Computer and Technology Section

Circuits

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

Table of Contents

Featured Articles

Op-Eds

Short Circuits

CircuitBoards

Table of Contents

Feature Articles:-

Op-Eds:-

Short Circuits:-

CircuitBoards:-

Letter from the Chair

By John G. Browning

As the end of the calendar year (but not the bar year!) approaches, it’s a great time to reflect on what the Computer & Technology Section has accomplished, as well as what lies ahead for the future. Membership is up, and we continue to be one of the fastest-growing sections in the State Bar. The Adaptable Lawyer CLE track was a tremendous success at the Annual Meeting in June 2019, and we are looking ahead to 2020. We have even more outstanding programming planned when the next Annual Meeting kicks off in Dallas. We’ve also continued to add to the many and varied technology CLE offerings for the State Bar, including more Tech Bytes and State Bar webcasts on thought-provoking subjects like artificial intelligence and its impact on the legal profession. By the time you read this, we will have had our annual CLE, “With Technology and Justice for All,” in Dallas featuring great topics and speakers, including a Texas Supreme Court Justice and a Houston Court of Appeals Justice. We’re also very proud of the variety and quality of articles that we continue to bring you in *Circuits*. Our Section members generously share their expertise on a wide variety of topics at the intersection of technology and the law, not only in CLEs for the State Bar and local bar associations, but in Tech Byte videos and articles that you read here, in the *Texas Bar Journal*, and in other legal publications. A number of our *Circuits* articles have even been reprinted with permission by national legal journals.

So how do we continue to live up to our mission of helping Texas practitioners navigate the murky waters of technology’s impact on the law and maintain competent representation of clients in an age that demands our awareness of the benefits and risks of relevant technology? By volunteering to help, of course. We need members who are interested in sharing their expertise as an author for *Circuits* or as a speaker. Perhaps you’ve just handled an interesting case that involves technology, or analyzed a recent decision for a motion or brief. Share that knowledge (and showcase your practice) through an article or presentation.

And even if you feel you don’t have the time to contribute an article or give a presentation, you can still support the Computer & Technology Section by spreading the word to prospective members. Every area of practice is impacted by technology, from daily practice management to the legal issues that we confront. So encourage your colleagues to join the Computer & Technology Section—that $25 investment pays big dividends!

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

COMPUTER AND
TECHNOLOGY
SECTION

Letter from the Editor

By Sanjeev Kumar

Welcome to the second issue of *Circuits* for the 2019-20 bar year!

We open this issue with an article by Council Member William Smith with discussion and analysis of recently enacted California's new Bot disclosure law and the proposed Federal legislation with its many parallels to the California law.

We continue with an article by Pierre Grosdidier (Past Editor and Council Member) discussing the legality of governments agents compelling a suspect to surrender the password for password-protected devices as follow up to his article in the previous issue of *Circuits* that dealt with the government agents compelling biometric unlock of protected devices.

Next, our former Section Chair Ron Chichester walks us through the emerging legal issues due to artificial intelligence (AI) as related to Intellectual Property ownership in copyrights and or patents or culpability of cyber criminals utilizing AI to commit those crimes and whether the disparate treatment of AI in the two situations can be reconciled.

In our great State of Texas, the ransomware attacks of multiple municipalities seem to confirm the old adage that everything is bigger in Texas. In the final feature article, Section Chair, John Browning discusses the multiple ransomware attacks on governmental entities in Texas.

In *op-eds*, yours truly discusses the vote by American Bar Association to urge the legal community to address the emerging ethical and legal issues with AI.

In *Short Circuits*, Pierre Grosdidier discusses the best practices for municipal entities in handling the mobility data sets as related to the privacy data associated with these data sets. Mobility data sets are fast emerging as a valuable tool for municipalities for urban development planning and for entrepreneurs for finding the right locals for their product/service offerings.

In the next article of *Short Circuits*, Ron Chichester discusses the ramifications of *United States vs. O'Rourke* court decision, where even a mistaken belief of stolen data to be trade secret was sufficient to incur liability even though the data may not have been trade secret.

In the third article of *Short Circuits*, John Browning discusses the patchwork of state privacy laws and how does our great state of Texas ranks among its peers.

In our *Circuitboards* section, Council Member Alex Shahrestani discusses a number of valuable tools available to practitioners of law to automate our practices in his article on Tech for Small Firms.

Finally, as the last article of *Circuitboards*, yours truly provides a brief outline of the proposed and possibly the new emerging landscape for copyright enforcement.

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

Kind Regards,
Sanjeev Kumar, Editor

FEATURE ARTICLES:-

Is that a Human Post?

By William Smith

Is That a Human's Post? California's New Bot Disclosure Law and Proposed Federal Parallels

Software that communicates with users in a way designed to mimic human interaction, commonly referred to as a "bot," has become an increasingly prominent feature of political and commercial activities over the past few years. With the introduction of SB-1001[1], California has recently become the first state in the U.S. to impose disclosure requirements on communications performed by a bot online. While the version of the statute enacted was significantly narrower than the original proposal, California may be a bellwether for future regulation in other states or at the federal level. As the underlying automation technology becomes more sophisticated, bot usages are likely to expand, raising public awareness about bot usage and potential harms and therefore the possibility of broader regulation. This article summarizes the history of the bot disclosure law in California and its requirements, as well as the expanded scope of the federal bot law proposed in Congress.

Background of California SB-1001

In the political context, public awareness of bot use developed mainly during and after the 2016 U.S. presidential election. Twitter found that 50,000 bots had accounted for nearly 500,000 retweets of then-candidate Trump's Twitter posts during the campaign, and the Clinton campaign's tweets had also been amplified by bot retweets, though at a lower rate[2]. Consumers are also interacting with "chatbots," which mimic interaction with human business representatives, with growing frequency: a March 2019 survey by software provider Salesforce found that 23% of customer service organizations surveyed currently used chatbots, and a further 31% planned to start using them within 18 months[3]. While chatbots often enable consumer benefits in the form of faster service and support, businesses also use social media bots in ways similar to political actors, to artificially increase the apparent popularity of their

[1] Sen. Bill 1001, 2017-2018 Reg. Sess. (Cal. 2018) (https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001).

[2] The New Yorker https://www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy July 2, 2019.

[3] Salesforce https://www.salesforce.com/blog/2019/08/chatbot-statistics.html August 4, 2019.

brands. This practice and the use of bots in politics were both cited in the Senate Floor Analysis presented with SB-1001[4].

California BPC §17940

SB-1001 added §§17940-17943 to the California Business and Professions Code, which became effective on July 1, 2019[5]. This statute makes it unlawful for any person to 1. "use a **bot** to communicate or interact with another person in California **online**," 2. "with the intent to mislead the other person about its artificial identity," 3. "for the purpose of knowingly deceiving the person about the content of the communication," 4. "in order to incentivize a purchase or sale of goods or services in a commercial transaction," 5. "or to influence a vote in an election."[6] It requires disclosure by providing that "a person using a bot shall not be liable under this section if the person discloses that it is a bot."[7] This disclosure must be "clear, conspicuous, and reasonably designed" to inform persons with whom it communicates that it is a bot[8].

"Bot" is defined as "an automated online account where all or substantially all of the actions or posts of that account are not the result of a person," meaning that periodic human supervision of an account is not sufficient to remove it from the scope of the disclosure requirement if "substantially all" of its activity is automated.[9] "Online" is defined as "appearing on any public-facing Internet Web site, Web application, or digital application, including a social network or publication."[10] The public-facing element means that most email, where use of marketing automation software is common, will be excluded[11].

While earlier drafts of the legislation would have imposed several responsibilities on social media platforms themselves, the final law does not, and in fact states explicitly that, "this chapter does not impose a duty on service providers of online platforms, including, but not limited to, Web hosting and internet service providers."[12] "Online platform" is defined as "any

[4] S. Rules Comm. Office of S. Floor Analyses, S. Floor Analyses, SB 1001, at 4 (Cal. Aug. 30, 2018) (http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB1001).

[5] California Business and Professions Code Chapter 6. Bots (Cal. BPC) §§17940-17943.

[6] Cal. BPC §17941(a).

[7] *Id.*

[8] Cal. BPC §17941(b).

[9] Cal. BPC §17940(a).

[10] Cal. BPC §17940(b).

[11] Research and Markets https://www.researchandmarkets.com/reports/4841395/marketing-automation-market-by-component September 2019.

[12] Cal. BPC §17942(c).

public-facing Internet Web site, Web application, or digital application, including a social network or publication, that has 10,000,000 or more unique monthly United States visitors or users for a majority of months during the preceding 12 months."[13]

The California bot disclosure law does not contain an explicit enforcement mechanism. It is possible that a violation of BPC §17941 could give rise to a remedy under California's false advertising statute, which provides for misdemeanor criminal liability and fines up to $2,500 per violation[14]. Additionally, there is precedent in California for interpreting an implied private right of action in a statute, but it is not clear that the bot disclosure law would meet this standard[15]. The lack of clear remedies or regulatory enforcement responsibility significantly limits the impact of the new law. The author is not aware of any litigation or regulatory actions under the law since it became effective. Given this, the law may be most significant as a preview of future regulation, perhaps at the federal level. Reviewing the legislative history of the bot disclosure law in California offers some insights into areas where debate and pushback is likely.

Legislative History of SB-1001

A number of interest groups, including the Electronic Frontier Foundation (EFF) and the Internet Association, an organization representing members of the technology industry including Facebook and Twitter, lobbied against provisions in the original draft of the bot disclosure legislation[16]. This lobbying resulted in two significant changes to the final legislation. First, in the original version of the legislation, the prohibited use of bots was broader as only the "intention of misleading" was required, without the additional purpose requirements in the final version of §17941(a)[17]. The EFF and other commentators argued that this lack of context

[13] Cal. BPC §17940(c).

[14] Cal. BPC §17500.

