glenn Rodriguez, an inmate at the Eastern Correctional Facility in upstate New York with a virtually spotless rehabilitation record, was denied parole due to a "high risk" COMPAS score. The bewildered Rodriguez consulted with lawyers and was able to review the 137-item questionnaire that had been filled out about him and which comprised the basis for his COMPAS score. Rodriguez found a mistake in an answer given by the correctional officer who had filled out the form, and learned that other inmates had nearly identical questionnaires to him, but with entirely different scores. Although he had no access to the methodology of the COMPAS assessment, at his second parole hearing in January 2017, Rodriguez argued that since the input was wrong, his final risk score could not possibly be accurate. Yet because he did not know how the information was weighted in the algorithm's code, he could not prove how significant the error was. Rodriguez was ultimately granted parole in May 2017, but without being able to challenge the troubling issues of his COMPAS risk score.[14]

COMPAS remains the most widely used algorithm for risk assessment. At least nine states—Arizona, Colorado, Delaware, Kentucky, Louisiana, Oklahoma, Virginia, Washington, and Wisconsin—use its assessments during criminal sentencing hearings. And despite continued concerns about accuracy, the lack of transparency, and of course the perpetuation of biases, risk assessment algorithms like COMPAS are still used at multiple junctures throughout the

---

[13] *Id.* at 774-75.

[14] Jenny Jiao, *The Pandora's Box of the Criminal Justice System*, JURIS (Sept. 25, 2017).

criminal justice process: (1) to determine the length of sentences; (2) to direct defendants to alternatives to incarceration like rehabilitation; and (3) to shorten sentences for good behavior.

If courts are not going to be receptive to challenges of intelligent algorithms because they are apparently more protective of a company's intellectual property rights in its proprietary software than of an individual defendant's due process rights, what about challenges to algorithms that are based on product liability theories?[15] In the first case of its kind, a federal court in New Jersey considered a product liability claim brought against the owners of an algorithm risk assessment tool.[16] Plaintiff June Rodgers sued over the death of her 26 year-old son Christian Rodgers at the hands of Jules Black on April 9, 2017. Black had been arrested on April 5, 2017, by New Jersey State Police and charged with being a felon in possession of a firearm. According to the lawsuit, Black was released on non-monetary conditions the next day because he had a low Public Safety Assessment (PSA) score, pursuant to the defendant's algorithm. Mrs. Rodgers brought suit under the New Jersey Product Liability Act, arguing that the algorithm had turned out a low PSA for Black because it was a defective product.

The court, however, disagreed. It held that the PSA is not a product as defined by New Jersey's statute. Moreover, the judge reasoned, the algorithm is "neither a tangible product or a non-tangible other item as contemplated by section 19 of the Restatement of Torts and it is not distributed commercially."[17] Ruling that the PSA "constitutes information, guidance, ideas, and recommendations as to how to consider the risk a given criminal defendant presents," the court reasoned that the PSA could not be subject to tort liability since it would be properly treated "as speech, rather than product."[18] The court also rejected Rodgers' contention that such PSAs "thwart" the role of judges, noting that "the PSA does not supplant judicial decision making but merely informs a judge's decision of whether to release or detain a defendant pending trial."[19]

---

[15] Risk assessment algorithms are not the only tech tool being challenged by criminal defendants. The makers of TrueAllele, a software program used to analyze traces of DNA from crime scenes, have faced legal action from defendants seeking to review its source code in order to confront and cross-examine its programmer about how the software works. Like Northpointe, TrueAllele's developers have successfully relied on trade secret evidentiary privilege to quash such attempts at discovery. *See, e.g.*, People v. Chubbs, 2015 WL 139069 (Cal. App. June 9, 2015).

[16] Rodgers v. Laura & John Arnold Foundation, 2019 WL 2429574 (D.N.J. June 11, 2019).

[17] *Id.*

[18] *Id.*

[19] *Id.*

V. MEASURES ADDRESSING ALGORITHMIC BIAS

On the international level, the European Union has already taken steps to address the fallibility of algorithms. Article 22 of the General Data Protection Regulation (GDPR) protects most people from wholly automated decision-making processes, requiring (in many circumstances) human review of appealed automated decisions—even where wholly autonomous decision-making processes are permitted.[20] On a far more local level, the New York City Council reacted to ProPublica's study by establishing the Automated Decision System Task Force in 2017 to study and make recommendations of policies, practices, and guidelines on the use of such systems in all city-wide public agencies. The task force hopes to curb algorithmic bias and promote transparency, including in the area of criminal sentencing.

During the Obama Administration, an effort at introducing an algorithmic accountability law as part of the Consumer Privacy Bill of Rights failed. In April 2019, Senators Ron Wyden (D-Ore.) and Cory Booker (D-N.J.) introduced their own Algorithmic Accountability Act. Under it, the Federal Trade Commission would compel companies to test both their algorithms and training data for any defects that could lead to biased, inaccurate, discriminating, or otherwise unfair decisions. Companies would be required to assess the objectivity of their algorithms, and to address any flaws uncovered during the assessment. In addition, entities subject to the Act would need to ensure that they are protecting the privacy and security of the consumer data being fed into the algorithms. The Act would apply to companies that make over $50 million a year, hold information on at least one million people or devices, or which primarily act as data brokers buying and selling consumer data. The bill was introduced just weeks after Facebook was sued by the Department of Housing and Urban Development, which alleged that the site's ad targeting tools unfairly discriminated on the basis of gender and race in determining who would see certain housing advertisements. As Senator Wyden noted in introducing the bill:

> computers are increasingly involved in the most important decisions affecting American lives—whether or not someone can buy a home, get a job or even go to jail. But instead of eliminating bias, too often these algorithms depend on biased assumptions or data than can actually reinforce discrimination against women and people of color.

But the proposed Act is geared toward consumer protection, not protection of due process and other rights of criminal defendants. Perhaps the best way to address algorithmic bias is not to

---

[20] General Data Protection Regulation 2016/679, art. 22, Automated Individual Decision-Making, Including Profiling, http://www.privacy-regulation.eu/en/article-22-automated-individual-decision-making-including-profiling-GDPR.htm.

be found in legislative solutions at all, but in improving the technology itself. The Laura and John Arnold Foundation, a Houston-based philanthropic organization, has developed the Public Safety Assessment Court tool, an algorithm used in bail decisions. Currently used in thirty jurisdictions, the PSA court tool is not "black boxed" and does not rely on socio-economic factors or gender. Instead, it considers nine factors related to a person's criminal history before providing a risk assessment on how likely the person is to fail to appear for a court date, or commit a new crime or violent crime while on release. The factors include prior misdemeanor and felony convictions, previous failures to appear, and the defendant's age. Studies of the tool are encouraging; research into its use in Ohio, for example, found that outcomes did not show any race or gender bias. The number of people released without the need for bail doubled from 14% to nearly 28%. The percentage of pretrial defendants arrested for other crimes while on bail was cut in half (from 20% to 10%), and the percentage of those arrested for violent crimes while out on bail also dropped (from 5% to 3%). The Arnold Foundation touts not only these results but also the transparency of the PSA court tool.

