Survey of the Law of Cyberspace: An Introduction

*By John A. Rothchild**

The global COVID-19 pandemic, which will soon enter its third year, continues to have an impact on e-commerce and cyberlaw. According to federal government statistics, in the first calendar quarter affected by the pandemic e-commerce sales rose an astounding 43.8 percent from the year-earlier period.[1] As face-to-face shopping gradually returned, the growth of e-commerce has returned to historical rates, but the volume of e-commerce sales remains at an all-time high. Although employers that early in the pandemic instantly directed their employees to work from home are gradually calling them back to centralized workplaces, it seems likely that the incidence of remote work will remain elevated compared to pre-pandemic levels, and that the increased use of online communication technologies will continue to generate novel legal issues.

The essays in this survey, which cover developments during the year ending May 2021, as usual touch upon a wide range of legal issues.

Privacy and data security. David Sella-Villa assesses the impact of the COVID-19 pandemic on privacy. The shift to working remotely has added avenues for collecting personal information that are not available in face-to-face communications. The essay notes that the Zoom teleconferencing platform is the subject of several lawsuits claiming that Zoom violated its users' privacy. It goes on to discuss the privacy implications of contact-tracing apps, vaccine mandates, and vaccine passports, as well as the impact of privacy protections on the ability of government to implement policies aimed at stemming the pandemic.

Meg Strickler provides an overview of several privacy-related developments. In a discussion of litigation based on misuse of data, she reviews ongoing lawsuits against Zoom and Google. She explains the impact of a decision by the Court of Justice of the European Union that upended the international protocol that has allowed personal information to be transferred from Europe to companies in the United States. She also reviews developments in biometric privacy: court decisions and settlements based on Illinois' biometric privacy law, proposed laws in other states, and bans on facial recognition technology.

Garylene Javier's essay looks at developments in state privacy laws. A primary focus is on the evolving landscape in California, which enacted the California

* Professor, Wayne State University Law School.

1. *Quarterly Retail E-Commerce Sales: 2nd Quarter 2021*, U.S. Census Bureau (Aug. 19, 2021), https://www.census.gov/retail/ecommerce/historic_releases.html.

Consumer Privacy Act ("CCPA") in 2018 and amended that law with the California Privacy Rights Act ("CPRA") in 2020. The essay includes a detailed look at regulations and amended regulations under the CCPA, as well as changes made by CPRA that will be effective in 2023. It also previews the new Virginia privacy law. The remainder of the essay discusses some of the early litigation under the CCPA.

Roland L. Trope discusses the paradigm shifts brought about by the recent occurrence of high-impact, low-frequency events such as the COVID-19 pandemic, enterprise adaptations to it, and a surge in cyberattacks on tech companies and critical infrastructure. He notes that attacks have become so sophisticated that the targeted companies can no longer determine with certitude whether their remediation efforts have succeeded. As a result, companies should henceforth assume that compromised networks remain persistently insecure. His essay reviews recent attacks, a judicial decision on a targeted enterprise's entitlement to insurance recovery for a ransomware attack, and a U.S. Supreme Court decision that resolved a conflict among the federal appellate courts on the proper construction of the Computer Fraud and Abuse Act.

Contracts. Nancy S. Kim offers a tour through the latest developments in online contracting. As she demonstrates, in recent cases the courts look beyond the point in time when the terms are presented and include in their assessment the totality of the user's interaction with the company. She also presents several cases dealing with the substance of contract terms, including applicability of the Federal Arbitration Act, drafters of the contracts arguing against the terms that they themselves produced, and companies reeling from the costs of enforcement of the arbitration clauses that they insisted on including in the contract.

Electronic payments and financial services. Stephen T. Middlebrook, Sarah Jane Hughes, Tom Kierner, and Peter Maskow address the complexities of electronic financial services. Their essay includes: disputes between federal and state authorities over the regulation of FinTech entities and virtual currencies; application of a money transmission statute to a virtual currency business; guidance from the Consumer Financial Protection Bureau regarding products that allow employees to obtain access to their salaries before they are paid and a court challenge to the Bureau's regulations governing prepaid accounts; and a warning from the Federal Trade Commission against using artificial intelligence algorithms that improperly discriminate.

Intermediary liability. Chase J. Edwards brings us up to date on developments relating to liability of online intermediaries. Two courts addressed negligent-design claims against Snapchat for its speed filter, holding Section 230 immunity was unavailable. Another case found Section 230 unavailable to shield Clearview AI from claims under state consumer protection law. Courts reached differing conclusions on whether Amazon.com is liable under state product liability laws for harm caused by products it sells. Several cases addressed the application of FOSTA, an amendment to Section 230 that denies immunity for websites that host content promoting sex trafficking. Finally, the essay considers legislative efforts to limit the applicability of Section 230.

Intellectual property. The essay by John A. Rothchild highlights some important developments in copyright and trademark law. The essay first describes the U.S. Supreme Court's ruling on fair use in connection with application programming interfaces in a high-profile dispute between Google and Oracle. It then discusses cases involving the volitional-conduct requirement for direct copyright liability and the making-available right. On the trademarks side, the essay examines a U.S. Supreme Court decision on the protectability of a domain name that is built on a term that is generic in the trademark sense, and another case dealing with the liability of the operator of an online marketplace based on infringing items that third parties offer for sale.

Consumer law. In his essay Richik Sarkar covers developments in advertising and consumer protection law. He discusses several cases that reach differing conclusions on the impact of a 2020 decision by the U.S. Supreme Court invalidating a provision of the Telephone Consumer Protection Act ("TCPA"), as well as a new decision by the Supreme Court clarifying what constitutes an automatic telephone dialing system under the TCPA. The essay also reviews cases involving social media accounts, the Computer Fraud and Abuse Act, deceptive online business practices, and cybersecurity.

The COVID-19 Pandemic One Year On: Finding Balance Between Privacy and Public Health

*By David Sella-Villa**

I. Introduction

During the COVID-19 pandemic stay-at-home orders and social distancing requirements limited the possibility of safe and lawful in-person interactions for over a year.[1] Many people in the United States responded to these circumstances by resisting challenges to their sense of decisional privacy—"non-interference in one's decisions and actions."[2] Instead, they chose to relinquish some data privacy[3] by sharing both new and existing types of data about themselves in efforts to enjoy the simulacrum of human contact.

Use of digital services that helped approximate in-person interactions increased dramatically.[4] Video conferencing features in Zoom and dating apps, for example, collected new types of data about people and offered novel means by which information once exchanged primarily in person could be collected, processed, and stored.[5] Privacy and data protection jurisprudence has helped address the circumstances where an individual's privacy interests may have been compromised. An overview of the privacy litigation involving Zoom

* David Sella-Villa serves as Interim Chief Privacy Officer for the State of South Carolina and is an adjunct professor at William & Mary Law School and the University of South Carolina School of Law. The views and opinions expressed in this survey are those of the author in his individual capacity, and do not reflect the opinions, policies, or positions of any of his employers or affiliated organizations or agencies.

1. *Compare* Cnty. of Los Angeles Dep't of Pub. Health, Order of the Health Officer, Safer at Home Order for Control of COVID-19 (Apr. 10, 2020), https://covid19.lacounty.gov/wp-content/uploads/HOO_Safer-at-Home-Order-for-Control-of-COVID_04102020.pdf, *with* Cnty. of Los Angeles Dep't of Pub. Health, Order of the Health Officer, A Safer Return Together at Work and in the Community (June 15, 2021), http://publichealth.lacounty.gov/media/coronavirus/docs/HOO/HOO_SaferReturnWorkCommunity.pdf.

2. Josephine Van Zeben & Bart A. Kamphorst, *Tracking and Nudging Through Smartphone Apps: Public Health and Decisional Privacy in a European Health Union*, 11 Eur. J. Risk Reg. 831, 835 (2021); *see also infra* Parts III & IV.

3. Bert-Jaap Koops et al., *A Typology of Privacy*, 38 U. Pa. J. Int'l L. 483, 500–01, 568 n.331 (2017) (discussing the terms "data privacy" and "informational privacy").

4. *E.g.*, *Activity on Dating Apps Has Surged During the Pandemic*, Fortune (Feb. 12, 2021, 11:30 AM), https://fortune.com/2021/02/12/covid-pandemic-online-dating-apps-usage-tinder-okcupid-bumble-meet-group/ (discussing the 70 percent increase in Bumble's video calls).

5. *See* David Sella-Villa, *An Early Evaluation of the Privacy Impacts of the Covid-19 Pandemic*, 76 Bus. Law. 261, 261–63 (2021).