[15] See Richard Schwartz, *A Lack of Disclosure on Bot Disclosure,* Association of Business Trail Lawyers Report Los Angeles, Winter 2019, for further discussion on this point.

[16] The New Yorker https://www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy July 2, 2019.; Electronic Frontier Foundation https://www.eff.org/deeplinks/2018/10/victory-dangerous-elements-removed-californias-bot-labeling-bill October 5, 2018.

[17] California SB-1001 Amended Senate Bill March 14, 2018 ("March 2018 Draft") §17941(a) (https://leginfo.legislature.ca.gov/faces/billVersionsCompareClient.xhtml?bill_id=201720180SB1001&cversion=20170SB100198AMD).

limitation raised First Amendment concerns, and the added elements in the final version of §17941(a) reflect this critique.[18]

Second, the March 2018 draft of the statute imposed obligations on social media platforms to police users' compliance with the bot disclosure rules[19]. The EFF's lobbying was particularly critical of these provisions. It argued that the track record of content moderation by the platforms is poor, and that the difficulty of identifying who or what is behind a user would inevitably lead to policies against anonymous speech[20]. In the final version, this section was removed and changed to an exemption for online platforms (*see* above). With that change, the lowering of the minimum monthly users required to meet the definition of "online platform" from 50 million to 10 million had the effect of expanding the scope of the online platform exemption, because websites with fewer visitors could still enjoy protection by the exemption. Practically, social media providers would have the greatest ability to identify and remediate undisclosed bot accounts, so this change represented the most significant reduction in the impact the law could have on the ground. According to social media companies, existing content moderation is very costly[21]. It is likely that social media platforms were moved to advocate for removal of the obligations to police bot use on their platform by concerns of similar costs.

Proposed Federal Bot Legislation

Senator Diane Feinstein introduced S.2125 on July 16, 2019, which would regulate "the use of automated software programs intended to impersonate or replicate human activity on social media".[22] Senator Feinstein had previously introduced a bot regulation bill in 2018.[23] S.2125 contains findings that bots, including ones controlled by foreign actors, had a prominent role in the 2016 presidential election and that this activity was especially prevalent in key swing states in the electoral college.[24]

[18] Electronic Frontier Foundation https://www.eff.org/deeplinks/2018/10/victory-dangerous-elements-removed-californias-bot-labeling-bill October 5, 2018.; John Frank Weaver, *Everything Is Not Terminator,* Robotics, Artificial Intelligence & Law / November-December 2018, Vol. 1, No. 6, pp. 431-438.

[19] March 2018 Draft.

[20] Electronic Frontier Foundation https://www.eff.org/deeplinks/2018/10/victory-dangerous-elements-removed-californias-bot-labeling-bill October 5, 2018.

[21] Wired https://www.wired.com/story/facebook-community-standards-report/ May 23, 2019.

[22] Bot Disclosure and Accountability Act of 2019, S.2125, 116th Cong. (2019).

[23] Bot Disclosure and Accountability Act of 2018, S.3127, 115th Cong. (2018).

[24] S.2125 §2. Findings.

The law would direct the Federal Trade Commission to implement regulations (and give them enforcement powers) to require social media users to "publically [*id.*] disclose the use of any automated software program or process intended to impersonate or replicate human activity".[25] Similar to the original version of the California statute, the law would require social media platforms to enforce these rules on their platforms, including a process to identify bot posts, to mitigate attempts to disguise the use of bots, to remove undeclared bot posts it finds, and to allow for an appeal process where a user can demonstrate that a removed post was actually in compliance.[26] As with the March 2018 Draft of the California law, this is a key area which will determine how much impact the legislation actually has in practice. Therefore, if a federal bot regulation bill gets traction in Congress, it is likely that the major social media platforms will again marshal lobbying resources to seek to walk back these provisions.

Separately, the bill would amend the Federal Election Campaign Act of 1971 to prohibit candidates and political parties from using bots for campaign communications. A more limited set of prohibitions would also apply to political committees, corporations, or labor organizations within the scope of section 316(b) of the Election Campaign Act.[27] The last action on S.2125 was referral to the Committee on Commerce, Science, and Transportation.[28]

A parallel bill was introduced in the House of Representatives on September 26, 2019, without the campaign law amendment component.[29] It is currently before the House Committee on Energy and Commerce.[30]

Conclusion

The use of bots to influence voters and consumers via social media is one of many areas where technological capabilities have developed much faster than the law. California's bot disclosure law represents the first, albeit limited, attempt to regulate these activities, and is likely to be the beginning rather than the end of the policy conversation on this issue. Robert Hertzeberg, the California state senator who sponsored the law, told an interviewer "People have free

[25] S.2125 §4(b).

[26] S.2125 §4(c)(3) – (6).

[27] S.2125 §2.

[28] Congress.gov https://www.congress.gov/bill/116th-congress/senate-bill/2125 accessed November 14, 2019.

[29] Bot Disclosure and Accountability Act of 2019, H.R. 4536, 116th Cong. (2019).

[30] Congress.gov https://www.congress.gov/bill/116th-congress/house-bill/4536?s=1&r=5 accessed November 14, 2019.

speech. Bots are not people."[31] Others argue that the First Amendment should be construed broadly in this context, and should protect freedom of speech for artificial intelligence.[32] Regulation in this area also implicates social media and other technology companies, which have a financial interest in minimizing their compliance costs and significant resources to protect those interests. In those ways, the intersection of the First Amendment and bot speech is reminiscent of the question of First Amendment protection for corporate speech which the Supreme Court addressed in Citizens United.[33] It is likely that technological development will make these questions more pressing, and if further regulations are pursued we may see a similar level of tension between the impetus to protect speech itself and the need to protect individual political discourse among voters in a democratic system, as well as the interests of consumers.

About the Author

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

[31] The New Yorker https://www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy July 2, 2019.

[32] John Frank Weaver, Everything Is Not Terminator, Robotics, Artificial Intelligence & Law / November-December 2018, Vol. 1, No. 6, pp. 431-438.

[33] *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010).

The Fragmented Case Law Over Gaining Access to Password-Protected Devices

By Pierre Grosdidier

Can authorities compel a suspect to surrender the password to a protected device?[1] Even though this question's answer is squarely rooted in the suspect's Fifth Amendment rights against self-incrimination, the case law in this area is surprisingly fragmented and unsettled.[2] As a general proposition, and without more, a suspect cannot be forced to verbally surrender a password because such as act is a compelled and incriminating testimonial communication.[3] The touchstone of Fifth Amendment protection is the government's inability to force a suspect "to use 'the contents of his own mind'" to his or her prejudice.[4] For this reason, a suspect can be obligated to surrender the key to a safe, but not its combination.[5]

But, the Fifth Amendment suffers an important exception under the "foregone conclusion" exception. A suspect may be compelled to produce documents if the authorities can show that they know of their existence, location, and authenticating evidence with reasonable particularity. In that case, the suspect's production is not testimonial because it adds nothing to the authorities' knowledge of the documents' existence, location, and authenticity, which are a foregone conclusion. The suspect enjoys no Fifth Amendment protection because his mind is not used against him in the act of production.[6]

Courts have applied the foregone conclusion exception to adjudicate access to encrypted devices in different ways. In *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, the suspect invoked the Fifth Amendment to refuse to produce unencrypted laptops and hard drives that authorities suspected contained child pornography.[7] The Eleventh Circuit Court of

[1] *See* this article's companion piece: Pierre Grosdidier, *Can authorities compel a suspect to use his or her biometrics to unlock a digital device?*, Circuits, Sept. 2019, p. 7.

[2] For a more in-depth analysis of this topic, *see* Orin S. Kerr, Compelled Decryption and the Privilege Against Self-Incrimination, Tex. L. Rev., Vol 97, No. 4.

[3] *Sec. & Exch. Comm'n v. Huang*, No. 15-269, 2015 WL 5611644, at *4 (E.D. Pa. Sept. 23, 2015) (act of producing passcodes is testimonial in nature).

[4] *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1342, 1345 (11th Cir. 2012).

[5] *Id.* at 1345; *In re Search of [Redacted] Wash., D.C.*, 317 F. Supp. 3d 523, 535 (D.D.C. 2018) (mem. op.).

[6] *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1344.

[7] *Id.* at 1337-39.

Appeals held that the decryption and production of the devices' contents would amount to testimony by the suspect that he had "knowledge of the existence and location of potentially incriminating files, . . . possession, control, and access to the encrypted portions of the drives," and the ability to decrypt the files.[8] The Court reasoned that the act of production would require the use of the suspect's mind and could not be characterized as a merely physical act. Moreover, the foregone conclusion exception did not apply because the government did not show with reasonable particularity that it knew what the encrypted devices contained nor that the suspect could access them. For these reasons, the Court held that the suspect properly invoked his Fifth Amendment privilege.[9] In a similar possession-of-child-pornography case, the Third Circuit Court of Appeals upheld a district court's contempt order against a suspect who refused to decrypt hard drives on Fifth Amendment grounds because prosecutors adduced ample evidence that the devices contained incriminating contraband.[10]

In *G.A.Q.L. v. State*, prosecutors sought to compel a minor involved in an ethylated and deadly car accident to produce an iPhone passcode and an iTunes password.[11] Prosecutors argued that the act of surrendering the passcodes was not testimonial because their existence, custody, and authenticity were a foregone conclusion. The trial court agreed but, the court of appeals did not. It held that the foregone conclusion exception applied to the documents hidden behind the passcodes—the actual target of the inquiry—not to the passcodes. To hold otherwise would gut the Fifth Amendment's protections because "it would be a foregone conclusion that any password-protected phone would have a passcode."[12] The court concluded that in the absence of any specifics, let alone any reasonable particularity, as to the documents sought on the iPhone, the foregone conclusion exception did not apply and it quashed the district court's order.[13]

The Massachusetts Supreme Judicial Court reached the opposite result in *Commonwealth v. Jones*, a case of alleged sex trafficking.[14] The Court held that in a case of compelled decryption, the evidence sought is the passcode, not its device's contents, and that the suspect

[8] *Id*. at 1346.