VI. CONCLUSION

In a 2014 address to the National Association of Criminal Defense Lawyers, then-U.S. Attorney General Eric Holder warned of the dangers of algorithmic bias:

> Although these measures were crafted with the best of intentions, I am concerned that they may inadvertently undermine our efforts to ensure individualized and equal justice . . . By basing sentencing decisions on static factors and immutable characteristics—like the defendant's education level, socioeconomic background, or neighborhood—they may exacerbate unwarranted and unjust disparities that are already far too common in our criminal justice and in our society.

While the use of intelligent algorithms for criminal risk assessment has been promoted as a means of eliminating human bias in sentencing, the fact is that methodologies that are necessarily created by individuals may reflect human bias. When data points that may be race neutral on their face—such as zip codes or family history of incarceration—but which can serve as proxies for race are employed, human bias is not only not eliminated, it is automated. The *Loomis* case and others discussed in this article illustrate this danger, particularly when courts place a higher priority on the protection of intellectual property rights—the "black box" or proprietary "secret sauce" of an intelligent algorithm. Without greater transparency into the workings of a given algorithm, the opaque nature of letting machines function as judge and

jury means no one knows if poor results are being produced until the damage has already been done.

But there is hope. As the field of "algorithmic fairness" grows, data scientists are developing ways to identify and correct disparate impact in machine learning algorithms. After all, part of the problem lies in the reiterative nature of algorithms, many of which "learn" from themselves by running repeatedly, studying and reapplying the results, and compounding them. When even a small amount of bias is introduced, such an algorithm cannot help but reproduce it in a troubling feedback loop.

The complexity of achieving justice rests in the balancing of many factors—deterrence, fairness, proportionality, empathy, victims' and society's calls for punishment, to name just a few. While algorithms can illuminate these goals, they should not be the determinative factor in decisions impacting individual rights.

About the Authors

John 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.

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.

Expecting a Federal Consumer Data Privacy Law in the US?

By Lisa M. Angelo

The use of online services available through apps, cloud, internet-connected cars and devices, and social media is widespread. There is no question that *data* is an important commodity. As consumers, we give away information about ourselves with every account, subscription, and visit to a website. Some information is given away knowingly, while other information is taken from us behind the scenes.

Much of the personal data collected is being used to create frighteningly accurate profiles to predict our every move. Other information is aggregated and studied for the purposes of – well, you name it. At times, it seems the Internet knows us better than we know ourselves.

Because the world is becoming more connected online where it is universally accepted that data breaches are unavoidable, the topic of consumer data protection has risen to the surface of a global discussion.

In the United States, each state[1] has a law that requires businesses to notify consumers of a data breach. In addition to breach notification laws, several states have passed or proposed consumer data privacy legislation to protect consumers. You can find such legislation in California, Connecticut, District of Columbia, Hawaii, Illinois, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Nevada, New Jersey, New Mexico, New York, North Dakota, Rhode Island, Texas, Utah, Vermont, and Washington.[2] There is a minimum threshold for when each state law will apply, but generally, businesses can expect to be subject to the consumer data privacy laws in the states where their customers reside. In other words, most companies doing business online may be subject to multiple—if not all—state consumer privacy laws regardless of the company's state of incorporation or principle place of business.

Initially, achieving compliance with each state's consumer data privacy law is challenging for many companies. The varying thresholds of application of law, definitions, and obligations make compliance a full-time job. Many states sprinkle data protection throughout various

---

[1] References to "states" herein include US territories and the District of Columbia.

[2] Mitchell Noordyke, "US State Comprehensive Privacy Law Comparison", IAPP website, April 18, 2019. (updated by Westin Research Center).

regulations and codes, making it difficult to locate all of the requirements in the first place.[3] The challenges are further exasperated because some of the laws are amended just before being enacted, making compliance feel like a game of catchup.

With so much variance among state legislation to keep track of, companies with customers nationwide are hoping for uniformity. Talks of a federal consumer data privacy law echo throughout the country, but given the history of this type of legislation, nothing is expected to be enacted anytime soon. In the past, federal consumer data privacy legislation has come and gone without ever becoming law. The difference today is, with so many states adopting their own versions of privacy protection laws, the demand for a federal law has grown. Over the past two years, numerous pieces of federal legislation have surfaced and although they have not become law, they provide insight into where data privacy legislation is headed in the United States.

American Data Dissemination Act of 2019

The American Data Dissemination Act of 2019 (ADD Act) was introduced in January 2019.[4] The ADD Act applies to people who provide a service using the internet and, in connection with that service, collect information about an individual. The ADD Act calls for the Federal Trade Commission to develop privacy requirements to restrict the disclosure of personal information and provide individuals with rights to access and correct personal information maintained in records. Under the ADD Act, the Federal Trade Commission would recommend privacy requirements for Congress to impose that are similar to the Code of Fair Information Practice governing the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained federal agencies under the Privacy Act of 1974. Newly formed small businesses and persons subject to other federal privacy laws such as Health Insurance Portability and Accountability Act would be excluded from the ADD Act. If enacted, the ADD Act would supersede state law. Violations would be subject to enforcement by the Federal Trade Commission. The Add Act has been referred to the Committee on Commerce, Science, and Transportation.

---

[3] Nuala O'Connor, Reforming the U.S. Approach to Data Protection and Privacy, Council on Foreign Relations, Digital and Cyberspace Policy program's Cyber Brief, Jan. 30, 2018. (https://www.cfr.org/report/reforming-us-approach-data-protection (accessed July 13, 2019).

[4] ADD Act, S. 142, 116th Cong. § 1 (as introduced Jan. 16, 2019).

Customer Online Notification for Stopping Edge-provider Network Transgressions

The Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act was introduced in April 2018.[5] It would have the Federal Trade Commission establish privacy protections for customers of online edge providers. Under this act, "edge providers" interact with customers online and provide "edge services" which are broadly defined as situations where the customer subscribes to a service, makes a purchase, searches a database using keywords, or divulges what the act refers to as "sensitive customer proprietary information" including information pertaining to children, content of communications, and other more traditional forms of personally identifiable information.

Deceptive Experiences to Online Users Reduction Act

The Deceptive Experiences to Online Users Reduction Act (DETOUR Act) was introduced to prohibit the usage of exploitative and deceptive practices by large online operators, and to promote consumer welfare in the use of behavioral research by such providers.[6] Specifically, this act prohibits large online operators from designing user interfaces with the purpose of impairing or obscuring a user's choices to give consent or give up data. This act embodies the concept of privacy by design where the design of the user interfaces cannot appear to be something it is not.[7] For example, this act would likely prohibit a data-collecting application from appearing to be nothing more than a convenient flashlight app. This act also appears to spell out what could constitute deceptive and unfair business practices.