(Part II) provides an illustrative example of some of the privacy consequences of the pandemic.

Many people have been reluctant to share data in more collective efforts at fighting the COVID-19 pandemic. Attempts at adding a digital layer to activities traditionally perceived to be data-light met strong resistance (Parts III and IV).[6] Decisional privacy and data privacy are compromised when some combination of infection, vaccination, location, and demographic data are aggregated, processed, and shared.[7] Discussions of the limited successes of tracking apps and policies related to the administration of the COVID-19 vaccine show that privacy interests during the pandemic may have trumped public health concerns.

II. Zoom Litigation Update

Online meeting platforms have served as the venue for activities that previously took place in person. The Zoom platform was subject to several privacy lawsuits.[8] Uninvited parties entered many private Zoom meetings and disrupted them by displaying graphic images—a practice known as "Zoombombing."[9] Zoom has since improved the security features of its platform,[10] but liability for potential privacy violations is being determined in court.

Several cases and two class actions alleging Zoom's privacy violations were consolidated into a proceeding styled *In re Zoom Video Communications Inc. Privacy Litigation*.[11] These complaints allege that Zoom violated users' privacy by "(1) sharing Plaintiffs' personally identifiable information with third parties; (2) misstating Zoom's security capabilities; and (3) failing to prevent security breaches known as 'Zoombombing.'"[12] The alleged causes of action include invasion of privacy, breach of implied contract, breach of the implied covenant of good faith and fair dealing, and violations of several California consumer protection statutes.[13]

By addressing its security issues, Zoom has limited incidents where uninvited parties have access to new data—the content of Zoom meetings intended to be

6. *See infra* notes 68 & 69 and accompanying text.

7. Jane Bambauer & Brian Ray, *COVID-19 Apps Are Terrible—They Didn't Have to Be*, LAWFARE (Dec. 21, 2020, 8:01 AM), https://www.lawfareblog.com/covid-19-apps-are-terrible-they-didnt-have-be [hereinafter *COVID-19 Apps*].

8. *The Boom in Zoom and Related Class Action Filings*, Buchanan Ingersoll & Rooney PC (Nov. 4, 2020), https://www.bipc.com/the-boom-in-zoom-and-related-class-action-filings.

9. *In re* Zoom Video Commc'ns Inc. Privacy Litig., No. 20-CV-02155-LHK, 2021 WL 930623, at *1 (N.D. Cal. Mar. 11, 2021).

10. Press Release, Fed. Trade Comm'n, FTC Requires Zoom to Enhance Its Security Practices as Part of Settlement (Nov. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement.

11. Order to Consolidate Actions and Set Scheduling Deadlines, *In re* Zoom Video Commc'ns Inc. Privacy Litig., No. 20-CV-02155-LHK (N.D. Cal. May 28, 2020), https://storage.courtlistener.com/recap/gov.uscourts.cand.357336/gov.uscourts.cand.357336.62.0.pdf.

12. *In re Zoom Video Commc'ns*, 2021 WL 930623, at *1.

13. *Id.* at *2. Though plaintiffs' claims of invasion of privacy by Zoom sharing PII with third parties were initially dismissed, the amended complaint has attempted to address this deficiency in the pleadings. Second Amended Consolidated Class Action Complaint at paras. 76–149, *In re* Zoom Video Commc'ns Inc. Privacy Litig., No. 20-CV-02155-LHK (N.D. Cal. May 11, 2021).

private. Independent of the outcome of the *Zoom Privacy* litigation, many organizations have decided to incorporate remote work into their post-pandemic business models.[14] This means that video communication technologies are likely to be a regular part of at least professional life,[15] and in some cases education,[16] healthcare,[17] and religious experiences as well.[18] Where technologies continue to replace in-person activities new data will continue be generated.[19] The privacy impact of these new data streams remains to be seen.

III. Contact Tracing

Digital contact tracing aided some countries in managing the COVID-19 pandemic.[20] Because of the prevalence of Apple and Android smartphones, the most readily available platforms for contact tracing apps have been the Apple and Google APIs.[21] Google and Apple made their jointly created contact tracing API available only to public health authorities, as a platform upon which they could develop their own contact tracing apps.[22]

Several features of these platforms that emphasized individual decisional privacy and data privacy over public health goals meant that contact-tracing apps have proven not to be an effective tool for U.S. public health authorities.[23] Individuals had to choose to download the contact tracing app, rather than having it pushed to their devices.[24] Individuals who downloaded the app then would have

14. *PwC's US Remote Work Survey*, PwC (Jan. 12, 2021), https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html.

15. *E.g.*, Husch Blackwell, *Husch Blackwell Announces Creation of Virtual Office* (July 13, 2020), https://www.huschblackwell.com/inthenews/husch-blackwell-announces-creation-of-virtual-office.

16. *E.g.*, *Guide to 2021–2022 Schedule of Classes*, DePaul Univ., https://resources.depaul.edu/student-success/success-strategies/Pages/course-modalities.aspx (last visited Sept. 12, 2021).

17. *E.g.*, Jered Wosik et al., *Telehealth Transformation: COVID-19 and the Rise of Virtual Care*, 27 J. Am. Med. Informatics Ass'n 957, 962 (2020).

18. *E.g.*, Jillian Cheney, *Virtual Reality and Livestreams: How Online Church Will Continue Post-Pandemic*, Religion Unplugged (June 1, 2021), https://religionunplugged.com/news/2021/6/1/why-church-online-will-continue-post-pandemic.

19. Other examples include restaurant food delivery and online counseling. David Curry, *Food Delivery App Revenue and Usage Statistics (2021)*, Bus. Apps (May 17, 2021), https://www.businessofapps.com/data/food-delivery-app-market/; Hannah Calkins, *Online Therapy Is Here to Stay*, *2021 Trends Report* Am. Psychol. Ass'n, https://www.apa.org/monitor/2021/01/trends-online-therapy (last accessed Nov. 11, 2021).

20. *See* Sangchul Park et al., *Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies*, 323 J. Am. Med. Ass'n 2129 (Apr. 30, 2020), https://jamanetwork.com/journals/jama/fullarticle/2765252.

21. Bobbie Johnson, *The Covid Tracing Tracker: What's Happening in Coronavirus Apps Around the World*, MIT Tech. Rev. (Dec. 16, 2020), https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker#usa-data.

22. Apple & Google, Exposure Notifications: Frequently Asked Questions 6 (Sept. 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf.

23. Privacy considerations hindered public health authorities from effectively using contact tracing apps to help slow the spread of COVID-19. *See COVID-19 Apps*, *supra* note 7.

24. Apple & Google, *supra* note 22, at 3–5. *But see* Ron Amadeo, *Even Creepier COVID Tracking: Google Silently Pushed App to Users' Phones [Updated]*, Ars Technica (June 21, 2021, 2:07 PM), https://arstechnica.com/gadgets/2021/06/even-creepier-covid-tracking-google-silently-pushed-app-to-users-phones/.

to choose to enter their COVID-19 status,[25] thereby preserving individuals' decisional privacy about whether to share their COVID-19 status with public health authorities.[26] The API only allows use of Bluetooth beacons alone, and not in combination with other location data,[27] thereby preserving greater data privacy by limiting the amount and type of location data collected about individual app users.[28] This and other potentially relevant data is stored on users' devices, not in a centralized location,[29] where it might be more easily correlated with other data relevant to stopping the spread of COVID-19.[30] Only then could public health authorities use the app to alert individuals that they have potentially been exposed to someone who may been infected with the coronavirus.

Due to their emphasis on decisional privacy and data privacy, "the [U.S.] COVID-19 apps in operation today are underpowered and undersubscribed."[31] In short, contact tracing apps in the United States did not have a negative impact on people's privacy because they were designed to prioritize decisional privacy. Though private entities may have been able to require employees or customers to use contact tracing apps (even ones with more effective, data-intensive options), public sentiment would likely be against it.[32]

IV. Vaccines, Data, and Privacy

According to public health officials, if a large enough percentage of the U.S. population receives a COVID-19 vaccine then "herd immunity" will stop the

25. Apple & Google, *supra* note 22, at 5.

26. This feature is a sharp contrast to Israel's contact tracing app, which does not give Israelis a choice whether to share their COVID-19 status. Tehilla Shwartz Altshuler & Rachel Aridor Hershkowitz, *How Israel's COVID-19 Mass Surveillance Operation Works*, Brookings (July 6, 2020), https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/ (describing how the Israeli Health Ministry provides the agency operating the Israeli tracking app "with the name, ID number, and cellphone number of individuals who have received a confirmed COVID-19 diagnosis").