[9] *Id*. at 1352.

[10] *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3rd Cir. 2017).

[11] 257 So. 3d 1058, 1059 (Fla. Dist. Ct. App. 2018).

[12] *Id*. at 1063.

[13] *Id*. at 1065; *compare with State v. Stahl*, 206 So.3d 124, (Fla. Dist. Ct. App. 2016) (foregone conclusion exception applies to passcodes, which are the target of prosecutors' inquiry).

[14] 117 N.E.3d 702 (Mass. 2019).

can only be compelled to enter the passcode to unlock the phone, but not disclose it.[15] Therefore, the foregone conclusion exception applied only when prosecutors showed beyond a reasonable doubt that the suspect knew the passcode.[16]

Jones is one of the few cases that has addressed the applicable standard for the foregone conclusion exception. In *United States v. Spencer*, the court held that applying the "reasonable particularity" standard to compelled decryption was "nonsensical."[17] The court reasoned that this standard applied to a situation where physical evidence could be described with more or less specificity, but was inapplicable in a situation where a suspect either could or could not decrypt a device. The court opted instead to place the burden on the government to show that the suspect could decrypt a device by clear and convincing evidence.[18]

The case law is otherwise replete with very fact-specific but otherwise interesting special cases. For example, in *United States v. Oloyede*, a suspect complied with an FBI agent's casual request to unlock her phone before she had been read her *Miranda* rights.[19] The suspect entered her passcode out of the agent's view, but later argued that "entering her passcode was a communicative act that amounted to self-incrimination."[20] The court held that hers was a voluntary statement and it upheld the district court's denial of her motion to suppress.

In *People v. Davis*, Davis offered his phone and passcode to a police officer to call his girlfriend to retrieve her car (which Davis was driving) following his arrest.[21] The police eventually used the passcode to search the phone pursuant to a valid warrant. Davis sought to suppress the results of the search, arguing that the police exceeded the scope of the consent under which Davis communicated his passcode. The Colorado Supreme Court held that a person does not retain any expectation of privacy in information voluntarily communicated to authorities, "'even if the information is revealed on the assumption that it will be used only for a limited purpose.'"[22] For this reason, it reversed the trial court's evidence suppression order.

[15] *Id.* at 711 nn. 9, 10.

[16] *Id.* at 714; *see also State v. Pittman*, No. A162950, --- P.3d ---, 2019 WL 5204815 (Or. Ct. App. Oct. 16, 2019) (same).

[17] No. 17-cr-00259, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018).

[18] *Id.*

[19] 933 F.3d 302, 308 (4th Cir. 2019).

[20] *Id.* at 308-09.

[21] 438 P.3d 266, 267 (Colo. 2019).

[22] *Id.* at 271 (citing *United States v. Miller*, 425 U.S. 435, 443 (1976)) (emphasis in original)). Note that *Davis* was decided on Fourth Amendment grounds.

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.

~~Corporate~~ AI Personhood: Avoiding Past Mistakes

By Ronald L. Chichester

1. Introduction

The intellectual property world has been dealing with a conundrum. How does the law handle authorship – and thus copyrightability – when artificial intelligence[1] (AI) generates new content?[2] Similarly, how does the law handle inventorship when AI is undeniably one of the inventors?[3] This is one area where copyright law and patent law have converged, albeit in an instructive way. Incidentally, intellectual property is not the only area affected by the designation (or not) of AI as a person. For the past decade, AI has taken on many of the cyber-security roles formerly handled by humans. Unfortunately, just as humans are susceptible to "social engineering,"[4] so too is AI susceptible to its own set of similar "social engineering" vulnerabilities that are being exploited by cyber-criminals precisely because AI is *not* treated as a person.[5] So how should the cyber-criminal statutes be updated to encompass crime committed via AI? Do we treat AI like persons for cybercrime, but not for intellectual property? How can we reconcile the disparate treatment of AI?

[1] For this paper, the words "artificial intelligence" have their broadest, or most general meaning. AI is often grouped in four different categories: "Acting as a Human" (the Turning Test approach); "Thinking as a Human" (the cognitive modeling approach); "Thinking Rationally" (the "laws of thought" or "logic" approach); and "Acting Rationally" (the rational agent approach). Stuart J Russell & Peter Norvig, ARTIFICIAL INTELLIGENCE, 3rd ed., 1-5 (2018). This paper does not limit AI to any particular category.

[2] *See, e.g.,* Thomas Macaulay, *Legal issues around IP for AI: Who owns the copyright on content created by machines?* TechWorld (January 26, 2018), https://www.techworld.com/data/ip-rights-for-ai-who-owns-copyright-on-content-created-by-machines-3671082/ (last visited Nov. 13, 2019); Andres Guadamuz, *Artificial intelligence and copyright*, WIPO Magazine (October 2017), https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html (last visited Nov. 13, 2019); Nicole Martinez, *Can an AI Machine Hold Copyright Protection Over Its Work?* Artrepreneur Art Law Journal (June 1, 2017), https://alj.artrepreneur.com/ai-machine-copyright/ (last visited on Nov. 13, 2019).

[3] *See, e.g., World-first Patent Application Filed for AI Inventor's Ideas,* E&T (August 1, 2019), available at: https://eandt.theiet.org/content/articles/2019/08/world-first-patent-application-filed-for-ai-inventor-s-ideas/

[4] *See e.g.,* "Social Engineering – Definition" Kaspersky Labs, available at: https://usa.kaspersky.com/resource-center/definitions/social-engineering

[5] *See, e.g.* Ryan Calo, *How New A.I. Is Making the Law's Definition of Hacking Obsolete,* Medium (August 21, 2019), https://onezero.medium.com/how-new-a-i-is-making-the-laws-definition-of-hacking-obsolete-eb2ab1a50961 (last visited Nov. 13, 2019).

With respect to AI, copyright law seems to have adopted the same approach that was established earlier by court precedent involving things *other* than AI. In the seminal (if not infamous) "Monkey Selfies" case, a seven-year-old crested macaque named Naruto became adept at taking selfies of himself with someone's cell phone – leading to a legal squabble over who could own (and thus sell) the subsequent novelty photos. In *Naruto v. David Slater*,[6] the Ninth Circuit held that the monkey's complaint "included facts sufficient to establish Article III standing because [the complaint] alleged that the monkey was the author and owner of the photographs and had suffered concrete and particularized economic harms."[7] The panel concluded that the monkey's Article III standing was not dependent on the sufficiency of People for the Ethical Treatment of Animals, Inc., as a guardian or "next friend."[8] However, the panel held that the monkey lacked statutory standing because the Copyright Act does not expressly authorize animals to file copyright infringement suits.[9] In other words, if you are not a human, you cannot get a copyright (although the non-human might be able to sue). What about corporations? It is well settled that corporations can be the owner of a copyright when a *human* employee created the work.[10] It is also well established that the user of software will own the copyright even when the software did the vast bulk of the content creation because, simply, it was the human that *caused* the software to generate the work. With respect to AI, it was a human who caused the AI to generate the work in the first place even if the human user had no idea what the AI would write, and so authorship would to be attributed to that human user. For copyright, the degree of autonomy matters less than the biological status of those involved.

The Patent statute and case law have taken a similar approach. Identifying the correct set of inventors is crucial to the validity of the patent in question, and is defined in Section 100 of the Patent Act.[11] Excluding an inventor from the patent can result in the patent being

[6] *Naruto v. David Slater*, 16-15469 (9th Cir. 2018), available at: https://www.courtlistener.com/opinion/4489119/naruto-v-david-slater/ (last visited on Nov. 13, 2019).

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] As a "work made for hire," with status denoted by the Copyright Act. *See, e.g.,* Copyright Office Circular 9 "Works Made for Hire," available at https://www.copyright.gov/circs/circ09.pdf.

[11] 35 U.S.C. 100, *et. seq.* See in particular § 100(f) "[t]he term "inventor" means the individual or, if a joint invention, the individuals collectively who invented or discovered the subject matter of the invention." *See also* § 116 (on inventorship).

unenforceable.[12] Currently, in the U.S., an inventor is designated as a "person"[13] who has to sign an oath or declaration,[14] although AI can be the source of prior art that can invalidate a patent.[15] However, in contrast to copyright law, corporations cannot be designated as inventors – even though both are equally treated as "persons" in other areas of law. While it is currently not known how the Patent Office will handle the AI-as-an-inventor issue, but my guess is that the designated "inventor" will be the human that caused the AI to perform the invention process, which should cause a redefinition of "one of ordinary skill in the art."[16]

In hindsight, Congress was working under a presupposition that the requisite thinking for authorship or inventorship could only have been performed by a human. However, rapid advances in AI have brought Congress' presupposition into question. Under both sets of IP laws, AI *could* be designated as a "person" if Congress so amended both Acts. Whether Congress *should* designate AI as a person is the subject of this article.

2. The Problem

There has been an enormous body of books, articles, conferences and other works about AI as a person or at least about AI being capable of thinking like a person.[17] The implications for the intellectual property laws (and law in general) are obvious. Interestingly, this question of

[12] *See*, 35 U.S.C. § 116; *Frank's Casing Crew & Rental Tools, Inc., v. PMR Techs., Ltd.*, 292 F.3d 1363 (Fed. Cir. 2002); *Trovan, Ltd v. Sokymat SA*, 299 F.3d 1292, 1302 (Fed. Cir. 2002).

[13] 35 U.S.C. § 102.

[14] 35 U.S.C. § 115.