Consumer Data Protection Act of 2018

At the end of 2018, there was discussion about drafted legislation that would require companies be transparent about data-sharing practices and provide consumers with rights to manage the sharing of their data.[8] Violations of the Consumer Data Protection Act of 2018 could result in civil fines and criminal liability for the officers of a company.

The drafted act amends the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information for the purpose of

---

[5] CONSENT Act, S. 2639, 115th Cong. § 2 (as introduced April 10, 2018).

[6] DETOUR Act, S. 1084, 116th Cong. § 1 (as introduced April 9, 2019).

[7] Woodrow Hartzog, "Privacy's Blueprint: The Battle to Control the Design of New Technologies". (2018).

[8] Consumer Data Protection Act of 2018 (https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20one%20pager%20Nov%201.pdf)

protecting personal information.[9] Covered entities include people, partnerships, or corporations with over $50 million in average annual gross receipts for the prior 3-taxable year period and having personal information of over 1 million consumers. In addition, this act applies to commercial entities substantially involved in the business of collecting, assembling, or maintaining for sell or trade the personal information of individuals who are not customers or employees. As drafted, this act allows recourse for victims of data breaches resulting in noneconomic impact and risk of unjustified exposure of personal information. This ability to recover is important because courts have considered whether data breach victims have suffered sufficient, concrete injury to warrant requisite standing to bring a lawsuit. This act also permits the Federal Trade Commission to impose a discretionary civil penalty of up to $50,000 per violation and 4% the total annual gross revenue of the covered entity for the prior fiscal year – language reminiscent of Europe's General Data Protection Regulation that went into effect May 2018. For covered entities with over $1 billion in revenue each year, this act requires an annual data protection report documenting compliance. Such annual reports would need to be accompanied by written certification from the chief executive officer, chief privacy officer, and chief information security officer. Another component to his drafted act is that the Federal Trade Commission implement and maintain a "Do No Track" data sharing opt-out website where consumers may manage the status of their opt-outs.

Digital Accountability and Transparency to Advance Privacy Act

The Digital Accountability and Transparency to Advance Privacy Act (DATA Privacy Act) was introduced in February 2019.[10] It requires entities that collect, process, store, or disclose data "practicably linkable" to an individual or device associated with an individual post a privacy notice and comply with minimum data processing requirements. Covered entities would also need to provide consumers with methods to control personal information, implement policies and procedures for information security standards, and designate a privacy protection officer. Few exceptions would exist for businesses with data of less than 3,000 individuals and for information used for the purpose of employment. Otherwise, covered entities would be subject to enforcement by the Federal Trade Commission and State Attorneys General.

---

[9] Dr. Lorrie Faith Cranor, et. al. "Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy" (Nov. 1, 2018). (https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy)

[10] DATA Privacy Act, S. 583, 116th Cong. § 1 (as introduced Feb. 27, 2019).

Social Media Privacy Protection and Consumer Rights Act of 2018

The Social Media Privacy Protection and Consumer Rights Act of 2018 was introduced in April 2018 and aims to protect the privacy of social media users. This act requires covered online platforms to make disclosures about privacy, obtain initial consent, and discover the user's privacy preferences before the consumer uses the platform. In addition, the covered entity would need to provide a conspicuous and comprehendible disclosure about data collection, maintain a data security program, and permit users to access their own personal information. This act would also require the covered entity notify users of a data breach within 72 hours of becoming aware that personal data of a user was transmitted in violation of the security program. Unlike other legislation, this act would apply to nonprofit organizations.

Although there have been numerous pieces of federal legislation, it is uncertain if anything currently drafted will become law. However, it is important to observe trends in data privacy legislation to help companies prepare for a future federal consumer data privacy law.

Companies can also appreciate that despite a lack of federal law, compliance with state consumer data privacy laws will likely help companies avoid unfair and deceptive practices prohibited by state general consumer protection statutes and the Federal Trade Commission.[11] As we look forward to uniformity among the states, businesses with customers in multiple jurisdictions should waste no time implementing a data protection program to comply with applicable state laws. Many state data privacy laws will go into effect in January 2020 and the enforcement actions won't be too far behind.

About the Author

Lisa M. Angelo advises clients on data privacy, cyber insurance disputes, data breach response, technology transactions, and other matters related to technology and cyber law. She has two internationally-recognized certifications in information privacy: a Certified Information Privacy Manager and a Certified Information Privacy Professional/US. She is licensed to practice law in Texas and Colorado.

[11] Matthew Denn & Amanda Fitzsimmons, "*District of Columbia v. Facebook*: General Consumer Protection Statute Can Serve as Vehicle for State Attorney General Seeking Redress for Data Privacy Violations", DLA Piper Litigation Alert. (June 12, 2019).

Demonetization and Censorship on YouTube: You're Not Gonna Win

By: Gwendolyn Seale[1]

Introduction

Google unveiled new changes to YouTube's ad monetization policies last January, astonishing members of the creative community. Previously, the threshold for a channel to be able to qualify for YouTube's Partner Program, which enables creators to collect ad revenue, was a total of 10,000 views. Now, in order to receive ad revenue, channels must have a minimum of 1000 subscribers and 4000 hours of total watch-time over a 12-month period. These changes stemmed from YouTube having faced a rash of criticism from advertisers whose ads were run alongside of unsuitable and inappropriate video content. Following popular vlogger, Logan Paul's, broadcast of a suicide victim's body on the platform and the outrage that Paul was able to continue to monetize his channel despite those atrocities, YouTube released a statement, "[t]hey [the new thresholds] will allow us to significantly improve our ability to identify creators who contribute positively to the community and help drive more ad revenue to them [and away from bad actors]."[2] Despite YouTube's arguably good intentions with their new policies, both indie creators and creators with more established YouTube channels have subsequently paid the price. Many indie creators can no longer qualify for YouTube's Partner Program so as to monetize their channels, since subscriber numbers were never previously determinants for monetization. And even for creators with more well-established channels, certain videos are now being demonetized due to video thumbnails, captions or content being deemed inappropriate in the eyes of Google, which is the focus of this piece.[3]

A Brief History of YouTube

In 2005, YouTube launched as a video-sharing website and Google purchased it in 2006, calling it "the next step in the evolution of the internet."[4] By 2007, YouTube introduced the "YouTube Partner Program" enabling creators to monetize their video content through ads

---

[1] Gwendolyn Seale is a 2016 graduate of SMU Dedman School of Law and practices entertainment law at Mike Tolleson and Associates. This article was originally prepared for the State Bar of Texas Entertainment Law Institute in November 2018.