27. *See* Ramesh Raskar et al., *Adding Location and Global Context to the Google/Apple Exposure Notification Bluetooth API*, Arxiv (July 25, 2020), https://arxiv.org/pdf/2007.02317.pdf.

28. For a discussion of the increased privacy impact of GPS location data in COVID-19 tracking apps as compared to the Bluetooth beacons used in Apple and Google API, see Dong Wang & Fang Lui, *Privacy Risk and Preservation For COVID-19 Contact Tracing Apps*, Chance, Oct. 7, 2020, at 49, 51–52, https://www.tandfonline.com/doi/pdf/10.1080/09332480.2020.1820252 ("GPS-based apps collect time-stamped GPS points from individuals on a 24/7 basis. . . . Unlike the GPS-based privacy-preserving scheme, the Bluetooth-based contact-tracing apps do not collect exact location information from their users, so users may feel more private and less anxious about their whereabouts being monitored 24/7.").

29. Apple & Google, *supra* note 22, at 5.

30. South Koreans' COVID-19 status was correlated with other centrally collected data sets such as credit card transactions, proximity to cell towers, and surveillance footage to facilitate more detailed contact tracing. Justin Fendos, *PART I: COVID-19 Contact Tracing: Why South Korea's Success Is Hard to Replicate*, Geo. J. Int'l Affairs (Oct. 12, 2020), https://gjia.georgetown.edu/2020/10/12/parti-covid-19-contact-tracing-why-south-koreas-success-is-hard-to-replicate/. For an example of a South Korean contact trace, see Gyuwon Jung et al., *Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People with COVID-19 in South Korea*, Frontiers Pub. Health 4 tbl. 2 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7314957/pdf/fpubh-08-00305.pdf.

31. *COVID-19 Apps*, *supra* note 7, at 2.

32. *See id.* at 5.

spread of the virus.[33] The vaccination program generates a tremendous amount of new data in the form of digital records of every vaccination.[34] To date, no level of government in the United States has required every resident in its jurisdiction to receive a COVID-19 vaccine.[35] The lack of a government-enforced vaccine mandate prioritizes decisional privacy. In preserving decisional privacy, efforts at achieving herd immunity use personal data from other sources to target populations with lower vaccination rates.

In the absence of vaccine mandates from governments, privacy considerations play an important role not only in administering vaccines but also in communicating vaccine status to help communities reopen without COVID-19-related limitations. Current activities relating to vaccine administration, vaccine mandates, and vaccine passports all raise interrelated decisional privacy and data privacy issues. From one perspective, an individual's vaccination status constitutes personal healthcare information.[36] But information about vaccine status is also relevant to public health authorities working to end a pandemic.[37] Considering the strong protections for healthcare information under U.S. law, the COVID-19 vaccination program must operate with careful attention to data privacy issues.

State, federal, and tribal programs have made COVID-19 vaccines widely available across the United States. Vaccination rates, though, vary greatly across sensitive demographic criteria such as race[38] and income levels.[39] Persons of color have suffered higher mortality rates from exposure to the coronavirus than white Americans.[40] Efforts to address these disparities involve consideration of at least two types of sensitive personal information—ethnicity and medical information.[41] From a privacy best practices perspective this may constitute

33. *See* Apoorva Mandavilli, *Reaching "Herd Immunity" Is Unlikely in the U.S., Experts Now Believe*, N.Y. Times (May 3, 2021), https://www.nytimes.com/2021/05/03/health/covid-herd-immunity-vaccine.html.

34. *See COVID-19 Vaccines That Require 2 Shots*, Ctrs. Disease Control & Prevention (June 3, 2021), https://www.cdc.gov/coronavirus/2019-ncov/vaccines/second-shot.html#vaccination-second-shot [hereinafter *CDC Second Shot*] ("Vaccination providers are required to report COVID-19 vaccinations to their IIS [immunization information system] and related systems.").

35. *See* MaryBeth Musumeci & Jennifer Kates, *Key Questions About COVID-19 Vaccine Mandates*, Kaiser Fam. Found. (Apr. 7, 2021), https://www.kff.org/coronavirus-covid-19/issue-brief/key-questions-about-covid-19-vaccine-mandates/.

36. *See Immunization Data Sharing, HIPAA, and MIIC*, Minn. Dep't Health, https://www.health.state.mn.us/people/immunize/miic/privacy/hipaa.html (last visited Sept. 12, 2021).

37. *Id.*

38. *COVID Data Tracker: Demographic Characteristics of People Receiving COVID-19 Vaccinations in the United States*, Ctrs. Disease Control & Prevention (June 17, 2021), https://covid.cdc.gov/covid-data-tracker/#vaccination-demographic.

39. *See COVID-19 Vaccination Rates: State-level and Subpopulation Evidence from the Household Pulse Survey—Update 4*, St. Health Access Data Assistance Ctr. (Mar. 25, 2021), https://www.shadac.org/news/covid-19-vaccination-rates-state-level-and-subpopulation-evidence-household-pulse-survey-0.

40. *COVID-19 Racial and Ethnic Health Disparities*, Ctrs. Disease Control & Prevention (Dec. 10, 2020), https://www.cdc.gov/coronavirus/2019-ncov/community/health-equity/racial-ethnic-disparities/disparities-deaths.html.

41. At least two states and several federal agencies consider ethnic and medical information "sensitive" data or information. Cal. Civ. Code § 1798.140(ae)(1)(D), (2)(B) (2021) (effective Jan. 1, 2023); Va. Code § 59.1–575 (2021) (effective Jan. 1, 2023); U.S. Census Bureau, DS022: Personally Identifiable

a new instance of data processing and therefore would necessitate a reexamination of the privacy risk[42] for the individuals potentially affected.[43]

The case of Stanford Medical Center highlights how a proposed vaccine distribution system could have exacerbated the disparate racial and social impact of COVID-19. The Stanford Medical Center proposed a vaccine distribution formula that prioritized age as a risk factor.[44] The result was a proposed distribution schedule that deprioritized vaccinations for front-line healthcare workers,[45] often the group that has the highest percentage of medical professionals who happen to be people of color.[46]

Private employers and educational institutions have issued vaccine mandates.[47] Decisional privacy is less of a legal issue in these established relationships because individuals lose some privacy protections to receive the benefits of employment or a formal education.[48] In many contexts employees and students must submit themselves to drug testing as a condition of their employment or education, thereby limiting the number of otherwise legal substances they

---

Information (PII) Breach Policy 4 (June 29, 2018), https://www2.census.gov/foia/ds_policies/ds022.pdf; Dep't of Homeland Security, Handbook for Safeguarding Sensitive PII 5 (Dec. 4, 2017), https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf; *CUI Category: Sensitive Personally Identifiable Information*, Nat'l Archives (May 27, 2021), https://www.archives.gov/cui/registry/category-detail/sensitive-personally-identifiable-info.

42. Nat'l Inst. of Stds. & Tech., U.S. Dep't of Commerce, NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management 30 (Jan. 16, 2020), https://doi.org/10.6028/NIST.CSWP.01162020 [hereinafter NIST Privacy Framework] ("Privacy Risk [is] [t]he likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.").

43. *Id.* at 23 ("Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's . . . governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.").

44. Deborah Lupton, *The Quantified Pandemic: Digitised Surveillance, Containment and Care in Response to the COVID-19 Crisis*, *in* Everyday Automation: Experiencing and Anticipating Automated Decision-Making (Sarah Pink et al. eds., forthcoming 2021), https://ssrn.com/abstract=3806386 (at pages 7–8 of draft chapter).

45. Eileen Guo & Karen Hao, *Pandemic Technology Project: This Is the Stanford Vaccine Algorithm that Left Out Frontline Doctors*, MIT Tech. Rev. (Dec. 21, 2020), https://www.technologyreview.com/2020/12/21/1015303/stanford-vaccine-algorithm/.

46. Nat'l Ctr for Health Workforce Analysis, U.S. Dep't of Health & Human Servs., Sex, Race, and Ethnic Diversity of U.S. Health Occupations (2011–2015) 12–13 (Aug. 2017), https://bhw.hrsa.gov/sites/default/files/bureau-health-workforce/data-research/diversity-us-health-occupations.pdf.