[15] *See, e.g.,* European Patent Office, "What is prior art?", https://www.epo.org/learning-events/materials/inventors-handbook/novelty/prior-art.html (last visited on Nov. 22, 2019); AllPriorArt.com, https://allpriorart.com/about/ (last visited on Nov. 22, 2019) (uses AI and other algorithms to generate "inventions" that can be used as prior art to invalidate existing patents or cause the rejection of claims in patent applications); AllTheClaims.com, http://alltheclaims.com/ (last visited on Nov. 22, 2019) (uses AI and other algorithms to generate claims that can cited as prior art against patents and patent applications).

[16] *See, e.g.,* Ben Hattenbach & Joshua Glucoft, *Patents in an Era of Infinite Monkeys and Artificial Intelligence*, 19 Stan. Tech. L. Rev. 32 (2015); World Economic Forum, Artificial Intelligence Collides with Patent Law (April 2018), http://www3.weforum.org/docs/WEF_48540_WP_End_of_Innovation_Protecting_Patent_Law.pdf (last visited on Nov. 16, 2019). AI is also currently generating prior art citable against patent applications in the U.S. Patent Office. *See* "*All Prior Art: Algorithmically generated prior art*" at https://allpriorart.com/ (last visited on Nov. 16, 2019) which is a website that continually generates inventions to be used as prior art against later-filed patent applications.

[17] *See, e.g.,* John Brockman et al., WHAT TO THINK ABOUT MACHINES THAT THINK: TODAY'S LEADING THINKERS ON THE AGE OF MACHINE INTELLIGENCE (2015).

applying personhood status to AI parallels another – and very similar – line of inquiry, namely *corporate* personhood. Almost one hundred years ago, one of America's greatest philosophers, John Dewey, penned his seminal work on corporate personhood, which was later published in the Yale Law Journal in 1926.[18] Dewey was not the first (or last) to write on the topic, but he was the most cogent.[19] Considering what has transpired since he wrote that paper, Dewey was right to warn about the procrustean bed made by conferring the status of "person" onto a corporation. We should avoid the same mistake with AI.

Congress could be forgiven for allowing corporations to be treated like humans because there *were* humans acting behind the corporate veil. Moreover, humans were the *only* right-and-duty-bearing unit conceived under law. There had been centuries of law that focused on people before the notion of corporations was invented, the ancient practice giving rise to a presupposition toward the use of "person." Lawyers, a status-quo lot indeed, tend to apply *existing* words and legal concepts to new entities (or facts), rather than choosing the more difficult chore of inventing a new word or legal concept. However, as Dewey pointed out:

> If in justification of a particular decision in some particular and difficult controversy, a court supports itself by appealing to some prior properties of the antecedent non-legal "natural person," the appeal may help out the particular decision; but it either involves dependence upon non-legal theory, or else it extends the legal concept of "natural person," or it does both. This statement cuts in two ways. On the one hand, it indicates that much of the difficulty attending the recent discussion of the real personality of corporate bodies is due to going outside the strictly legal sphere, until legal issues have got complicated with other theories, and with former states of scientific knowledge; and on the other hand it suggests that law, at critical times and in dealing with critical issues, has found it difficult to grow in any other way than by taking over contemporary non-jural conceptions and doctrines. Just as the law has grown by taking unto itself practices of antecedent non-legal status, so it has grown by taking unto itself from psychology or philosophy or what not extraneous dogmas and ideas. But just as continued growth with respect to the former requires that law be again changed with

[18] John Dewey, *The Historic Background of Corporate Legal Personality*, 35 Yale L. J. 655 (1926).

[19] *See, e.g.,* Susanna Ripken, *Corporations Are People Too: A Multi-Dimensional Approach to the Corporate Personhood Puzzle*, 15 Fordham Journal of Corporate & Financial Law (2009); Susanna Ripken, CORPORATE PERSONHOOD (2019); Lucia M Rafanelli, *A Defense of Individualism in the Age of Corporate Rights*, The Journal of Political Philosophy (2017); Adam Winkler, WE THE CORPORATIONS: HOW AMERICAN BUSINESSES WON THEIR CIVIL RIGHTS (1 ed. 2019).

> great changes in further practices, just as, to be specific, the adoption of the law-merchant will not provide law adequate for the complex industrial relations of today, so it is even more markedly true that old non-legal doctrines which once served to advance rules of law may be obstructive today. We often go on discussing problems in terms of old ideas when the solution of the problem depends upon getting rid of the old ideas, and putting in their place concepts more in accord with the present state of ideas and knowledge. The root difficulty in present controversies about "natural" and associated bodies may be that while we oppose one to the other, or try to find some combining union of the two, *what we really need to do is to overhaul the doctrine of personality which underlies both of them*.[20]

Dewey foresaw that the (selectively) equal treatment of corporations as "persons" had extra-legal effect by diffusing the value of each human within the electorate, and that the super-human abilities of corporations are inherently anti-democratic because they give their owners undue representation within the government.[21] It is equally conceivable that if AI is similarly attached to the rubric of "person" then the owners of that AI could leverage still more undue representation within the government.

3. A Potential Solution

When Dewey suggested that an "overhaul of the doctrine of personality was needed," he himself was tantalizingly close to solving the riddle, but he did not take the last necessary step. I'm going to take that short intellectual step and suggest that the fits and conundrums that we currently encounter when trying to wedge artificial intelligence (or corporations) into the rubric of "personhood" are eerily similar to the types of problems encountered by astronomers who adhered to an Earth-centric version of astronomy. Copernicus solved many problems in astronomy by adopting a Sun-centric theory of the solar system. The important aspect of the change propounded by Copernicus was subtle but vital. He recognized that the Sun and Earth were both celestial bodies, but allowed their physical distinctions – rather than theological traditions – to guide his conclusions. As Dewey pointed out, Law has adopted a similar, theologically-tainted starting point – "person" – that has led to unwarranted

[20] Dewey, Corporate Legal Personality, *supra* note 16 at 657-658 (emphasis added).

[21] *See, e.g.,* Lawrence Lessig, Republic, Lost Version 2.0 (2nd ed. 2015).

conclusions, just as in pre-Copernican astronomy. [22] We too could avoid a great many legal and philosophical problems if we similarly adopt a non-person-centric theory of rights and duties in law over the current person-centric theory.

The question is, if not person-centric, than “what”-centric? Ideally, we would have a new word to describe some entity that has the capacity for rights and duties, a word that does not have any social/metaphysical/theological baggage. However, we need to go one step further. That word also cannot possess any *particular* rights or duties so that it can refrain from acquiring the aforementioned baggage. Unfortunately, lawyers were not in the habit of thinking of a right-and-duty-bearing unit in the abstract. Such a concept, however, can be borrowed from computer scientists, namely something they call a “base class.”[23] The base class does nothing, other than provide a framework for deriving other classes that actually *do* something. The base class has the core elements that are common to all of the derived classes, and thus represents the core essence of a thing. As Dewey has pointed out, for law, those common elements are *rights* and *duties*, to which I would add *characteristics*, because the characteristics that define the entity affect what rights and duties the entity is capable of but also distinguish it from other instances of like-classes. So our legal base class would be an “entity” that is capable of acting within an environment and would have rights, duties and characteristics.

As in computer science, the name of the base class is arbitrary, although as mentioned previously, picking the wrong name can lead to unintended consequences. Computer science actually solved that problem by prohibiting (or at least frowning upon) the use of a defined term of a programming language as the name of a class. I toyed with the idea of naming the base class “RADB” (Right-And-Duty-Bearing) (pronounced “radab”) but that was orally cumbersome. For this article, I am using word “agent” (in the most fundamental meaning) as that base right-and-duty-bearing unit because that word is derived from the Latin *agere*, to

[22] As Dewey pointed out: “The foregoing section [of his paper] does not attempt to define what it is to be a “person” in the sense of a right-and-duty-bearing unit. Its purpose is to show the logical method by which such a definition should be arrived at; and, secondly, to show that the question has been enormously complicated by the employment of a wrong logical method, and by the introduction of irrelevant conceptions, imported into legal discussion (and often into legal practice) from uncritical popular beliefs, from psychology, and from a metaphysics ultimately derived from theology.” Dewey, Corporate Legal Personality at 662-663.

[23] In object oriented programming, a base class is an object that has the framework for adding properties and methods for specialized methods. The use of a base class is to provide the framework for making other – more specialized – classes. *See, e.g.,* https://www.techopedia.com/definition/26896/base-class

do.[24] Secondly, each object oriented computer language has its own syntax for identifying where a particular class fits within the hierarchy of classes. For this paper, I have modified the "dot" notation common to JAVA[25], with a modifier that defines a class tacked on from the base class (with a ".") to reach the level within the hierarchy. [26] For example, a human being would be an agent.human. A human that is a citizen would be an agent.human.citizen because not all humans are citizens within a particular jurisdiction and citizens enjoy some rights (and duties) that others do not, which is useful when that distinction needs to be made for some reason. A corporation would be an agent.corporation. The federal government would be agent.government.federal. Similarly (and importantly), AI would be agent.AI. Such an arrangement suggests that some elements of autonomy and "thinkings" (however defined) are essential to the second level of the hierarchy. However, the elements that define the levels of the hierarchy have yet to be worked out, but can be, preferably in a democratic manner. Nevertheless, under the agent-centric theory, *law* would be defined as "the regulation of actions between agents within an environment."