[2] Neal Mohan and Robert Kyncl, *Additional Changes to the YouTube Partner Program (YPP) to Better Protect Creators*, (Jan. 16, 2018), https://youtube-creators.googleblog.com/2018/01/additional-changes-to-youtube-partner.html.

[3] Interview with Evan Bregman, September 17, 2018.

[4] Associated Press, *Google buys YouTube for 1.65 Billion*, (Oct. 10, 2006), http://www.nbcnews.com/id/15196982/ns/business-us_business/t/google-buys-youtube-billion/.

being run alongside their videos.[5] By this time YouTube entered into the mainstream—not only was it a forum in which one could upload and watch funny content, but it also had become a platform that encouraged people to engage with others politically. For example, YouTube partnered in 2007 with CNN to host the 2008 Presidential Debate, and Americans submitted video questions through the platform to the candidates.[6] And during the 2011 Arab Spring, protestors and activists were able to upload videos to the platform, publicizing the plight of authoritarianism within areas of the Middle East and Northern Africa and providing political commentary for the rest of the world to absorb.[7] YouTube has since launched features such as: live streaming, film rental services, Vevo—a multi-channel network (MCN), which hosts music videos from the major record labels, YouTube Red (now Premium), which features the ability for viewers to watch videos without ads, YouTube music—a music streaming application, and YouTube TV, which provides access to the 5 major American television networks, along with other channels that are found on cable or satellite.[8] Over the last few months, YouTube has also launched a channel membership feature and a merchandise store for creators.[9] More-established creators, whose channels have 100,000 or more subscribers now have the ability to offer channel memberships to subscribers, which provides access to more exclusive content and custom emojis.[10] And channels with 10,000 or more subscribers can sell merchandise such as tee-shirts, hats and coffee mugs directly to fans via links under the video content.[11] To this date, YouTube is the second largest search engine, the third most visited site on the internet,

---

[5] John Biggs, *YouTube Launches Revenue Sharing Partners Program, but no Pre-Rolls*, TechCrunch (May 4, 2007), https://techcrunch.com/2007/05/04/youtube-launches-revenue-sharing-partners-program-but-no-pre-rolls/ .

[6] *Your voice to be heard in historic debates*, CNN Politics, (July 4, 2007), http://www.cnn.com/2007/POLITICS/07/04/youtube.debates/index.html .

[7] Catherine O'Donnell, *New study quantifies use of social media in Arab Spring*, UW News, (Sept. 12, 2011). http://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/ .

[8] *YouTube*, Wikipedia, https://en.wikipedia.org/wiki/YouTube#cite_note-306 .

[9] Sarah Perez, *YouTube introduces channel memberships, merchandise and premieres*, TechCrunch, (June 21, 2018), https://techcrunch.com/2018/06/21/youtube-introduces-channel-memberships-merchandise-and-premieres/ .

[10] *Id.*

[11] *Id.*

following Google and Facebook — and on average— people view 1 billion mobile videos each day.[12]

Since March 2017, a time declared by the creative community as the "Adpocalypse", YouTube has received a considerable amount of backlash due to their monetization criteria changes.[13] The March 2017 changes to the platform included the changing the threshold of monetization to 10,000 views on a video (which has since been replaced by the new thresholds mentioned at the beginning of this article) and new guideline restrictions regarding ads.[14] Although the guidelines are not public information, a member of YouTube's ad monetization team recently published a video aimed at providing guidance to users regarding profanity and ad monetization.[15] The video indicated that words like "dang," "damn," and "hell" are not words that concern YouTube and would not impact monetization.[16] The video also advised against using words like "bitch," "whore," and "f*%$" in the video caption and thumbnail, and repeatedly within the beginning of the actual video content, as those terms could impact a creator's ability to monetize her content.[17] And as to be expected, the video additionally expressed zero-tolerance towards racist, violent and hateful material.[18] The rationale behind enacting the guidelines made sense, as companies like AT&T, Verizon Communications, Pepsico and Starbucks, reportedly discontinued advertising on the platform for a period of time.[19] And through the altering of the algorithms within AdSense[20], videos can be

---

[12] *36 Mind Blowing YouTube Facts, Figures and Statistics – 2017 (re-post)*, Videonitch (Dec. 13, 2017), http://videonitch.com/2017/12/13/36-mind-blowing-youtube-facts-figures-statistics-2017-re-post/ .

[13] Bill Sussman, *How Influencers Get Creative In The Face Of Lower YouTube Revenue*, Forbes (Sept. 5, 2017), https://www.forbes.com/sites/forbesagencycouncil/2017/09/05/how-influencers-get-creative-in-the-face-of-lower-youtube-revenue/#386a219cfb41 .

[14] *Id.*

[15] Creator Insider, (Jan 14. 2019) https://www.youtube.com/watch?v=VWAdzMmNLy0.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] From a content creator's standpoint, Google has a platform called AdSense, which places ads against the creator's videos. Once the content creator has signed up with AdSense and has enabled monetization on his/her channel, different types of ads will be placed against videos that contain the creator's content. When an ad is placed on the video, Google makes ad revenue based on either a CPM (cost per thousand impressions) or CPC (cost per click) criteria (the advertiser chooses this criteria) and Google provides the content creator with a cut.

demonetized based upon a video caption, video thumbnail or video content being classified as inappropriate or unsuitable, effectuating the goals of the new guidelines.[21]

Channel Demonetization and Censorship

YouTube's resulting guidelines resulting from the Adpocalypse and the Logan Paul fiasco have frustrated many creators, as they claim that their videos have been wrongly demonetized. One of such example is Zombie Go Boom (ZGB), a company that operated a YouTube channel with videos that they self-described as "The Walking Dead meets Mythbusters" ---a channel that boasted over 1.6 million subscribers and millions of video views each month, whose videos were being demonetized.[22] ZGB subsequent to these guideline changes filed a class-action suit against Google, stating that their videos were unfairly demonetized.[23] They pointed to the fact that after March 27, 2017, their ad revenue went from $300-$500 dollars per day to $20-$40 dollars per day, a 90% -95% decrease, essentially overnight.[24] ZGB based their case on several claims, including 1) breach of contract; 2) tortious interference with contractual relations; and 3) breach of the duty of good faith and fair dealing.[25] Regarding the breach of contract claim, ZGB claimed that YouTube breached the contract between the parties "by altering the terms and conditions that governed how ZGB and the classes' videos would be monetized."[26] ZGB's tortious interference claim reasoned that the monetization criteria changes and demonetizing videos without notice or recourse directly impacted contracts that ZGB and the class had entered into with third parties.[27] The breach of the duty of good faith and fair dealing claim addressed ZGB's assertions that these policy changes unfairly prevented ZGB and the class from receiving the benefits of the contract and had resulted in significant economic loss.[28] These arguments proved futile as the judge dismissed the claims, stating that the contract between creators and YouTube was explicit, as the terms read that YouTube was under no obligation to display advertisements alongside creators' videos.[29]

---

[21] Interview with Evan Bregman, September 17, 2018.