47. Michael J. Vernick, Molly E. Whitman & McKenzie F. Miller, *The Mandate Maze*, Inside Higher Ed (May 25, 2021), https://www.insidehighered.com/views/2021/05/25/advice-legal-issues-related-vaccine-mandates-opinion; Ryan Beene, *No Vaccine, No Desk: Firms Weigh Whether to Make Shots Mandatory*, Bloomberg (May 5, 2021, 5:00 AM), https://www.bloomberg.com/news/articles/2021-05-05/no-vaccine-no-desk-firms-weigh-whether-to-make-shots-mandatory. In late summer 2021 the prevalence of the COVID-19 Delta variant has spurred other employers to institute vaccine mandates. Michael Corkery et al., *After Months of Avoiding the Vaccine Issue, Companies Begin to Mandate*, N.Y. Times (Aug. 5, 2021), https://www.nytimes.com/2021/08/03/business/vaccine-mandate-employees-microsoft.html.

48. Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 Cornell J.L. & Pub. Pol'y 609, 619 (2009) ("an employee is entitled to virtually no expectation of privacy in the workplace"); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 657 (1995) ("students within the school environment have a lesser expectation of privacy than members of the population generally" (internal citation omitted)).

might consume. Employees and students might choose to limit their communications because technology use policies grant employers and schools access to electronic communications that would be considered private in other contexts. In the same vein, nothing under federal law prevents "an employer from requiring all employees physically entering the workplace to be vaccinated for COVID-19."[49] If an employer imposes such a vaccine mandate the Equal Employment Opportunity Commission cautions that information about an employee's COVID-19 vaccination is confidential medical information under the Americans with Disabilities Act.[50] This information "must be kept confidential and stored separately from the employee's personnel files."[51]

Consistent with privacy best practices, the separate storage of employees' COVID-19 information calls for a reexamination of the privacy risks for at least two reasons.[52] For many employers, this may be a new type of data. Employers who do not typically collect medical information will have to set up data governance separate from employees' personnel files to collect and store vaccination information. Some vaccine data repositories run by states have extensive policies and safeguards, such as de-identification and privacy audits, to help protect people's privacy interests.[53] Employers who fail to institute similar policies and safeguards may adversely impact their employees' privacy interests.

Additionally, vaccination rates have not been equal across protected classes under the federal employment laws.[54] The EEOC cautions that a vaccine mandate from an employer may have a discriminatory disparate impact.[55] Personnel files often contain information about employees' age, race, color, religion, sex, or national origin.[56] But because vaccine information must be kept confidential and stored separately from personnel files, an employer may not be able to correlate the two data sets to determine if in fact a vaccine mandate is having a disparate impact. These circumstances essentially pit privacy protection against discrimination avoidance. Employers with vaccine mandates can make reasonable accommodations[57] or offer incentives[58] aimed at limiting the potential discriminatory impact of the vaccine mandate, but the potential privacy impact of the proliferation of new data sets remains.

49. *What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws*, U.S. Equal Emp't Opportunity Comm'n K.1 (May 28, 2021), https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws [hereinafter *EEOC COVID*].

50. *Id.* at K.4.

51. *Id.*

52. *See* NIST Privacy Framework, *supra* note 42, at 23.

53. Ryan Blaney, *Federal Vaccination Tracking Raises Privacy Concerns*, Nat'l L. Rev. (Apr. 20, 2021), https://www.natlawreview.com/article/federal-vaccination-tracking-raises-privacy-concerns.

54. Hannah Recht, Rachana Pradhan & Lauren Weber, *Stark Racial Disparities Persist in Vaccinations, State-Level CDC Data Shows*, WebMD (May 20, 2021), https://www.webmd.com/vaccines/covid-19-vaccine/news/20210520/racial-disparities-persist-in-vaccinations-cdc-data-shows.

55. *EEOC COVID*, *supra* note 49, at K.1.

56. *EEO-1 Data Collection*, U.S. Equal Emp't Opportunity Comm'n, https://www.eeoc.gov/employers/eeo-1-data-collection (last visited Sept. 12, 2021).

57. *EEOC COVID*, *supra* note 49, at K.2.

58. *Id.* at K.16–K.21.

From a privacy perspective vaccine mandates are effectively a single exchange of data. An employee, for example, delivers proof of vaccination once and the employer makes a record of that event. Privacy protections apply to that single data record. Vaccine passports, though, are not limited to a single exchange of data. They require people to demonstrate their vaccination status to entities with whom they do not have established relationships. Privacy protections, therefore, need to cover any records created from each of these data exchanges.

The easiest way to protect privacy while proving vaccine status is to have no record of the data exchange. The entity that administers each vaccine provides recipients with a physical COVID-19 Vaccination Record Card ("Vaccine Card").[59] Just as a person might present her ID to a bouncer at a bar who visually inspects but does not retain it, so might she present her Vaccine Card and a form of identification for visual inspection by someone at the entrance to an establishment requiring vaccination. The establishment keeps no record of this data exchange. In this way the physical Vaccine Card serves as a vaccine passport.[60]

This approach to vaccine passports has several drawbacks. Vaccine Cards are too large for most wallets[61] and medical experts advise against laminating them.[62] Additionally, official Vaccine Cards can be difficult to replace.[63] For these reasons, people are reluctant to carry their Vaccine Cards around with them. Physical Vaccine Cards are easy to forge.[64] Establishments, therefore, have reason not to trust them. Digital vaccine passports address many of these concerns, but also have the potential to create a new data set—records of where someone presented a digital vaccine passport. This proliferation of data means that digital vaccine passports have potentially significant privacy implications.

New York's Excelsior Pass program serves as a useful example.[65] Built on IBM's Digital Health Pass technology, Excelsior Pass's privacy-protecting features

59. *See CDC Second Shot*, *supra* note 34.

60. This would be very similar to the "Yellow Card" the World Health Organization has used to show proof of yellow fever vaccination. *See* Sebastian Guidi, Alessandro Romano & Chiara Sotis, *Depolarizing the COVID-19 Vaccine Passport*, 131 YALE L.J. (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3850152 (at page 7).

61. *See* Chandra Steele, *How to Carry Your Vaccination Card on Your Phone*, PC MAG (May 24, 2021), https://www.pcmag.com/how-to/how-to-carry-your-vaccination-card-on-your-phone; Liza Corsillo, *What's the Best Way to Store and Protect My COVID Vaccine Card?*, STRATEGIST (Apr. 12, 2021), https://nymag.com/strategist/article/covid-vaccine-card.html.

62. Sara Berg, *6 Things to Tell Patients About Their COVID-19 Vaccine Card*, AM. MED. ASS'N (June 11, 2021), https://www.ama-assn.org/delivering-care/public-health/6-things-tell-patients-about-their-covid-19-vaccine-card.

63. *See id.*

64. *See* Jaclyn Diaz, *Fake COVID Vaccine Cards Are Being Sold Online. Using One Is a Crime*, NPR (June 8, 2021, 5:47 AM), https://www.npr.org/2021/06/08/1004264531/fake-covid-vaccine-cards-keep-getting-sold-online-using-one-is-a-crime.

65. The Excelsior Pass also shows proof of negative COVID test results. *Excelsior Pass: What You Need to Know*, N.Y. STATE DEP'T HEALTH, https://covid19vaccine.health.ny.gov/excelsior-pass-what-you-need-know (last visited Nov. 10, 2021) [hereinafter *Excelsior Pass*]. This feature is beyond the scope of this essay.

include decentralized data storage and data minimization.[66] When scanned at an establishment, "the Excelsior Pass Scanner app collects analytics about the type of Pass and the result of the scan. No personal information from Passes is collected or stored."[67]

Policy makers have weighed these privacy concerns against the social and public health need to end the COVID-19 pandemic. Some states, like New York, believe that their vaccine passport programs will produce public health benefits that outweigh the privacy impacts. New York's program has taken particular steps to address data privacy risks. Other states like Montana[68] and Arkansas[69] find the privacy costs of vaccine passports too great to bear, even considering the continued social and public health impact of the pandemic.

V. Conclusion

As long COVID-19 is part of daily life in the United States, choices balancing privacy and public health will need to be made. Only time and history will judge if the privacy impact of certain policies outweighed the public health consequences. New data related to the virus, its treatment, and policy outcomes will continue to be generated. Additionally, technologies that helped approximate in-person interactions have created new data streams. The privacy impact from this new data remains to be seen.

66. *See Governor Cuomo Announces Launch of Excelsior Pass to Help Fast-Track Reopening of Businesses and Entertainment Venues Statewide*, State N.Y. (Mar. 26, 2021), https://www.governor.ny.gov/news/governor-cuomo-announces-launch-excelsior-pass-help-fast-track-reopening-businesses-and. For a discussion of digital health credentials see Frost & Sullivan, Digital Health Credentials for COVID-19 and Beyond 5–6 (undated), https://www.ibm.com/downloads/cas/QRP1EP1V

67. *Excelsior Pass*, *supra* note 65.