While the notation adopted above may be cumbersome, it has the benefits of transparency and precision. Agent.corporations are easily distinguished from agent.humans. Yet while both are right-and-duty-bearing entities, they are ***expected*** to have distinguishable *sets* of rights and duties precisely because they have inherently different characteristics that caused them to be

[24] *See*, The Latin Dictionary, http://latindictionary.wikidot.com/verb:agere (last viewed on Nov. 14, 2019). Incidentally, the Latin form of agency, while the root of the Western view of agency, is distinct from non-Western views of agency. For example, some streams of Native American philosophy hold distinctly different views on agency. *See, e.g.,* Scott L. Pratt, *Persons in Place: The Agent Ontology of Vine Deloria, Jr.*, APA Newsletter, Spring 2006, Vol. 6, No. 1, pp. 4-9, https://cdn.ymaws.com/www.apaonline.org/resource/collection/13B1F8E6-0142-45FD-A626-9C4271DC6F62/v06n1American_Indians.pdf (last visited on Nov. 22, 2019) ("Deloria also proposes no simple attribution of a "human-like nature" to non-human others but, rather, argues for different "natures" in different forms of agency. Finally, it is important to note that Deloria does not hold that such vitalism marks a difference between what we view as animate and inanimate beings. Everything has its particular "vital force" manifested in its activities.") Consequently, the word "agency" has its own "baggage" and a completely new word should be adopted for the legal base class which has a rigorous definition that transcends philosophical and cultural traditions.

[25] *See, e.g.,* https://en.wikipedia.org/wiki/Java_(programming_language).

[26] *See, e.g.,* Nirosh, *Introduction to Object Oriented Programming Concepts (OOP) and More*, Code Project (Feb. 4, 2015), https://www.codeproject.com/Articles/22769/Introduction-to-Object-Oriented-Programming-Concep (last visited on Nov. 13, 2019). *See also, "abc — Abstract Base Classes,"* The Python Standard Library, https://docs.python.org/3/library/abc.html (last visited, Nov. 22, 2019).

distinguishable in the first place. Specific rights and duties would depend upon the place and role of the agent within the hierarchy and the characteristics defining that class. For example, an agent.AI and an agent.corporation can be owned by an agent.human, but an agent.human cannot be owned. Agent.humans can marry but agent.corporations cannot. Agent.corporations can merge, but agent.humans cannot. An agent.monkey could still take a photograph that would be owned by an agent.human to satisfy the current copyright laws. Congress could amend the Patent Act to allow an agent.AI (but not an agent.corporation) to be an inventor, but the ownership of the patent would rest with the owner of that agent.AI, precisely analogous to the practice under current copyright law.

An agent-centric viewpoint is also highly useful in identifying fallacies in case law. For example, when Congress passed the Reconstruction-era Fourteenth Amendment, they were clearly referring to agent.humans. Had we had the agent-centric theory in 1886, the Supreme Court would have had a much harder time applying the Fourteenth Amendment to agent.corporations as they did in *Santa Clara*.[27] Similarly, strict constructionists could easily argue that the Founding Fathers were referring *only* to agent.human.citizen when they drafted the free speech clause of the First Amendment, in stark contrast to the Supreme Court's contrary holding in *Citizens United*.[28]

Finally, one of the great things about computer science is that you can make up whole languages that cater to specific purposes. This means that we can create a computer language specifically for law as outlined above, and use that language to create software that mimics (or implements) legal relations between agents. Similarly, statutes could identify the specific classes of entities to which a particular law relates, providing proper guidance to lawyers and courts alike.

[27] *Santa Clara County v. Southern Pacific Railroad Company*, 118 U.S. 394, 6 S. Ct. 1132; 30 L. Ed. 118; 1886 U.S. LEXIS 1942 (1886) (which held that corporations are "persons" within the intended meaning of the Fourteenth Amendment).

[28] *Citizens United v. Federal Election Commission*, 558 U.S. 310, 130 S. Ct. 876; 175 L. Ed. 2d 753; 2010 U.S. LEXIS 766 (2010) (holding that restrictions on money expenditures by agent.corporations were unconstitutional because an earlier Supreme Court had given agent.corporations the same status as agent.human.citizen in *Santa Clara, Id.* The agent.corporation's characteristic of money highlights the procrustean bed made by the Supreme Court when they realized that agent.corporations did not have the same characteristics for speech that agent.humans possess. To remedy that shortcoming, the Supreme Court equated money from agent.corporations with traditional speech by agent.humans so that both could fit within the rubric of "person." The problem of course, is that the exchange of money does not convey information. Rather, money conveys influence and thus representation within government).

4. Conclusion

An agent-centric theory of law sidesteps the problems inherent with the person-centric theory, the latter being saddled with all of the unintended baggage identified by Dewey and others. The agent-centric theory is also a useful tool of inquiry to identify the sources of inequality and other injustices in society. The significance of the agent-centric theory for society is obvious and important because it can provide a rigorous framework for inquiry as well as for devising efficient solutions to common problems.

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 Committee 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.

Ransomware Attacks on Texas Governmental Entities

By John G. Browning

It is often said that everything is bigger in Texas. Unfortunately, that apparently includes ransomware attacks. On August 16, 2019, twenty-three local government entities in Texas, including a number of small north Texas cities, were hit by a coordinated attack by a single source using ransomware—a broad term given to describe malware that prevents or limits users from accessing their computer systems, either by locking the computer's screens or by encrypting the users' files until a ransom is paid. Even in a year that has witnessed cities like Baltimore and Albany similarly victimized, this ransomware strike made national headlines and is believed to be the largest such hack from a single source. With city functions from processing traffic ticket fines and other payments to issuing birth certificates crippled while the hackers demanded a collective $2.5 million in ransom, the episode has sent shock waves through not only the public sector, but the private sector as well.

Even before the attacks, ransomware attacks on businesses had been skyrocketing. According to antivirus firm Malwarebytes, the second quarter of 2019 witnessed a staggering 363% year-over-year increase in ransomware attacks directed against companies using its business software. TrendMicro's 2019 ransomware report also indicates that ransomware activity is on the rise, with over 40 million ransomware "detections" made between January and April of this year—compared to just over 50 million for all of 2018. And the costs of rescuing your files from attackers is going up as well. According to cybersecurity company Coveware, the average ransom paid per incident during the first quarter of 2019 was $12,762, nearly double the $6,733 average ransom during the fourth quarter of 2018. Coveware's *Ransomware Marketplace Report* also reflects that the average number of days that a ransomware incident lasts is going up as well, from 6.2 days in 2018 to 7.3 days in 2019—a reflection of more sophisticated ransomware techniques and use of encryption tools that are more difficult to defeat. Cyber Security Ventures estimates that a new organization will fall prey to ransomware every 14 seconds in 2019, with that figure jumping to every 11 seconds by 2021.

Small to medium-sized businesses, which typically spend less on cyber security, are the hardest hit by ransomware attacks. According to Beazley Breach Response Services, roughly 70 percent of ransomware attacks in 2018 targeted such companies, making an average ransomware demand of $116,000 (the highest reported ransom demand was $8.5 million). Healthcare companies were targeted more often than any other sector. Malwarebytes reports that, in the case of small and medium-sized companies, 37% of the ransomware attacks resulted from malicious email attachments. And for smaller businesses, the impact of a ransomware attack can be devastating: 22% of these victims had to cease business operations immediately.

For larger companies, ransomware attacks can be crippling as well. A variation of the "WannaCry" ransomware struck Taiwan Semiconductor Manufacturing Company (TSMC) during the summer of 2018, forcing it to temporarily shut down several chip-fabrication factories. In 2017, Reuters reported that the "NotPetya" ransomware attack had cost FedEx $300 million during the first quarter of that year. And in 2018, the criminal actors behind the "SamSam" ransomware launched an attack on the city of Atlanta's infrastructure, holding hostage municipal functions like paying bills or parking tickets while making a $51,000 demand. The city refused to pay, and instead incurred an estimated $17 million in recovery costs while spending an estimated $5 million to rebuild their infrastructure. In May of this year, hackers who targeted the city of Baltimore's computer system demanded about $76,000 in Bitcoin to unlock the city's files and allow municipal employees access to their computers. Mayor Bernard Young refused to pay, and over the next several months, the city spent over $5.3 million on computers and contractors to recover from the attack. One estimate puts the total impact, with not just city expenditures but loss of revenue as well, in excess of $18 million.

Given the staggering potential cost in terms of not just dollars but also reputational damage, the question becomes: to pay or not to pay? When Lake City, Florida was struck with a ransomware attack earlier this year, city leaders opted to pay the ransom demand—about $460,000 in Bitcoin—after considering the cost of reconstructing its systems. The FBI and most cybersecurity experts counsel against giving in to the hackers' demands, pointing out the lack of guarantees that such payments will restore access to computer systems and data, as well as the fact that payments will only embolden criminals and lead to more attacks and higher ransom demands in the future. The Texas Department of Information Resources (DIR), which is leading the investigation of the mass ransomware attack on Texas municipalities, reports that none of the affected entities paid any ransom, and in fact reported that within a week of the attack, more than half had resumed normal operations. By August 23, the DIR stated, "All the impacted entities had transitioned from assessment and response to remediation and recovery with business-critical services restored."

Cities across the country have been reeling from ransomware attacks. In late April, Cleveland's Hopkins International Airport was hit with a ransomware attack. Like the Texas municipalities, no ransom was paid and the city simply "moved on and fixed it." But not everyone has fared as well. In April as well, Augusta, Maine suffered a highly-targeted malware attack that froze the city's entire network and shut down the city center. That same month, hackers stole about $498,000 from the city of Tallahassee, Florida's employee payroll system. The city of Albany, New York spent over $300,000 recovering from a ransomware attack in March. What makes governments such inviting targets? The culprits behind such attacks assume—often correctly—that cash-strapped local governments are the least likely to have updated their cyberdefenses or backed up their data.

Texas governmental entities were targeted even before August's concerted attack. Earlier this year, Potter County government was crippled by a ransomware attack; county leaders voted against giving in to the attackers' demands, and by June 2019, the county had spent over $253,000 in data recovery costs. Lubbock County government systems were among the targets in the August attack, but fared better than their counterparts. The threat was over within 40 minutes of being detected, saving the county potentially hundreds of thousands of dollars and untold hours to restore lost files and repair computers. Isaac Badu, Lubbock County's first in-house director of technology and information systems, attributes this to training and resources that enabled technicians to recognize and respond to the attack quickly. Of course, not every local government has taken such steps, or has the resources to do so, and as a result such governments are increasingly targeted by cyberbandits. In 2017, 38 state and local systems were attacked; in 2018, that number surged to 53, and 2019 will certainly eclipse that.