[22] Jonathan Stempel, *Google defeats Zombie Go Boom 'Adpocalypse' lawsuit*, Reuters (Mar. 8, 2018), https://www.reuters.com/article/us-alphabet-adpocalypse-lawsuit/google-defeats-zombie-go-boom-adpocalypse-lawsuit-idUSKCN1GK28D .

[23] *See generally*, *Sweet v. Google*, No. 17-cv-03953-EMC. N.D. California, 2018.

[24] *Id*. at 2.

[25] *Id*. at 2-3.

[26] *Id*.

[27] *Id*.

[28] *Id*.

[29] *Id*. at 7-8.

YouTube has also seen outrage from creators due to perceived video censorship. For example, Prager University, a producer of conservative video content, filed suit against Google asserting numerous claims, one of which was the violation of Prager University's First Amendment rights.[30] Prager reasoned that YouTube's censorship of some of its videos was based upon animus towards its political viewpoints, as opposed to the content of the videos, and therefore sought an injunction against the platform.[31] YouTube did, in fact, impose age restrictions upon and demonetized certain Prager videos.[32] By placing these age restrictions on the certain videos, YouTube viewers, whose accounts have "Restricted Mode" turned on, were unable to watch these videos.[33] The complaint noted in particular, a restricted Prager video titled, "Are 1 in 5 college women raped," while a CBS video titled, "Author John Krakauer on new book Missoula and the college rape epidemic," was not restricted, and surmised that its video was restricted because of Prager's political viewpoints.[34] Prager's arguments were to no avail -- the judge denied the injunction and granted Google's motion to dismiss, reasoning that YouTube was not a public forum run by a state actor.[35] In the same vein, in March 2019, the U.S. District Court for the District of Columbia dismissed a lawsuit based on the First Amendment and the Sherman Antitrust Act, brought by Freedom Watch, a "conservative non-profit public interest organization," and Laura Loomer, a conservative journalist, against Google and other social media platforms.[36] Freedom Watch and Loomer claimed that their YouTube channel and other social media accounts had generated revenue for many years, but that following the election of Donald Trump, due to the suppression of conservative content, their social media revenue plateaued or decreased.[37] The Sherman Antitrust Act claims failed, as Freedom Watch and Loomer provided no factual matter that established the social media platforms engaged in a conspiracy or monopolistic practices.[38] And just as in Prager, the plaintiffs First Amendment claim failed as Google and the other social media outlets are not state actors.

---

[30] *See generally*, *Prager University v. Google,* No. 17-CV-06064-LHK, N.D. California, 2018.
[31] *Id* at 1-2,5.
[32] *Id*. at 1-2.
[33] *Id.*
[34] *Id*.
[35] *Id*. at 5-8.
[36] Freedom Watch, Inc. v. Google Inc., 368 F. Supp. 3d 30, 35-41 (D. D.C. 2019).
[37] *Id.*
[38] *Id.*

Conclusion

Because of the actions of some bad actors in the YouTube community, the platform changed its monetization policies – so now, videos can be demonetized due to a video caption, a thumbnail or the content itself. As outlined in the cases above, it will be nearly impossible for a party to successfully sue Google/YouTube based upon their monetization policy changes, as YouTube's terms and conditions read that not only can it change its policies at will, but also, the platform does not even have a duty to display ads in connection with creators' video content. And finally, it will be virtually impossible to successfully sue Google/YouTube on First Amendment grounds if one's video content is restricted or demonetized, as it will be incredibly difficult to sufficiently allege that these platforms are state actors.

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.

Competency Requirements and Technology: I am a Lawyer – I know the Law, so why do I need to Understand or Use Technology?

By Sanjeev Kumar

As lawyers, we are expected to provide competent and diligent representation to our clients. The Texas Disciplinary Rules of Professional Conduct specifically require us not to accept or continue representation of a client in a legal matter that we determine to be beyond our competence. Comment 8 to Rule 1.01 for maintaining competence specifically states that each lawyer should strive to become and remain proficient and competent in the practice of law, *including the benefits and risks associated with relevant technology* (emphasis added). Change is hard, and a number of lawyers and law firms have continued to do business without gaining the requisite knowledge or incorporating appropriate technology in our practice of law.

With increased cyber threats, it is imperative that lawyers also consider security aspects of their practice of law and take reasonable steps to secure their network and client data to avoid unnecessary and expensive intrusions and loss of data, as well as costly downtime. Technical competence, like competence in a particular practice area, does not require a lawyer to become a technology expert; rather, we should understand the technical aspects of our practice and gain requisite knowledge to implement reasonable security features in our practice and systems. Taking those reasonable steps may not be a guarantee against a cyberattack, but it will for sure serve as an insurance policy and probably meet the standards required towards our professional responsibility in serving our clients. This is not only true for large law firms, but it also equally applies to solo and small law firms, even though what is reasonable may be different for smaller firms and may even differ based on practice areas.

Adopting technology is also a necessity for law firms to have a better and more efficient practice, provide faster and more proactive service to our clients, and provide channels of communications to our clients that most other professions have already implemented. Implementing the use of numerous new applications on portable devices like iPads and other tablets and smartphones allows us lawyers to have access to our client matters and may help us in streamlining our work flows, increasing the efficiency of our practices. With the changing work environment in law firms, it is not justifiable for any of us lawyers to be completely computer illiterate or be fearful of the new technologies.

One easy way to acquire required technical competence and maintain that competency is by joining the Computer & Technology Section of the State Bar of Texas (shameless plug!), which strives to assist members by various means, such as tech-bytes; presentations on various apps for lawyers; timely articles through our quarterly newsletter, *Circuits*; section's legal app for smartphones and tablets that provides handy access to most of the common federal and state laws; and various CLE opportunities at the State Bar Annual Meeting as well as CLE co-sponsored by the section.

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.

More Than Meets the Eye? Why Deepfakes Are Trouble Under Existing Copyright & Privacy Laws

By Tom Kulik

You've seen it, and you probably don't even realize it. If you haven't, you will probably ask yourself the same question everyone else does, which is: How in the heck do they *do* it? For the uninitiated, I am talking about "deepfakes" (an interesting combination of the phrase "deep learning" and the word "fake"). Often described as "a technique for human image synthesis based upon artificial intelligence," deepfakes are essentially altered photos or videos that are definitely not what they seem, and in the context of copyright and privacy laws, disrupting more than you think.

First, some understanding of deepfakes is necessary to understand the context and scope of the issues. Altering images and video to be something other than originally intended is nothing new, but these altered images and videos go far beyond simple alteration – these are (usually) created by using a machine learning construct known as generative adversarial network(GAN). A GAN essentially involves two artificial neural networks working off each other based on a specific training objective (such as the creation of an image indistinguishable from the original), with the "generative" network creating new images that are then compared by a "discriminative" network until the generative network meets the objective. Of course, this is a gross simplification of a complex process, but you get the gist – deepfakes are *very* convincing computer-generated "fakes." You don't believe me? Look at an example of here. Although there is definitely room for improvement, we are rapidly approaching a time when such deepfakes will be extremely hard, if not impossible, to detect.