68. Governor Greg Gianforte, Executive Order 7-2021 (Prohibiting Vaccine Passports), State of Montana (Apr. 13, 2021), https://governor.mt.gov/EO-7-2021-Prohibiting-Vaccine-Passports.pdf.

69. Ark. Code Ann. § 20-7-142 (2021).

Privacy Law Update

*By Meg Strickler**

I. Introduction

The privacy law landscape continues to evolve with new and emerging issues. This essay will address several significant legal developments in privacy law in the past year.[1] In the first case, *In re Zoom Video Communications Inc. Privacy Litigation*,[2] plaintiffs allege that their personal information was shared with third parties without permission and that Zoom misstated its security capabilities and failed to prevent various instances of "Zoombombing" (Part II.A). In *Brown v. Google LLC*[3] and *Calhoun v. Google LLC*,[4] the plaintiffs alleged that Google collected data from them without permission despite representing that it would not do so (Part II.B). Finally, in *Data Protection Commissioner v. Facebook Ireland Limited*,[5] the Court of Justice of the European Union held that the Privacy Shield Decision, which allowed personal information to be transferred from the European Union to the United States, was invalid (Part II.C). The essay ends with a brief update on biometric privacy (Part III).

II. Data Misuse Litigation

A. *In re Zoom Video Communications Inc. Privacy Litigation*

Plaintiffs are Zoom users who alleged—on behalf of themselves and two putative nationwide classes—that (i) Zoom shared plaintiffs' personally identifiable information, such as their device carrier, iOS advertiser ID, iOS Device Model, and iOS Version, with Facebook, Google, and LinkedIn, without their permission; (ii) Zoom "misstated the security capabilities and offerings of its services" as providing end-to-end encryption, which only allows the meeting participants, not Zoom, to decrypt the meeting; and (iii) Zoom failed to prevent "Zoombombing," which occurs when an unauthorized person joins a

* ABA Fellow, Steering Group Member, ABA International Law Section. Partner, Conaway & Strickler, PC. The author gratefully acknowledges the contributions of Althea Min Hyung Kang, Emory University School of Law, J.D. candidate 2022.

1. The impact of the COVID-19 pandemic on privacy law is addressed in David Sella-Villa, *An Early Evaluation of the Privacy Impacts of the COVID-19 Pandemic*, 76 Bus. Law. 261 (2021).
2. No. 20-CV-02155-LHK, 2021 WL 930623 (N.D. Cal. Mar. 11, 2021).
3. No. 20-CV-03664-LHK, 2021 WL 949372 (N.D. Cal. Mar. 12, 2021).
4. No. 20-CV-05146-LHK, 2021 WL 1056532 (N.D. Cal. Mar. 17, 2021).
5. Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).

meeting and displays pornography, screams racial epithets, or engages in similarly despicable conduct.[6] Plaintiffs' allegations are based on Zoom's promises that it does not sell users' data, adequately protects users' personal information, and that videoconferences are secured with end-to-end encryption.[7] Plaintiffs raised nine claims, including two that involved privacy: (i) invasion of privacy in violation of California common law and the California Constitution, art. I, § 1 and (ii) violation of California's Comprehensive Data Access and Fraud Act ("CDAFA"), an anti-hacking statute.[8] To bring a claim under CDAFA, plaintiffs must show that they suffered "damage or loss by reason of a violation" of the statute.[9] The court held that the plaintiffs failed to allege such damage inasmuch as they did not claim that their personal information was disclosed to a third party.[10] Therefore, the court granted Zoom's motion to dismiss this claim. The court also dismissed most of the Zoombombing claims, finding them barred by section 230(c)(1) of the Communications Decency Act.[11]

B. *Brown v. Google LLC and Calhoun v. Google LLC*

Plaintiffs in *Brown v. Google LLC*,[12] seeking to represent two nationwide classes, are Google account holders who used their browser in private browsing mode (which the Chrome browser calls "Incognito mode"). Plaintiffs alleged that Google collects private data[13] from them while they are in private browsing mode "through means that include Google Analytics, Google 'fingerprinting' techniques, concurrent Google applications and processes on a consumer's device, and Google's Ad Manager."[14] Plaintiffs additionally alleged that Google can tell when a Chrome user enables private browsing mode.[15] Plaintiffs alleged that they relied on Google's representations that it would not collect their private

6. *In re* Zoom Video Commc'ns Inc. Privacy Litig., No. 20-CV-02155-LHK, 2021 WL 930623, at *1 (N.D. Cal. Mar. 11, 2021).
7. *Id.* at *2.
8. *Id.* at *19.
9. *Id.* at *20.
10. *Id.*
11. *Id.* at *5–11.
12. No. 20-CV-03664-LHK, 2021 WL 949372 (N.D. Cal. Mar. 12, 2021).
13. The data that Google allegedly collects is:

    1. Duplicate GET requests, which allows Google to learn exactly what content the user is viewing;
    2. User's IP address, which is unique to the user's device;
    3. User's information identifying the browser software, including "fingerprint" data;
    4. User's IDs issued by the website to the user, which can be used to track the user across the web;
    5. User's geolocation; and
    6. User's information in Google cookies, that show the websites that users visited previously.

Id. at *1–2.
14. *Id.* at *1.
15. *Id.* at *2.

data while they were in private browsing mode.[16] Plaintiffs brought claims for invasion of privacy under California and federal law.[17]

Similarly, plaintiffs in *Calhoun v. Google LLC*[18] sought to represent Google Chrome browser users who "chose not to 'Sync' their [Chrome] browsers with their Google accounts while browsing the web."[19] Plaintiffs alleged that Google collects data[20] from users of Google Chrome regardless of whether a user is logged-in to her Google account. Plaintiffs alleged they relied on Google's promises that Chrome users "don't need to provide any personal information to use Chrome" and that the "personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync."[21]

In both *Brown* and *Calhoun*, Google moved to dismiss all claims based on consent and statutes of limitations. Google argued that plaintiffs in both cases consented to Google's collection of data. Google additionally moved to dismiss the claims under the Wiretap Act and Stored Communications Act, arguing that the websites, through which plaintiffs' data was collected, consented to Google's receipt of the data. Moreover, Google argued that all claims in both cases are barred by the statutes of limitations. While the facts are different, the court used the same reasoning to dismiss Google's motion to dismiss in both cases.

The court held that Google did not demonstrate plaintiffs' consent because Google did not notify users that Google engages in the alleged data collection. Consent is a defense to plaintiffs' claims, but it is the defendant's burden to prove consent. The court held that consent must be "actual" and the disclosure must "explicitly notify" users of the practice at issue.[22]

In *Brown*, the court reasoned that 1) Google's Privacy Policy does not disclose that Google would collect plaintiffs' private information while they were in private browsing mode and, thus, led a reasonable user to conclude that Google does not collect data from users in private browsing mode;[23] and 2) Google affirmatively represents that it cannot view users' activity when they are in private browsing mode.[24] Therefore, the court held that Google did not show plaintiffs'

16. *Id.*
17. *Id.* at *4.
18. No. 20-CV-05146-LHK, 2021 WL 1056532 (N.D. Cal. Mar. 17, 2021).
19. *Id.* at *1.
20. The data that Google allegedly collects is:

    1. The user's cookie identifiers;
    2. The user's browsing history;
    3. The contents of the users' POST communications;
    4. The user's IP address and User-Agent information; and
    5. The user's X-Client Data Header.

Id.
21. *Id.* at *2.
22. *Calhoun*, 2021 WL 1056532, at *7; *Brown*, 2021 WL 949372, at *7.
23. *Brown*, 2021 WL 949372, at *8.
24. *Id.*

consent to Google's collection of data in private browsing mode. The court reached the same conclusion in *Calhoun*, based on similar reasoning.[25]

The court also denied Google's motion to dismiss claims under the Wiretap Act and Stored Communications Act. Google argued that websites had given Google implied consent to intercept the users' data. But the court held that, even assuming that Google has established that websites *generally* consented to the interception of their communications with users, "Google does not demonstrate that websites consented to, or even knew about, the interception of their communications with users who were using Chrome without sync."[26]

In assessing plaintiffs' invasion of privacy and intrusion upon seclusion claims the court applied a two-element standard: 1) whether plaintiffs had a reasonable expectation of privacy and 2) whether the intrusion was highly offensive.[27] On the first element, the court considered "the amount of data collected, the sensitivity of the data collected, and the nature of the data collection," as well as Google's representations.[28] On the second element, the court engaged in "a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive."[29] The court concluded that the plaintiffs' allegations were adequate to support both elements.[30]

C. *Schrems II*

The issue in the case commonly referred to as *Schrems II*[31] is whether Facebook Ireland should be prohibited from transferring personal data of Maximillian Schrems, an Austrian national residing in Austria using Facebook, to Facebook Inc. in the United States. Schrems argued that the United States did not ensure an adequate level of protection of personal data transferred from the European Union ("EU") to the United States. The Court of Justice of the European Union agreed, holding that the Privacy Shield Decision[32] ("PSD") is invalid.