But do municipalities that opt to pay the ransomware demands (like Del Rio, Texas did in response to a January attack) have the legal authority to do so? Texas is one of the few states with a ransomware-specific law on the books (2017's House Bill 9 criminalized ransomware), but neither the statute itself nor its legislative history mention ransom payment by the victim. Looking at other legal sources of authority, Texas Local Government Code Sec. 102.009(c) authorizes emergency expenditures in cases of "grave public necessity to meet an unusual and unforeseen condition." A ransomware attack would certainly seem to qualify. And in *Barrington v. Cokinos*, the Texas Supreme Court held that municipalities can pay private corporations "for the direct accomplishment of a legitimate public and municipal purpose." 338 S.W.2d 133 (Tex. 1960). So, while the U.S. Conference of Mayors recently passed a formal resolution discouraging cites from paying ransomware demands, Texas law at least apparently empowers local governments that choose to do so.

A ProPublica study suggests that insurance companies providing coverage for ransomware attacks and other cyber risks frequently recommend paying the ransom because it is cheaper than the cost of business interruptions, lost revenues, and fees for data recovery experts and lawyers. Fabian Wosar, chief technology officer for antivirus provider Emsisoft even went so far as to state that “Cyber insurance is what’s keeping ransomware alive today . . . They will pay anything, as long as it is cheaper than the loss of revenue they have to cover otherwise.” Dallas-based Steven Anderson, Vice President and Product Leader-Cyber for insurance giant QBE North America, disagrees. “The reality is that the average demand is between $5,000-$10,000,” he explained. “From an insurance carrier’s perspective, we want our insureds to have a solution that drives cost down, both for them and us. What we have seen is that by paying the ransom, those costs are mitigated in most cases.” The size of the company and its deductible are also factors, Anderson adds. “If the firm is a smaller firm, they may have a deductible that is well below the demand and therefore it makes sense to proceed with payment.” The costs of a ransomware attack, Anderson cautions, can be substantial, and include “investigation costs, legal liability, regulatory liability, business interruption, direct theft costs, and damage to customer relations and reputation.”

Of course, the ideal solution is to prevent one’s company or local government from being a ransomware victim in the first place. What lessons does this summer’s coordinated attack on 23 Texas municipalities offer for business owners and municipalities alike? Nationally-recognized cybersecurity/cyberliability attorney Shawn Tuma, a partner in the Plano office of Spencer Fane LLP, says this episode is a wake-up call for those companies who don’t consider themselves potential targets and plan accordingly. “For years, some companies and business owners have felt ‘hackers don’t care about us because our business is not that large or important’ or ‘because our data is not valuable to anyone’—well, your businesses’ data is valuable to your business and hackers have learned that if you don’t have access to your computer network or your data, you will pay to get it back because these days, nobody can run their business with a Big Chief tablet and a pencil.” Tuma also points out that there are legal dimensions mandating greater awareness of the risk of ransomware attacks. In addition to the various international, federal, state, and sometimes even local data breach notification laws that exist, he says, many companies have contractual agreements that obligate them to provide notice if they have had a cyber or data-related incident that impacts their network or data. “Most companies are not aware of these obligations and sign off on these agreements thinking ‘we’re not a technology company, this doesn’t apply to us’ when in reality, it does apply to them and they do not realize it until it is too late. Ransomware attacks may very well trigger these contractual obligations,” he notes.

Another key takeaway from the attack on the Texas municipalities, experts agree, is the importance of preparation. Small cities like Kaufman, Wilmer, and Keen may not have been prepared to deal with such a cyber assault, but the Texas DIR was, immediately implementing a previously established response plan that involved the support of at least 10 government agencies, including the Texas Department of Public Safety, Texas Division of Emergency Management, and the Texas A&M University System's Cybersecurity Critical Incident Response Team. Steven Anderson says prior planning involves multiple stakeholders, including IT professionals making sure that recovery systems are in place that include "proper patch management, offline backups, and software protection," as well as members of the legal department and compliance teams working with the CEO as first responders to develop an Incident Response Plan to assess and mitigate risk, including considering insurance coverage for such cyber risks. Companies "want to make sure proper processes are in place," Anderson observes, "so that when this occurs, the 'fire drill' doesn't cost the company time and money." And given the likely source of many ransomware attacks, Anderson adds, "TRAIN EMPLOYEES ON BEST EMAIL PRACTICES, and make spam filtering improvements."

Shawn Tuma agrees. "All companies need a cyber risk management program that is tailored to their unique needs . . . you need an Incident Response Plan and you need to practice the plan." Cyber insurance coverage can also play a critical role, Tuma points out, because when an attack occurs, "there are a lot of things that must be done very quickly in order to properly investigate and respond to it—those things are often quite expensive and, for many companies, the only way they have the financial ability to do those things is because they have cyber insurance." Tuma also recommends that companies use diligence and caution in vetting their IT services providers "and anyone else who has access to their data and networks."

With ransomware attacks on the rise, along with the cost of dealing with them, companies would be wise to remember the old adage, "An ounce of prevention is worth a pound of cure."

About the Author

John Browning is a partner in the Plano office of Spencer Fane LLP 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.

OP-EDS:-

Emerging Legal and Ethical Issues of AI

By Sanjeev Kumar

Earlier this year, the policy-making body of American Bar Association (ABA), its House of Delegates, passed a resolution dealing with the emerging ethical and legal issues related to the usage of artificial intelligence (AI) in the practice of law.

A number of issues that have been discussed in various applications of AI previously and were also included in the resolution passed by the ABA body include inherent bias, rationalization and explainability of such decisions, as well as transparency of automated decisions when using AI. Furthermore, the resolution included that there may be a need for guidance on ethical and beneficial usage of AI as well as a need to implement controls and oversight of AI and the vendors that provide AI.

The ABA Section on Science and Technology, which was the body that introduced the resolution, supported the adoption of the resolution with the rationale that legal practice is increasingly using AI for gains in efficiency as well as better accuracy in providing legal services, and although AI may offer multitude of advantages and benefits, it at the same time raises concerns regarding professional ethics.

Some of the uses of AI in practice of law, cited by the report included predictive coding in e-discovery, due diligence reviews, litigation analysis and legal research. The report referred to the ethical rule of duty of competency embodied within Rule 1.1, Comment 8 to be the main ethical issue for legal community when using AI in practice of law. There have been various articles written that discuss the inherent bias of the creators finding home in the AI system and one such example of this has been the claims against social media feeds having an inherent liberal bias, which has been referred multiple times by our political leaders, including President Trump. Most AI creators, for competitive reasons among others, are not willing to provide the details on the functioning of the system to enable the required transparency to analyze and root out any inherent biases. It has also been argued that the creators are unable to provide the details of the workings of the system due to lack of complete understanding even at their level (because AI system by definition learns and modifies its working with additional learnings).

In a similar vein to the discussion surrounding AI in other industry segments that have put AI to use, the ABA resolution or the report fails to provide much in the way of specifics with regard to how legal community should address these emerging issues.

Implementation plan of the resolution included a statement of intent to study a possible model standard for legal and ethical usage of AI by courts and lawyers and to use the resolution to promote continuing legal education related to AI. The report also referred to an additional purpose behind the resolution being to simply raise awareness of issues around the use of AI.

The United States criminal justice system is often criticized for its inherent racial bias based on prosecution and incarceration rates of minorities. Hopefully, the use of AI may help to overcome such criticism by removing these inherent human biases. On the other hand, considering the opaque nature of such AI systems when combined with absence of adequate controls and transparency, there is a danger that use of AI by the legal community may further exacerbate the issue. I guess the jury is still out!

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.

Short Circuits:-

Mobility Data Sets and Privacy Guidelines for Municipalities

By Pierre Grosdidier

Mobility data sets are the latest urban planning tool and a new data privacy frontier for municipalities. In their simplest form, these data sets are the GPS coordinates of persons or vehicles over time, often called "location stamps," from which city engineers can derive and analyze traffic patterns. They can be compiled from tracking Apps, public transportation smart card swipes, ride share service (*e.g.*, cabs, Uber, Lyft) data, rented scooter and bicycle pick-up and drop off data, toll road traffic data, Waze or GoogleMaps data, and, of course, automated license plate readers, just to name a few sources.[1] Municipalities want these datasets to better understand the movement of their citizens to improve traffic and better meet public service demands. Entrepreneurs want these datasets to make better investment decisions, such as where to best locate a gas station or a coffee bar.

But, as with everything that touches the Internet, we have just begun to see the potential applications. In Europe, the Horizon 2020 project CLASS[2] aims to share data in real time between drivers and their city.[3] Cameras and sensors located throughout a city will exchange data with cars to help improve traffic and road safety. For example, a driver who signals his or her intent to turn right at an intersection might be warned of pedestrians jaywalking ahead or children playing in the street.

Needless to say, municipalities or their contractors will quickly gain custody of massive mobility datasets. These datasets raise prickly privacy issues because an anonymized dataset can easily be crossed-checked with a deanonymized dataset to unmask personal identities. For example, repeated evening cab rides from a disreputable bar to a specific residential address can be linked to the homeowner's name through real property records. Last year, MIT researchers published the results of a study conducted on two large mobility datasets from

[1] Municipalities are not limited to the data they personally gather. They can agree to grant operating licenses (*e.g.*, Uber) in exchange for mobility data.

[2] CLASS is an acronym for edge and **CL**oud computation: **A** highly distributed **S**oftware for big data analytic**S**.

[3] Eduardo Quiñones, *Efficient distribution of big data analytics for urban mobility applications*, Intelligent Transport, Sept. 13, 2019.