Such convincing fakes are an amazing feat of technology, but present a host of thorny issues when it comes to their use. Although an interesting means for parody, the Mark Zuckerberg deepfake demonstrates how this technology can be used to create a false narrative attributable to a person who never said it. It can also be used to morph existing images into ones that may depict the original content (or the copyright owner) in manner that is disparaging, if not extremely damaging, to the work itself. In a nod to conspiracy theorists, it will not be outside the realm of possibility for such deepfakes to soon be used to induce anything from stock

market instability to an all-out war. It's not hard to imagine bad actors using this technology to further their own objectives, and unfortunately, the law has a lot of catching up to do.

The issues presented by deepfakes under copyright and privacy laws are troubling, and here are a few examples that should be pause for particular concern:

- **Fair Use**. Although the owners of copyrighted works enjoy certain exclusive rights to those works, the fair use doctrine allows for freedom of expression by permitting the unlicensed use of copyrighted works by others under limited circumstances, such as for criticism, comment, news reporting, teaching, scholarship, and research. Section 107 of the Copyright Act outlines these criteria, as well as four specific factors for consideration in the fair use analysis. It should come on little surprise that many deepfakes may fit squarely within enumerated exceptions, but when it comes to weighing the four factors, whether the deepfake is sufficiently transformative or whether the use would have a negative effect on the market for the work are far more complicated elements to consider. Needless to say, deepfakes can take the fair use analysis to a whole new level, much to the chagrin of the copyright owner.

- **The Digital Millennium Copyright Act (DMCA)**. Enacted in 1998, the DMCA provides (among other things) a mechanism for copyright owners to request a "takedown" of their copyrighted content from websites, but this mechanism is far from perfect. For example, the fair use doctrine listed above operates as a valid defense to such a takedown request. Further, DMCA take down notices are only as valid as the country that recognizes them, so they are not much help if the website hosting the infringing work is based in a far-off jurisdiction that does not recognize them. Moreover, it is not a stretch to assume that many deepfakes will be posted through social media channels such as YouTube and Facebook to name a few. Given the recent postings of deepfakes on social media platforms already, there does not seem to be any universally accepted way of handling such deepfakes, so each social media platform will handle it differently. This lack of continuity among social media platforms creates yet another layer of inconsistency in application of existing copyright laws.

- **Communications Decency Act (CDA) Section 230.** Section 230 of the CDA states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This language has been broadly interpreted by the courts as essentially immunizing internet service providers from liability for defamatory or infringing content created by third-

parties and passively published on the ISP's platform. Of course, Section 230 would not protect ISPs that *actively* create disparaging and/or infringing content, but you can see the problem – if ISPs cannot make out a deepfake for being, well, *fake*, they cannot be held liable for it being present on their platform.

- **State Privacy Torts.** Most states either recognize at common law or have enacted laws that address violations of individual privacy, generally addressing (i) intrusion upon seclusion or solitude, or into private affairs; (ii) public disclosure of embarrassing private facts; (iii) publicity which places a person in a "false light" in the public eye; and (iv) misappropriation of one's name or likeness for commercial gain. To the extent a deepfake crosses the threshold of liability under an applicable state tort, the individual damaged by the deepfake usually has the ability to seek redress. That said, not all states recognize all the aforementioned privacy torts. Moreover, redress may rest with the individual(s) depicted in the work as opposed to the copyright owner. Worse still, obtaining the identity of the actual creator of the deepfake is not a given, creating an impediment to the person damaged by the deepfake. When combined with the questionable liability of the actual service provider under the CDA, actual redress seems an uphill battle.

Whether we like it or not, deepfakes are here to stay, and are only going to get better and far more convincing. That said, the issues presented above are anything but clear, and will need to be addressed in more solid ways than through the existing copyright framework, the CDA and/or a patchwork of state privacy laws. Only time will tell if this will be accomplished through updates to the Copyright Act, the DMCA, CDA or through other federal legislative measures. Let's just hope it is sooner rather than later – until then, it seems that more than the lines between facts and fakes will remain blurry, at best.

About the Author

Tom Kulik is an Intellectual Property and Technology Law Partner at Scheef & Stone, a full-service commercial law firm based in Dallas, Texas. He uses his award-winning industry experience in technology to creatively help his clients navigate the complexities of law and technology in their businesses. A former Chairman of the Dallas Bar Association Science & Technology Law Section, he is also a regular commentator on nationally syndicated radio and television on trending legal issues involving emerging technologies, and a national IP columnist at AboveTheLaw.com. His full bio can be found at https://solidcounsel.com/attorney/tom-kulik/.

Instagram Will Get You If You Are Not Mindful

By Pierre Grosdidier

Jean-Philippe Smet[1] died in December 2017 at the age of 74 in a western Paris suburb. His potential heirs disputed his estate, two camps arguing over the dispositive application of French or California law based on Smet's residency. A French court found for France, in large part because of Smet's uncontroverted trail of Instagram posts from within that country.

Better known to his fans as Johnny Hallyday, Smet was dubbed the "French Elvis" by his country's press for his handsome looks and his incontrovertible role in introducing and popularizing rock music in France. Ever popular in the francophone world, he sold over 100 million records in a singing career that spanned nearly six decades. Hallyday left behind two adult children (David and Laura) from a former wife and a lover, respectively, a widow 31 year his junior, Laeticia, *née* Boudou, and two adopted minors from his last marital relationship.[2] His estate apparently consists mostly of intellectual property rights arising from his music, together with real properties in France, Saint Barthelemy, Los Angeles, and Santa Monica.

In a fact pattern reminiscent of a law school reading assignment, wills in one form or another surfaced from 1997, 2006, 2007, 2011, and 2014, including two in this last year alone, one of which was drafted in English. The two 2014 wills completely disowned Hallyday's two adult children in favor of his widow. Earlier wills had given the adult children their reserved shares under French law,[3] or 3/16th of the estate for each child.[4] Importantly, Hallyday declared in both of his 2014 wills that he was domiciled in Los Angeles County. The elder children sued in Nanterre, outside Paris, demanding, *inter alia*, that the court find that their father lived in France and hold that the Nanterre court had jurisdiction over his succession. The stakes could not be higher for the potential heirs. French residency and, therefore, French jurisdiction, would mean that the California wills might be held invalid and the adult children would receive their reserved shares. In the alternative, it would be up to a California court to rule on the

---

[1] Pronounced as in "met" and "net."

[2] *Smet v. Boudou*, Tribunal de grande instance de Nanterre, May 28, 2019. A *Tribunal de grande instance* is the French equivalent to a district court.