In the PSD, the European Commission had determined that "the United States ensures an adequate level of protection for personal data transferred from the Union to self-certified organisations in the United States under the EU-U.S. Privacy Shield."[33] In evaluating that determination, the court considered two issues: 1)

25. *Calhoun*, 2021 WL 1056532, at *8–9.
26. *Calhoun*, 2021 WL 1056532, at *10; *Brown*, 2021 WL 949372, at *11.
27. *Calhoun*, 2021 WL 1056532, at *15; *Brown*, 2021 WL 949372, at *18.
28. *Calhoun*, 2021 WL 1056532, at *16; *Brown*, 2021 WL 949372, at *19.
29. *Calhoun*, 2021 WL 1056532, at *16 (quoting *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 606 (9th Cir. 2020)); *Brown*, 2021 WL 949372, at *20.
30. *Calhoun*, 2021 WL 1056532, at *17; *Brown*, 2021 WL 949372, at *22.
31. Case C-311/18, Data Prot. Comm'r v. Facebook Ire. Ltd. (July 16, 2020), [hereinafter *Schrems II*].
32. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46 on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1.
33. *Schrems II*, *supra* note 5, at para. 45. The Privacy Shield Framework provides companies in the United States and the EU with a mechanism to comply with data protection requirements when transferring personal data from the EU to the Uinted States in support of transatlantic commerce.

whether the limitations on the protection of personal data under U.S. law are delimited in a sufficiently clear and precise manner; and 2) whether effective administrative and judicial redress exists for an individual to pursue a legal remedy for unlawful processing of his or her personal data.[34]

On the first element, the court held that the U.S. surveillance programs based on section 702 of the Foreign Intelligence Surveillance Act ("FISA") and Executive Order ("E.O.") 12333 do not lay down clear and precise rules for limiting their power to interfere with the fundamental rights conferred by the Charter.[35] The court, therefore, held that the surveillance programs in the PSD fail to include adequate safeguards.

On the second element, the court held that no effective judicial remedy exists with respect to the U.S. surveillance programs. The court found that section 702 of FISA and E.O. 12333 do not grant data subjects rights enforceable in the courts against U.S. authorities.[36] E.O. 12333 additionally states that at least some legal bases that U.S. intelligence authorities may use are not covered.[37] Thus, the court held that the Privacy Shield Decision also does not meet the second element.

The court's holding in *Schrems II* poses significant challenges to U.S. businesses or private entities in requesting the transfer of personal data from the EU to the United States. To overcome these challenges, the U.S. government clarified the meaning of existing legislation to demonstrate that the use of personal data is delimited in a clear and precise manner *and* that the United States has redress mechanisms in place for those individuals harmed by the transfer of personal data. In September 2020, a trio of U.S. government agencies published a white paper titled *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers After* Schrems *II* ("White Paper").[38] The White Paper explains that it is "not intended to provide companies guidance about EU law or what positions to take before European courts or regulators," but rather provides an "up-to-date and contextualized discussion of . . . U.S. law and practice."[39] Three main points of the White Paper are: (i) most U.S. companies do not engage in data transfers that are of interest to U.S. intelligence agencies and, therefore, do not pose types of risks that are concerned in *Schrems II*; 2) the U.S. government frequently shares intelligence information with EU Member States for terrorism or related purposes and such information-sharing serves important EU public interests; and 3) *Schrems II* does not take account of new developments in the United States since the Privacy Shield Decision.[40]

34. *Id.* at paras. 176, 188.
35. *Id.* at para. 184.
36. *Id.* at paras. 181–82.
37. *Id.* at para. 191.
38. U.S. Dep't of Comm. et al., Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers After *Schrems II* 1 (Sept. 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.
39. *Id.*
40. *Id.* at 1–2.

Private entities that previously relied on the Privacy Shield framework may wish to make use of what are known as Standard Contractual Clauses governing the transfer of personal data between the EU and the United States. As the White Paper explains, companies that take this route "are responsible for undertaking their own independent analyses of all relevant and current U.S. law relating to intelligence agencies' access to data, as well as the facts and circumstances of data transfers and any applicable safeguards."[41]

In other words, a well-worded contractual clause may strengthen a business's claim that the business itself can provide a sufficient level of protection for personal data transferred from the EU to the United States

III. Biometric Privacy

Illinois's Biometric Information Privacy Act ("BIPA"), enacted in 2008, was the first state statute that regulated the use of an individual's biometric information. BIPA defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[42] BIPA offers a justification for regulating the use of biometric identifiers and information: "[b]iometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[43]

BIPA provides a private right of action, allowing individuals, often representing a class, to bring lawsuits against corporations for violations of BIPA. A notable class action case is *In re Facebook Biometric Information Privacy Litigation*,[44] in which the U.S. District Court for the Northern District of California approved a $650 million settlement for a class of more than 6 million individuals.[45] The plaintiffs in this action alleged that Facebook violated BIPA section 15(a)[46] and (b)[47] by collecting and storing users' biometric data, such as digital scans

41. *Id.* at 1.
42. 740 Ill. Comp. Stat. Ann. 14/10 (2021).
43. *Id.* 14/5(c).
44. No. 15-cv-03747-JD, 2021 U.S. Dist. LEXIS 36801 (N.D. Cal. Feb. 26, 2021).
45. *Id.* at *28.
46. 740 Ill. Comp. Stat. Ann. 14/15(a) (2021) ("A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first . . . .").
47. *Id.* 14/15(b). The section states: "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

of their faces, without prior notice and consent in connection with Facebook's Tag Suggestions feature for users' uploaded photos.[48]

Courts have reached different results on the issue of whether a violation of BIPA meets the injury-in-fact requirement for Article III standing. The Seventh Circuit held in *Thornley v. Clearview AI, Inc*. that merely alleging the defendant's violation of BIPA section 15(c) without alleging that the plaintiffs suffered any injury as a result of the violation does not meet the injury-in-fact requirement. Because the allegation describes "only a general, regulatory violation," the court affirmed the district court's decision to remand the case to state court.[49] In contrast, the same court in *Fox v. Dakkota Integrated Systems, LLC* held that the defendant's alleged failure to develop and comply with a data-retention schedule as required by BIPA section 15(a) gave rise to harm satisfying the injury-in-fact requirement.[50] Earlier cases too reached different outcomes.[51] The outcomes of the cases depend on whether the plaintiffs stated claims under a particular BIPA provision and alleged a particularized harm or risk of harm as a result of the violation of BIPA.[52]

Following the enactment of BIPA, several other states enacted or are in the process of enacting comparable legislation. Texas[53] and Washington[54] adopted statutes in prior years, but neither of these includes a private right of action. Maryland[55] and New York[56] are each considering similar bills. As with BIPA, Maryland's and New York's bills provide a private right of action.

The major differences between BIPA and the bills in New York and Maryland rest on the definition of biometric identifier and the notice requirement. First, while the New York bill mirrors the definition of biometric identifier in BIPA, the Maryland bill excludes a specific reference to "scan of hand or face geometry." Instead, Maryland generally refers to "other unique biological" patterns or characteristics used to identify a specific individual and further adds "generic print"[57] to the definition.[58] Second, BIPA and the New York bill require that

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

Id.

48. *In re Facebook*, 2021 U.S. Dist. LEXIS 36801, at *6.

49. 984 F.3d 1241, 1248 (7th Cir. 2021).

50. 980 F.3d 1146, 1154–55 (7th Cir. 2020).

51. *E.g.*, Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020) (standing found for § 15 (b) claim but not for § 15(a) claim); Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019) (standing found for claims under § 15(a) & (b)); Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 15 (2d Cir. 2017) (no standing for a procedural violation that presents no "risk of real harm").

52. *Thornley*, 984 F.3d at 1246; *Fox*, 980 F.3d at 1153.

53. Tex. Bus. & Com. Code § 503.001 (2009).

54. Wash. Rev. Code Ann. § 19.375 (2017).

55. S.B. 16, Legis. Assemb. Reg. Sess. 2021–22 (Md. 2021), https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0016?ys=2021RS.

56. A.B. A27, Legis. Assemb. Reg. Sess. 2021–22 (N.Y. 2021), https://www.nysenate.gov/legislation/bills/2021/A27.

57. *Id*.