Singapore.[4] One data set came from a network operator and the other from a transportation system. The researchers estimated that they could match individuals in the two data sets with a success rate of 17 percent with just one week's worth of data. Estimated "matchability" increased to 55 percent with four weeks' worth of data and to 95 percent with 11 weeks.

Anticipating these issues, the National Association of City Transportation Officials (NACTO) and the International Municipal Lawyers Association (IMLA) jointly developed principles and best practices to share, protect, and manage large mobility datasets.[5] The advocated principles are relatively general in nature and arguably short on specifics. Still, they are a start and they clearly map out the issues that municipalities must eventually confront. Ultimately, the industry that arises from mobility datasets will have to deal with the tension that exists between the data's granularity and their usefulness. Mobility datasets with a resolution of a few feet are rich with possibilities but will unavoidably raise privacy issues. Alternatively, datasets with resolution rounded to the nearest city block or residential neighborhood and that protect privacy might be of limited usefulness to traffic engineers.

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.

[4] Rob Matheson, *The privacy risks of compiling mobility data*, MIT News Office, Dec. 7, 2018.

[5] *Managing Mobility Data*, NACTO Policy 2019.

United States v. O’Rourke: Even the Mistaken Belief that Information was a Trade Secret is Sufficient to Incur Liability

By Ronald L. Chichester

An Illinois businessman was convicted of the *intent* to steal trade secrets[1] and was sentenced to one year (plus one day) in federal prison and a $100,000 fine. [2]

Robert O’Rourke worked as an engineer for Dura-Bar, a cast-iron manufacturing company in Illinois. He accepted a position with Hualong, a competitor located in China. Ironically, it was O’Rourke who was being secretive about the move to the new company, perhaps because he had downloaded 1,900 documents onto a personal hard drive before he left Dura-Bar’s employ. Dura-Bar got wind of the move. Authorities were alerted. Warrants were issued and O’Rourke was apprehended at the airport with the alleged contraband. Whether O’Rourke was too foolish not to have uploaded the documents to a harder-to-trace cloud account or instead he did not think that he needed to have bothered is unclear.[3]

In a post-conviction motion, O’Rourke’s attorney argued, *inter alia*, that the downloaded documents were not trade secrets, and thus his client was not guilty of any crime. Judge Andrea Wood of the Northern District of Illinois held that, for attempted trade secret theft, the government did *not* need prove that the underlying information was a trade secret. Instead, all that the government needed to prove was that the defendant *thought* that the underlying information was a trade secret when the defendant appropriated that information.[4]

Trying to taint the warrant with lack of underlying substance is unlikely to get the evidence excluded. According to criminal law attorney Grant Scheiner, the court probably will *not* exclude the evidence “as long as the police had a good faith belief that the warrant was valid.”

[1] In July 2017, a grand jury returned a 13-count Indictment against O’Rourke, charging him with stealing, downloading, and possessing trade secrets (and attempting to do the same) in violation of 18 U.S.C. § 1832.

[2] *See, e.g.*, https://www.winston.com/en/privacy-law-corner/convicted-businessman-intercepted-at-ohare-for-stealing-trade-secrets-sentenced-to-one-year-and-one-day-of-jail-time.html

[3] *Id.*

[4] *See*, http://tsi.brooklaw.edu/cases/us-v-o’rourke. As the Trade Secret Institute points out, Judge Wood relied upon U.S. v. Hsu, 155 F.3d 189, 198 (3d Cir. 1998) for the proposition that the *intent* to steal trade secrets was itself a stand-alone crime and did not require that there was actual theft of a trade secret.

Is there any circumstance in which the judge my strike the admission of evidence obtained as a result of a search warrant, which was issued on the basis of false information? According to Scheiner, in a criminal case, the answer is "yes" — but it's hard to prove and that limitation generally only applies to false information on the part of the government (typically, police), rather than a former employer. Scheiner noted that in *Franks v. Delaware*,[5] the Supreme Court held that statements in a search warrant affidavit that are either false or in reckless disregard for their truth must be excised from a search warrant affidavit. If, after excision of the offending information, there is no probable cause set forth in the remaining portion of the affidavit, then the entire search warrant fails and any evidence obtained as a result of the search warrant is inadmissible. However, the problem with this rule is that it only applies to the government (*i.e.*, the police). So, if a former employer gives the police false information, and that information forms the basis of a search warrant, it generally makes no difference, unless the defense can further show that the police either knew the information was false or adopted the information in reckless disregard for its validity.

Chapter 90 of Title 18, United States Code is a powerful tool to deter corporate espionage and theft of trade secrets. However, that same tool is ripe for abuse by unscrupulous employers who — with impunity — wish to harass departing employees.

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 Committee 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.

[5] Franks v. Delaware, 438 U.S. 154 (1978).

Texas and Privacy Protection

By John G. Browning

State laws governing data privacy have been justifiably compared to a patchwork quilt, providing widely varying levels of protection. A recent study by the U.K. technology research firm Comparitech evaluated all 50 states on how well they protect privacy through various types of privacy statutes. The result of the study can be accessed via the following link: https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/.

Perhaps not surprisingly, California tops the rankings with its numerous privacy laws, including the strict California Consumer Privacy Act (CCPA) of 2018. Delaware is ranked number 2, with Utah, Illinois, and Arkansas making up the rest of the top 5. What separates California from the rest of the states? California has a comprehensive digital privacy law, and is the only state with a law specifically protecting data from the Internet of Things (IoT). It's also the only state having a constitution that explicitly mentions an inalienable right to privacy[1].

Wyoming ranked the lowest of the states. How did Texas, one of only 3 states with a biometric privacy statute, rank? Surprisingly, Texas is clumped together with a number of "second tier" states with identical rankings like Kansas, Tennessee, and Alabama. The scores were based only on whether a state had enacted any of 20 different types of privacy protection laws, such as a law requiring employers to inform employees if they are monitoring emails or internet usage. However, the study's methodology has a few obvious flaws. For example, it only looks at whether a law has been enacted, not at the state's track record of actual enforcement. In addition, the survey doesn't take into account privacy protections that exist thanks to case law developments. So maybe Texas deserves a higher ranking after all.

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.

[1] All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. California Constitution, Article 1, Section 1.

Automate My Practice

By Alex Shahrestani

When running a solo practice, I like to think my goal is to figure out how to put on as few hats as possible. There's not enough time in the day to answer phones, keep client files, keep time, make notes, network with colleagues, network with clients, keep books, manage schedules, draft emails, and, at some point, practice law.

Thankfully, you're reading *Circuits* and likely recognize that new tools are available. In this article, I'm going to talk to you about one way to use Zapier. Zapier is an automation tool built on workflows. In the same way that you might have a checklist that you run through when working a particular type of case, Zapier runs through different workflows based on circumstances — except it's built on the functions of the digital tools you already use. Tying one piece of software into another is called integration. Zapier has over 1,000 integrations, including Gmail, Google Drive, Clio, Calendly, Acuity, Trello, and many, many more.

You might be wondering, as I did, what can actually be done with these integrations. When you click on any particular integration option, Zapier spurs the imagination for you by listing the most popular tasks. One task might be "If I send an email through Gmail, save it as a PDF to my Dropbox." Another might be, "If someone fills out this Typeform, create a folder in Google Drive."

I'm going to walk you through one of my workflows that saves me a good five to ten minutes per client.

Full disclosure: I don't use Zapier because I build my own systems to my own particular preferences; I use Zapier for inspiration, and I have used the free account version in order to test the functions. It's up to you to decide if Zapier is right for you. With any software, it's important to check the privacy policies to ensure you are staying within the bounds of your ethical obligations.

You'll be able to make this integration and test it with a free trial account. I'm assuming you have a Gmail account, which includes Google Drive and Google Forms, and a Calendly account, but you can substitute your own versions of those apps, like Typeform and Outlook. You'll need a Google Drive Folder with templates of files that you give to every client, a Google Drive

Form for Potential Clients that collects at least the client’s name and email address, and a Calendly link for scheduling a consultation.

Integrate Google Forms

1. Go to your newly minted Zapier Dashboard and click “Make a Zap.”
2. Select the app you are connecting. We’ll start with Google Forms.
3. It’ll ask you for a “Trigger Event,” select “New Response in Spreadsheet,” and click “Next.”
4. The Zap creator will ask you to “Choose an Account” by “Signing in to Google Form.” Click to sign in, and choose the account you want to associate with Zapier (whichever account holds the appropriate template folders), then click Continue.
5. Next, you will select the spreadsheet associated with your Google Form. There’s a search function available in the dropdown list on Zapier if you don’t see it in the dropdown list.
    a. If you’re unsure of which spreadsheet to use, or you don’t have one, you can identify the sheet by doing the following: i) go to your Google Form; ii) select the “Responses” tab; iii) click on the green Google Sheets icon; and, if you haven’t created a spreadsheet yet, it’ll give you the choice to iv) click on either “Create a New Spreadsheet” or “Select Existing Spreadsheet.”
    b. If you’re unsure, create a new spreadsheet and make note of the name for the next step.
6. In the next dropdown list, you’ll have to pick the page of the spreadsheet that you want Zapier to connect to. Often there will only be one choice. If there’s more than one choice, pick the page of the spreadsheet that has or will have the potential new clients’ responses.
7. Next, click “Test and Review.” If there’s any data in the spreadsheet, Zapier will present it to you. Click on one of the entries and verify that you’ve connected to the right form. If you don’t have any data in the sheet yet, take a minute to fill out the Google form with some data to test it. Once you’ve verified the data, click “Done Editing.”

Integrate Google Drive

1. Under “Choose App,” select Google Drive, then select “Create a Folder” under the second dropdown menu, “Choose Action Event.”
2. Under “Choose Account,” again select the account which hosts the template folders.
3. In the next screen, choose “My Google Drive” from the first dropdown menu; for “Parent Folder,” select where you would like the new client folder to be hosted; then under

"Folder Name," click on the icon to the right of the text input box — then select the option containing the client's name or business name, whatever is typically the case for you.