[3] The *reserve héréditaire*, or hereditary reserve: the defunct's children inalienable share of the estate under French law.

[4] The children's reserved share is ¾th of the estate to be shared equally among the siblings.

validity of Hallyday's last wills. If these wills passed muster under California law, Boudou might inherit everything.

As a threshold issue, the court held that EU Regulation no. 680/2012 provided the dispositive law. Its Article 4 states that "[t]he courts of the Member State in which the deceased had his habitual residence at the time of death shall have jurisdiction to rule on the succession as a whole."[5] The Regulation's preamble helpfully provides that

> [i]n order to determine the habitual residence, the authority dealing with the succession should make an overall assessment of the circumstances of the life of the deceased during the years preceding his death and at the time of his death, taking account of all relevant factual elements, in particular the duration and regularity of the deceased's presence in the State concerned and the conditions and reasons for that presence.[6]

The court analyzed Hallyday's residency from both objective and subjective angles. Addressing the first, the court discounted Boudou's claim that the couple had settled in California since 2007 because written evidence showed that the couple claimed Swiss residency in 2007– 2011. In any event, these years did not precede Hallyday's death. Instead, a table of geo-locations from 2012 to 2017 that David prepared and adduced based on the couple's Instagram account swayed the court. The table showed—and Boudou could not but concur—that the couple was in France for at least 151 days in 2015 and 168 days in 2016. Significantly, the numbers of days spent in France in 2015–2016 were minima because one could infer that the couple remained in France during the time period between two closely-timed Instagram posts. It was also uncontroverted that Hallyday had continuously resided in France in the eight months that preceded his death in 2017. This evidence objectively established Hallyday's residence in France "during the years preceding his death and at the time of his death."

The court next reviewed subjective elements based mostly on Hallyday's social and professional life and concluded that they also weighed in favor of French residency. Hallyday indisputably spent time in Los Angeles but, Boudou could adduce no evidence showing that the couple had a substantial social life in Southern California. The couple's Instagram posts revealed that their social life was centered in France. Moreover, Hallyday was virtually unknown in the United States and his professional life (*e.g.*, his concerts) gravitated around France. He

---

[5] Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012, Art. 4.

[6] *Id.* cmt. 23; *see also id.* cmt. 24 (in complex cases, the decedent's habitual residence might be the "State of origin in which the centre of interests of his family and his social life was located.").

merely went to California to relax, recoup, seek inspiration, and possibly to try to escape the French *fisc*, but the record did not establish that he resided there.

About the Author

Pierre Grosdidier is Senior Assistant City Attorney at the City of 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. He was the Section's Webmaster and Circuits eJournal Co-Editor for 2018–19.

Service of Process via Social Media Comes to Texas

By John G. Browning

Back in 2010, the *Texas Bar Journal* published my article *You've Been Served – Without Ever Leaving the Computer*, in which I described the early but growing trend of various foreign countries and jurisdictions here in the United States recognizing the availability of using social networking platforms as a form of substituted service. Since then, the Texas Family Code (Annotated) has cited this article approvingly, the Texas Legislature in 2013 considered a bill to expressly authorize service using social media as an alternative means of service, and the number of American state and federal courts to give their blessing to "service by Facebook" has steadily grown. And while a number of Texas judges have informally approved of such electronic notification as an acceptable form of substituted service, the 2019 Texas Legislature finally made it official: service of process via social media is now a thing in Texas.

The text of Senate Bill 891 (an omnibus bill that amends multiple statutes) amends Chapter 17 of the Texas Civil Practice and Remedies Code specifically by adding Section 17.033, entitled *Substituted Service Through Social Media Presence*. It provides that, in cases that meet the requirements for substituted service under the existing Texas Rules of Civil Procedure, the court "may prescribe as a method of service an electronic communication sent to the defendant through a social media presence." The new 17.033, which was signed into law by Gov. Abbott on June 10, 2019, also specifies that the Supreme Court of Texas must adopt rules to provide for such "substituted service of citation by an electronic communication sent to a defendant through a social media presence" no later than December 31, 2020. In addition to this rule requirement, the new Section 17.033 will only apply to actions commenced "on or after the effective date of the rules adopted by the Supreme Court."

What might such rules involve for determining the appropriate circumstances for serving someone via social media? For guidance, one might look to the criteria discussed in an earlier legislative effort to authorize substituted service through social networking platforms—2013's H.B. 1989. In H.B. 1989's language, a court would have discretion to order such service of process after determining several factors. These factors were (1) whether the party to be served has an active social media profile on the site selected for service; (2) whether the social media profile is actually the profile of the party; (3) whether the party uses the social media profile on a regular basis; and (4) whether the party could reasonably be expected to receive the notice if the electronic communication is sent to the party's social media account.

These factors make sense, since they address some of the chief concerns about service of process via social media. One of these concerns is the authenticity of the defendant's profile. Given the ease with which fake profiles can be created, it won't be enough to simply point to a profile that has a picture of the defendant. The court will need greater assurances of authenticity such as the age of the profile, quantity and history of posts, instances of direct communication with the subject through the social media account in question, etc. As one New York federal court noted in rejecting a request for service of process via social media, "anyone can make a Facebook profile using real, fake, or incomplete information, and thus there is no way for the Court to confirm whether the Facebook page belongs to the defendant to be served."[1] Another understandable concern is the extent to which the defendant regularly uses that social media profile and can reasonably be expected to get notice of the lawsuit. While the issue of the service reaching its intended recipient exists with other forms of service, there are any number of ways an intended service of process via Facebook might go astray. For example, what if a Facebook account was left logged in on someone else's computer?

Concerns such as these, along with some discomfort with technology itself, were prominent when the Oklahoma Supreme Court addressed the issue of service of process via Facebook in a 2014 family law case.[2] *In re Adoption of K.P.M.A.* involved the termination of a father's parental rights for a child born out of wedlock and put up for adoption. The father appealed the termination of his rights, arguing that he had received improper, inadequate notice that he was the father. The child's mother had sent him a Facebook message "informing him that she was pregnant and plan[ned] to give the child up for adoption."[3] The father testified that he didn't see the message until later, and did not know how long it had been in his inbox. Holding that notice provided via Facebook did not satisfy the due process requirements of either the U.S. or Oklahoma constitutions, the Oklahoma Supreme Court noted that the mother could have used a more direct means of relaying the message. The Court also observed that "Facebook . . . is an unreliable method of communication if the account holder does not check it regularly or have it configured in such a way to provide notification of unread messages by some other means."[4]

But other jurisdictions have been more willing to embrace the concept of service via social media, especially in family court cases or in scenarios involving international defendants. In

---

[1] Fortunato v. Chase Bank, 2012 U.S. Dist. LEXIS 80594 (S.D.N.Y. June 7,2012)

[2] *In re* Adoption of K.P.M.A., 341 P.3d 38 (Okla. 2014).