58. S.B. 16, *supra* note 55, § 1 (adding § 14-4301(B)(1)).

the entity seeking to collect or obtain an individual's biometric identifier must provide notice of the collection and obtain the individual's consent.[59] Maryland's bill includes no such requirement.

Some state and local governments, in recognition that the facial recognition technology reinforces racial biases and contributes to privacy erosion,[60] have banned or limited certain uses of facial recognition technology. Virginia[61] has banned the use of facial recognition by police, and Washington[62] has imposed limitations on government's use of facial recognition technologies. Some cities, including San Francisco,[63] Minneapolis,[64] and Boston,[65] passed ordinances prohibiting the use of facial recognition technologies by police and/or city officers. The city of Portland (Oregon) has prohibited the use of facial recognition technologies by private parties in places of public accommodation.[66]

In 2021, the U.S. House of Representatives passed the George Floyd Justice in Policing Act, prohibiting any use of facial recognition technologies by federal law enforcement officers wearing a body camera.[67] The Act provides that "[n]o camera or recording device authorized or required to be used under this part may be equipped with or employ facial recognition technology, and footage from such a camera or recording device may not be subjected to facial recognition technology."[68]

IV. Conclusion

The privacy law landscape continues to evolve. Data security and biometric privacy will continue to remain top concerns. Staying ahead of the various issues will force businesses and companies to evolve and keep pace. Companies will need to continue to develop policies and procedures to combat the increasing litigation and new technologies will need to continue to monitor the ever changing landscape of U.S. privacy law.

59. 740 Ill. Comp. Stat. Ann. 14/15(b) (2021); A.B. A27, *supra* note 56, § 1 (adding § 676-B(2)).
60. Brian Fung, *Facial Recognition Systems Show Rampant Racial Bias, Government Study Finds*, CNN (Dec. 19, 2019), https://www.cnn.com/2019/12/19/tech/facial-recognition-study-racial-bias/index.html; Shira Ovide, *A Case for Banning Facial Recognition*, N.Y. Times (June 9, 2020; updated Jan. 31, 2021), https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html.
61. Va. Code Ann. §§ 15.2-1723.2, 23.1-815.1 (2021).
62. Wash. Rev. Code Ann. § 43.386 (West 2021).
63. S.F., Cal., Ordinance No. 103-19 (2019).
64. Minneapolis, Minn., Code of Ordinances ch. 41 (2021).
65. Bos., Mass., Ordinance No. 16-62 (2020).
66. Portland, Or., City Code ch. 34.10 (2021).
67. H.R. 1280, 117th Cong. (2021).
68. *Id.* § 374.

State Privacy Law Developments

*By Garylene Javier**

I. Introduction

The key developments in state privacy laws during the survey year occurred primarily in California and Virginia. The California Privacy Rights Act of 2020 ("CPRA")[1] expands consumer rights by amending the California Consumer Privacy Act ("CCPA").[2] The regulations issued by the California attorney general clarify how businesses are to comply with their CCPA obligations. Virginia's Consumer Data Protection Act[3] ("VCDPA") establishes a framework for controlling and processing personal data, making Virginia the second jurisdiction to adopt a comprehensive privacy law. The key provisions of these two state laws are discussed in Part II, and Part III touches on litigation under the CCPA.

II. State Privacy Legislation

A. California

The two principal developments affecting California state privacy law are: i) the issuance of regulations[4] and amended regulations[5] implementing CCPA and ii) adoption of the CPRA.[6]

The California attorney general issued regulations in June 2020 providing guidance on how to implement CCPA's requirements. The regulations address

* Garylene Javier is an associate and a Certified Information Privacy Professional (US) in the Washington, D.C. office of Crowell & Moring LLP. She is an ABA Business Law Section Fellow of the Cyberspace Law Committee and a Young Lawyer Representative to the Privacy and Data Security Subcommittee of the Consumer Financial Services Committee.

1. California Privacy Rights Act, 2020 Cal. Legis. Serv. Prop. 24 (to be codified at Cal. Civ. Code §§ 1798.100–199.100) (herein referenced as "CPRA"). California residents voted the CPRA into law when it was presented on the November 2020 ballot as Proposition 24. Text of California Proposition 24, https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020) (last visited Oct. 22, 2021). However, certain provisions became effective on January 1, 2021 (e.g., extension of the employee and business-to-business exemptions).

2. Cal. Civ. Code §§ 1798.100–1789.199.100 (eff. until Jan. 1, 2023).

3. Virginia Consumer Data Protection Act, 2021 Va. Laws 1st Sp. Sess. ch. 35 (S.B. 1392) (eff. Jan. 1, 2023) (herein referred to as "VCDPA").

4. The original CCPA regulations became effective August 14, 2020. *CCPA Regulations*, State of Cal., https://oag.ca.gov/privacy/ccpa/regs (last visited Sept. 12, 2021).

5. Amendments to the CCPA regulations became effective March 15, 2021. *Id.*

6. See *supra* 1.

how businesses must provide notices to consumers,[7] verify consumer identity and handle requests to exercise consumer privacy rights (i.e., right to know, right to access, right to delete, right to opt-out),[8] ensure consumers can exercise their privacy rights without discrimination,[9] and implement protections for consumers under sixteen years old.[10] After the initial version of the regulations became effective in August 2020, amendments to the regulations became effective on March 15, 2021 and included provisions amending certain opt-out requirements, such as the manner of providing the opt-out notice if collecting information offline,[11] the ability for businesses to use an opt-out icon in addition to, but not instead of, the requirement to post the notice of the right to opt out or a "Do Not Sell My Personal Information" link,[12] and the requirement to allow consumers to opt out using a mechanism that has a minimal number of steps and forbidding the use of "a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out."[13]

Although the regulations provide guidelines for implementing the CCPA's requirements, they do not offer any templates or model language for businesses to use when drafting privacy notices and policies. There is currently no indication of whether such guidance is forthcoming.

In November 2020, after the initial version of the CCPA regulations was finalized on June 2020, California voters passed the CPRA, which is known colloquially as "CCPA 2.0" and modifies certain consumer rights that the CCPA granted:

- **Creates a new enforcement and oversight landscape**. The CPRA establishes the new California Privacy Protection Agency, with authority to bring an administrative enforcement action against businesses that violate the CCPA. The agency may assess an administrative fine of $2,500 for each violation, or $7,500 for each intentional violation involving the personal information of minors under sixteen years old.[14] The attorney general will retain enforcement authority over the CPRA.[15] However, for administrative enforcement actions, the CPRA no longer provides a thirty-day right to cure an alleged violation.[16]
- **Amends the definition of "business."** The CPRA amends the definition of "business" under the CCPA and defines a "business" as an entity that either (i) has annual gross revenues in excess of $25 million in the preceding calendar year, (ii) buys, sells, or shares the personal information of

7. Cal. Code Regs. tit. 11, §§ 999.304–999.308 (West, Westlaw through June 11, 2021 Register 2021, No. 24).
8. *Id.* §§ 999.312–999.326.
9. *Id.* §§ 999.336–999.337.
10. *Id.* §§ 999.330–999.332.
11. *Id.* § 999.306(b)(3).
12. *Id.* § 999.306(f).
13. *Id.* § 999.315(h).
14. 2020 Cal. Legis. Serv. Prop. 24 (to be codified at Cal. Civ. Code § 1798.155(a)).
15. *Id.* § 1798.199.90.
16. *Id.* § 1798.155(a).

100,000 or more consumers or households (which increases the threshold of consumers from 50,000 to 100,000 and drops the reference to devices that was in the CCPA), or (iii) derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.[17] The CPRA also provides that a business includes any entity that controls or is controlled by a business, that shares common branding with the business, and with whom the business shares consumers' personal information.[18] A joint venture or partnership where each business has at least 40 percent interest is now considered a "business" under the CPRA.