4. Click on "Test and Review," and verify that a new folder has been created with the expected name. Click "Done Editing," then click the plus sign.

Copy Standard Documents to the New Folder

1. Under "Choose App," select Google Drive, then select "Copy File" under the second dropdown menu, "Choose Action Event."
2. Under "Choose Account," again select the account which hosts the template folders.
3. Under "File," go to the dropdown list, and select or search for the document you wish to copy to every new client folder, such as a welcome packet.
4. For this example, select "No" for Convert to Document. We'll assume the file is already in a format suitable for its intended use.
5. Under "File Name," type in the name of the file, followed by a space, then click on the icon to the right of the text input and select the option containing the client's name or business name.
6. Select the appropriate Drive under "Drive." Leaving it blank will attach it to your account's personal Drive.
7. Under "Folder," scroll to the bottom and select "Use a Custom Value." Then under "Custom Value for Folder ID," click on the icon, select "Create Folder," then select "ID." The text input field should say something like "ID:" followed by a bunch of random numbers and letters.
8. Click on "Test and Review," and verify that a new folder has been created with the expected name. Click "Done Editing."
9. Repeat this section for each file you would like copied into the new client folder, then click the plus sign.

Integrate Gmail

1. Under "Choose App," select Gmail, then select "Send Email" under the second dropdown menu, "Choose Action Event."
2. Sign into the Gmail account you would like to contact the client through – most likely whatever account holds your client files.
3. In the "To" field, click on the icon, select "New Response in Spreadsheet," and select the value that holds the client's email address.

4. In the “Subject” field, type in whatever subject suits your practice — for example, “Welcome to Shahrestani Law!”
5. In the “Body” field, type in your welcome message, include a Calendly link, and use values from the spreadsheet for personal information.
    a. To personalize the email, wherever you would enter the client’s name, click the icon next to the text input box and select “New Response in Spreadsheet,” then select the value that holds the client’s name.
6. Click on “Continue,” then “Test and Review” to make sure the email formats as you intended.
7. Select “Done Editing,” then click on the toggle that says “Zap is ready – now turn it on!”

Verify

To verify that your Zap is working, go to the Google form you linked to your Zaps, and submit another test answer. In about twenty minutes, check to see that a new folder has been created, the correct files have been copied into the new folder, and that the email was sent with your Calendly link.

About the Author

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

Changing Landscape of Copyright Enforcement

By Sanjeev Kumar

Under current laws for copyrights, all copyright suits must go through federal courts, which is a costly and time-consuming remedy for copyright owners if they choose to enforce their copyrights through litigation. In my intellectual property practice, I often come across artists who claim copyright infringement, but more often than not, the infringer is a much larger entity and the cost of enforcing their copyrights is an insurmountable hurdle for them.

Internet has resulted in copyright infringement more common and pervasive. It has made it easy for potential infringers, especially those with primarily online businesses, to reproduce and use creative works from other artists. The breadth of data aggregators and multitude of online stores further increases the complexity, by orders of magnitude higher, the efforts required to monitor and enforce one's copyrights.

Earlier this year, a new measure was passed in the House of Representatives with an overwhelming vote that has the potential of drastically shaking up copyright enforcement. This new measure will create small claims court that would enable online content creators to go after their infringers in a small claims court instead of the conventional federal court system.

The Copyright Alternative in Small-Claims Enforcement Act (CASE Act), was approved by an overwhelming 410-6 vote in the House of Representatives. The bill was introduced last year with the goal of giving graphic artists, photographers, and other content creators a more efficient pathway towards receiving damages if their works are infringed. The CASE Act is intended to streamline the copyright infringement claim process by providing the Copyright Office with a tribunal of "Copyright Claims Officers" who would help to resolve infringement claims. The bill proposes the damages to be capped at $15,000 for each infringed work and $30,000 total.

However, groups such as Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) have sounded warning notes about possible unintended negative consequences of the CASE Act, such as it could result in costing the average internet user thousands of dollars for a simple act of sharing a meme. They warn that it could also lead to encroachments on citizen's First Amendment rights. The danger lies with the fact that although many of these cases may be legitimate, some are not, even if they are brought in good faith.

Another criticism of the proposed bill is in regard to the fact that both parties need to agree to go forward with this remedy. Other warnings have been sounded because previous changes like the Digital Millennium Copyright Act (DMCA) have been wrought with abuse. Often, a recipient of DMCA takedown notice will take down perfectly legal content protected under “fair use” entirely out of caution to avoid legal action, whereas in other cases, the recipient fails to take down legitimate infringers by playing judge and jury in ruling that it may be similar but not an infringement. In my practice, I have come across artists dealing with both sides of the above-mentioned scenarios.

Another possible unintended consequence of this proposed bill may be similar to what has happened with Patent Trial and Appeal Board (PTAB). The intention behind Inter Partes Review (IPR) hearings at PTAB was to reduce the cost and complexity associated with patent litigation to help individual inventors enforce their patent rights without undertaking a multimillion dollar patent infringement lawsuit. What has come to fruition as reality is that PTAB has been used by the patent infringers with financial means to openly infringe on patent owner’s rights and they have used the IPR hearings at PTAB to get the owner’s claims cancelled at an alarmingly high rate. This has resulted in devaluing of patents for individual inventors and startup. As a result, individual inventors and startups are putting reduced focus on filing of patents which can be demonstrated by the increasing proportion of patent applications being filed by companies with significant financial means.

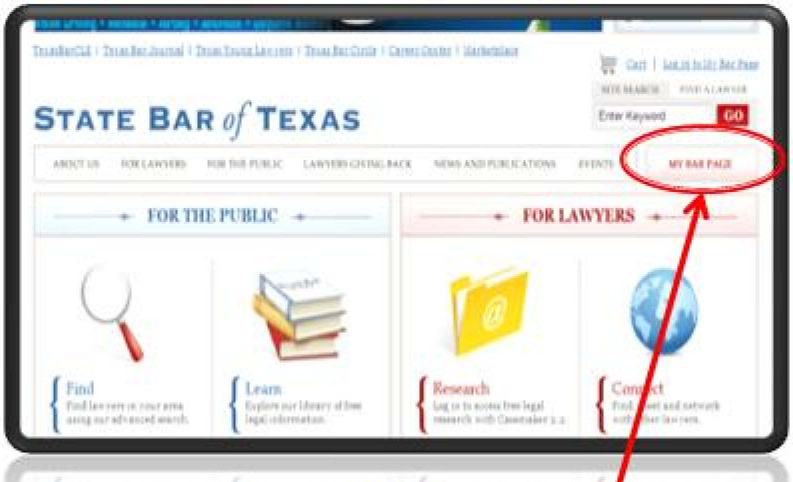
As it stands right now, the bill is already out of Senate Judiciary Committee and is awaiting a vote on the Senate floor.

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.

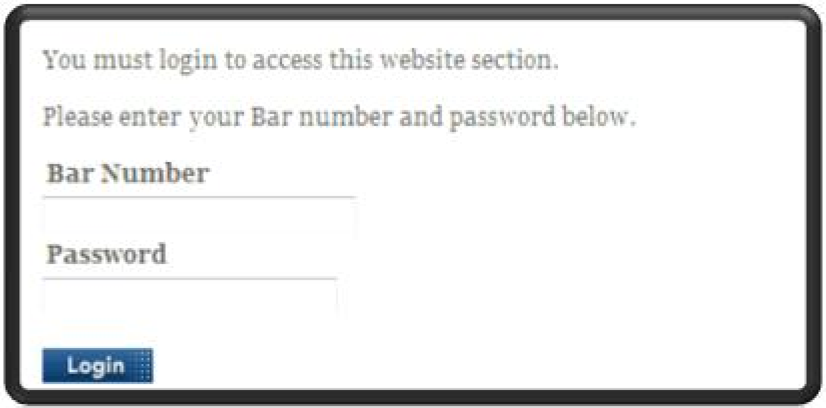
How to Join the State Bar of Texas Computer & Technology Section

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"



You must login to access this website section.

Please enter your Bar number and password below.

Bar Number

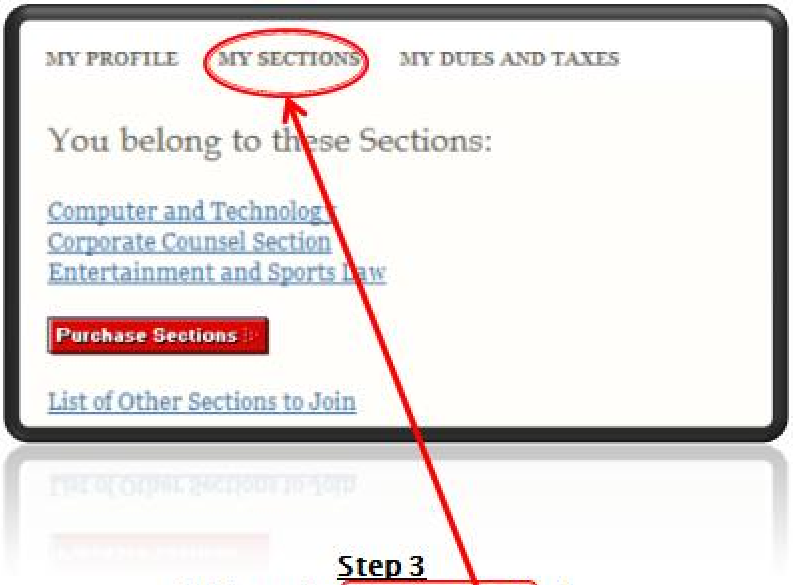
Password

Login

Step 2

Login using your bar number and password

(this will be the same information you'll use to login to the Section website)



You belong to these Sections:

Computer and Technology
Corporate Counsel Section
Entertainment and Sports Law

List of Other Sections to Join

Step 3

Click on the "My Sections" tab

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