[3] *Id.* at 40.

[4] *Id.* at 51.

Baidoo v. Blood-Dzraku, New York Supreme Court Judge Matthew Cooper permitted a divorce summons to be served solely by private message to the spouse's account.[5] The court held that such service "is the form of service that most comports with the constitutional standards of due process" after the plaintiff established that the account belonged to her husband, that he regularly logged onto the account, and that she did not have his current email or street address (making personal service impossible). Judge Cooper went on to note that regarding the idea of service via social media,

> a concept should not be rejected simply because it is novel or non-traditional. This is especially so where technology and the law intersect. In this age of technological enlightenment, what is for the moment unorthodox and unusual stands a good chance of sooner or later being accepted and standard, or even outdated and passé. And because legislatures have often been slow to react to these changes, it has fallen on courts to insure that our legal procedures keep pace with current technology.[6]

Similarly, in another New York family court case, the court allowed a father seeking modification of child support payments to serve the mother via Facebook.[7] After multiple efforts using traditional means of service had failed, the court permitted service through Facebook after the father showed the mother's active use of her Facebook account (by pointing out the mother's "likes" of photos posted by the father's current wife). And in a New Jersey case of first impression, the court allowed the plaintiff to serve an out of state defendant through Facebook after traditional methods proved ineffective and the plaintiff demonstrated that the defendant had been communicating with her through his Facebook account.[8]

But when plaintiffs cannot establish that other avenues of service have proven ineffective and that service via social media will be reasonably calculated to apprise the defendant of the action against him, courts will not hesitate to deny permission to use social media as a form of substituted service. For example, one Pennsylvania court denied an application to serve the defendant via his LinkedIn account because the plaintiff failed to describe in sufficient detail the other efforts at effecting service.[9] And in *Qaza v. Alshalabi*, the court denied an application to perfect service through Facebook because the plaintiff could not establish that the

---

[5] Baidoo v. Blood-Dzraku, 48 Misc.3d 309, 5 N.Y.S. 3d 709 (N.Y. Sup. Ct. 2015).

[6] *Id.*

[7] Noel B. v. Anna Maria A., 2014 N.Y. Misc. LEXIS 4708 (Fam. Ct. Sept. 12, 2014).

[8] K.A. v. J.L, 450 N.J. Sup. Ct. 247 (Ch. Div. 2016).

[9] Miller v. Native Link Const. LLC, 2016 WL 247008 (W.D. Pa. Jan. 21, 2016).

defendant's Facebook account was still being used by the defendant, casting doubt on whether such service would have actually put the defendant on notice of the lawsuit against him.[10]

Substituted service via social media—a concept already recognized in eight countries and multiple state and federal courts here in the U.S.—has finally and officially come to Texas. Given the ubiquity of social media use and the advantages it offers over other alternatives like service by publication (read any good legal notices lately?), it may prove, in the proper circumstances, to be the only method to comply with due process and reasonably apprise the defendant of the legal proceedings against him. Courts might be hesitant at first, but as one federal court observed about the "relatively novel concept" of service by Facebook, "history teaches that, as technology advances and modes of communication progress, courts must be open to considering requests to authorize service via technological means of then-recent vintage, rather than dismissing them out of hand as novel."[11]

About the Author

John 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 an adjunct professor at SMU Dedman School of Law and he serves as the Chair of the Computer & Technology Section of the State Bar.

[10] Qaza v. Alshalabi, 43 N.Y.S.3d 713, 717 (N.Y. Sup. Ct. 2016).
[11] FTC v. PCCare247 Inc., 2013 WL 841037 (S.D.N.Y. Mar. 7, 2013).

Legislative Update – Cybersecurity

By John G. Browning

The 2019 Texas Legislature tackled weighty issues like property tax relief and amending Texas' anti-SLAPP law, but perhaps lost in the shuffle was an important cybersecurity measure, HB 4390. This law creates a Texas Privacy Protection Advisory Council, intended to study privacy laws in Texas, other states, and foreign jurisdictions such as the EU. This Council will recommend statutory changes regarding privacy and data security via a report to the Legislature by December 31, 2020—just in time for the next legislative session in 2021. The Council is to consist of 15 appointed members from the Texas Senate and House of Representatives, technology/cybersecurity industry members, a representative of a non-profit group that studies data privacy issues from the consumer perspective, and a law professor who has published scholarly work in the area of data privacy.

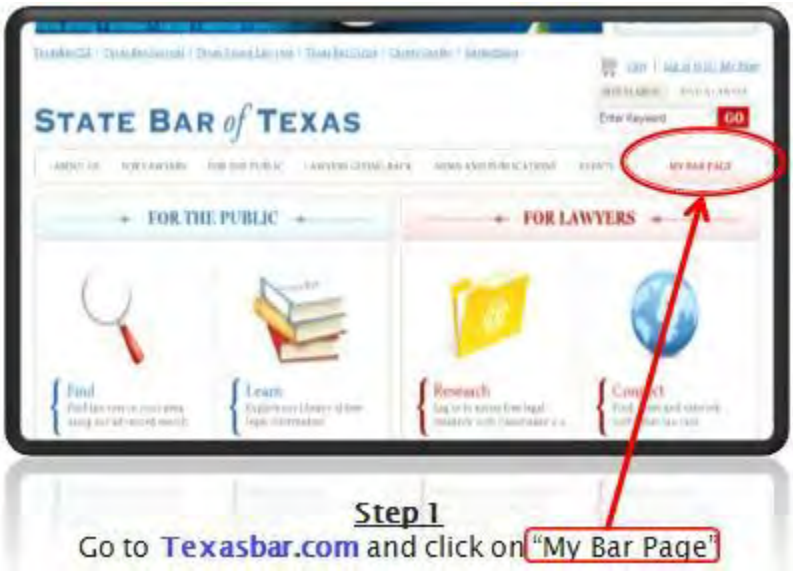
HB 4390 does more than create an advisory council. It also amends Texas' current data breach notification statute to require disclosure of a breach of certain personal data to be made no later than 60 days "after the date on which the person determines the breach occurred." What is considered a breach? "Breach of system security" is defined as "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data." In addition, the legislation (which takes effect September 1, 2019) imposes a duty on the part of the owner/licensor of the compromised data to notify the Texas Attorney General's office if the breach impacted 250 or more Texas residents. This notice must be provided within the same 60-day time period for notifying affected individuals. It must describe the nature of the breach, how many residents were affected, indicate the measures taken to remedy the breach, and state whether or not law enforcement is investigating. Since entities covered by this law are already facing substantial penalties from prosecution by the Texas Attorney General's office, compliance with these new requirements is well-advised.

About the Author

John 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 an adjunct professor at SMU Dedman School of Law and he serves as the Chair of the Computer & Technology Section of the State Bar.

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