- **Creates and expands consumer rights**. The CPRA grants consumers the new right to request that a business correct inaccurate personal information.[19] It also allows consumers to opt out of a business' *sharing* of personal information, an expansion of the original CCPA's right to opt out of *selling*.[20] However, the definition of "sharing" of personal information is limited to sharing, disclosing, or otherwise communicating a consumer's personal information to a third party for "cross-context behavioral advertising," regardless of whether any money changes hands.[21]
- **Expands protection from discrimination**. The CCPA prohibits businesses from discriminating against a consumer who exercises his or her rights.[22] The CPRA expands this right (i.e., prohibiting retaliation) to employees who exercise their privacy rights.[23]
- **Adds a new category of personal information**. The CPRA adds "sensitive personal information" as a new category of personal information protected by the law.[24] "Sensitive personal information" includes log-in or account information, along with any required security or access code, password, or credentials allowing access to the account. Additional categories of personal information include certain identifiers (e.g., social security number), geolocation, race, non-business-related communications (e.g., email, mail, text), genetic data, and biometric information.[25] Businesses collecting sensitive personal information must disclose the purpose of its collection, the categories of information collected, and whether it is sold or shared.[26]

17. *Id.* § 1798.140(d)(1).
18. *Id.* § 1798.140(d)(2).
19. *Id.* § 1798.106(a).
20. *Id.* § 1798.120(a).
21. *Id.* § 1798.140(ah)(1). There are limited exceptions to the definition of "share." *Id.* § 1798.140(ah)(2).
22. *Id.* § 1798.125(a)(1). Examples of prohibited discrimination under the CCPA include denying goods or services, charging different prices or rates for goods or services, providing a different level or quality of goods or services, and suggesting that the consumer will receive a different price or level of quality for goods or services. *Id.* § 1798.125(a)(1)(A)–(D).
23. *Id.* § 1798.125(a)(1)(E).
24. *Id.* § 1798.140(ae).
25. *Id.*
26. *Id.* § 1798.100(a)(2).

Under the CPRA, consumers now have the right to restrict the use of sensitive personal information to only what is necessary to perform services or provide goods requested by the consumer.[27] A business that collects sensitive information must provide a link on its homepage restricting its use or disclosure.[28] For financial institutions, the Gramm-Leach-Bliley Act ("GLBA") and the Fair Credit Reporting Act may exempt much of this category of information.[29]

- **Amends the data breach private right of action**. The CPRA amends the personal information subject to the data breach private right of action to align with the definition of "personal information" under California's data breach law—i.e., including in the definition of personal information an e-mail address in combination with a password or security question and answer that would permit access to an account.[30] Consumers must provide a business thirty days' written notice of the alleged violation.[31] If within thirty days the business cures the issue and provides the consumer a written statement that it addressed the violations and such violations will not reoccur, no action may be initiated.[32]
- **Extends certain exemptions**. The CPRA extends the exemptions for business-to-business communications and personal information of a business' employees until January 1, 2023.[33] The CPRA also now exempts personal information collected under the federal Farm Credit Act.[34] Originally, only personal information gathered under the GLBA and the California Financial Information Privacy Act were exempt.[35]
- **Introduces prohibition of dark patterns**. The CPRA introduces the concept of "dark pattern," which it defines as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice."[36] The statute adds a definition of "consent" which provides that "use of dark patterns does not constitute consent."[37]

B. Virginia

The Virginia Consumer Data Protection Act ("VCDPA") was approved on March 2, 2021, and is effective on January 1, 2023, making Virginia the second

27. *Id.* § 1798.121(a).
28. *Id.* § 1798.135(a).
29. *Id.* § 1798.145(d) & (e).
30. *Id.* § 1798.150(a)(1) (referencing Cal. Civ. Code § 1798.81.5(d)(1)(A)).
31. *Id.* § 1798.150(b).
32. *Id.*
33. *Id.* § 1798.145(m)(1).
34. *Id.* § 1798.145(e).
35. *Id.*
36. *Id.* § 1798.140(*l*).
37. *Id.* § 1798.140(h).

jurisdiction in the United States to pass a comprehensive privacy law.[38] The VCDPA applies to a person that conducts business in Virginia or produces products or services targeted to its residents and (i) either controls or processes personal data of 100,000 consumers in a calendar year, or (ii) controls or processes personal data of at least 25,000 consumers and over 50 percent of its gross revenue comes from the sale of personal information.[39]

Certain organizations and data are exempt from the VCDPA. These include, among other things, Virginia government entities, financial institutions and data subjected to the GLBA, data regulated by the Fair Credit Reporting Act, and entities governed by privacy, security, and breach notification rules of the Health Insurance Portability and Accountability Act or the Health Information Technology for Economic and Clinical Health Act.[40]

The Virginia law provides consumers many of the same rights as its West Coast counterpart, the CPRA, such as the rights to know and access personal information, correct inaccurate personal information, delete personal data, transfer data to another controller, and opt out of the processing of data for targeted advertising or sale of personal data.[41] One deviation from the CPRA, however, is in the VCDPA's definition of "consumer," which expressly excludes a "natural person acting in a commercial or employment context."[42] In contrast, such persons are within the definition of "consumer" under the CPRA, which defines "consumer" simply as "a natural person who is a California resident," and the exemptions that may apply to such persons under the CCPA sunset on January 1, 2023.[43] In another departure from the CCPA and CPRA, the VCDPA does not have a private right of action for violations under the law.[44]

The VCDPA also implements data protection and processing requirements similar to those of the European Union's General Data Protection Regulation.[45] The VCDPA requires a data processing agreement between a controller and processor to govern the data processing procedures.[46] Data controllers also must conduct data protection assessments when processing sensitive data, processing personal data for targeted advertising or profiling, selling personal data, and processing activities involving personal data that presents a heightened risk

38. Va. Laws 1st Sp. Sess. ch. 35 (S.B. 1392) (to be codified at Va. Code §§ 59.1-575-585).

39. *Id.* (to be codified at Va. Code § 59.1-576(A)).

40. *Id.* (to be codified at Va. Code §§ 59.1-576(B), 576(C)(10)). Nonprofits and institutes of higher learning are also exempted. *Id.*

41. *Id.* (to be codified at Va. Code § 59.1-577(A)).

42. *Id.* (to be codified at Va. Code § 59.1-575).

43. Cal. Civ. Code §§ 1798.140(i), 1798.145(m)(4), (n)(3) (inoperative Jan. 1, 2023).

44. 2021 Va. Laws 1st Sp. Sess. ch. 35 (S.B. 1392) (to be codified at Va. Code § 59.1-584(E)).

45. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

46. 2021 Va. Laws 1st Sp. Sess. ch. 35 (S.B. 1392) (to be codified at Va. Code § 59.1-579(B)) (eff. Jan. 1, 2023).

of harm to consumers.[47] The law is silent, however, as to the frequency of the data processing assessments.

After the close of the survey year Colorado joined California and Virginia as the third jurisdiction to adopt a privacy law.[48]

III. CCPA Litigation and Enforcement

A. CCPA Litigation

The CCPA provides a limited private right of action to consumers who experience a data breach as a result of a business' failure "to implement and maintain reasonable security procedures and practices."[49] Moreover, the CCPA explicitly provides that the CCPA shall not "serve as the basis for a private right of action under any other law."[50] Notwithstanding, plaintiffs filed numerous CCPA cases in federal courts[51] testing the boundaries of the CCPA private right of action by diversifying their claims:

- **Scope of data breach CCPA claims**. Some plaintiffs have filed civil actions under Section 1798.150 because of unauthorized access and theft of personal information.[52] Defendants filed motions to dismiss in response to CCPA claims and were successful in some instances. For example, in *Rahman v. Marriott International, Inc.*[53] the court opined that plaintiffs did not sufficiently plead that "more sensitive data—such as credit card information, passports, or social security numbers—has fallen into the wrong hands."[54] Without a breach of this type of sensitive information, the court found plaintiffs did not suffer an injury to meet standing requirements, and granted defendant's motion to dismiss.[55]
- **CCPA violations did not give rise to a private right of action**. In at least one case, *McCoy v. Alphabet, Inc.*, the plaintiffs claimed CCPA violations for failure to disclose sharing of information and purpose of collection, but the court dismissed the CCPA claim because it found that there were no allegation of a security breach.[56]

47. *Id.* (to be codified at Va. Code § 59.1-580).
48. S.B. 21-190, Reg. Sess. (Colo. 2021) (eff. July 1, 2023).
49. Cal. Civ. Code § 1798.150(a)(1) (2021).
50. *Id.* § 1798.150(c).
51. *See, e.g.*, Class Action Complaint, McCoy v. Alphabet Inc., No. 5:20CV05427 (N.D. Cal. Aug. 5, 2020); Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898 (S.D. Cal. 2020); Consolidated Amended Class Action Complaint, *In re* Hanna Andersson & Salesforce.Com. Data Breach Litig., No. 3:20CV00812 (N.D. Cal. June 3, 2020).
52. *See, supra* note 51.
53. No. SA CV 20-00654-DOC-KES, 2021 WL 346421 (C.D. Cal. Jan. 12, 2021).
54. *Id.* at *2.
55. *Id.* at *3.
56. McCoy v. Alphabet, Inc., No. 20-cv-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021).

- **CCPA violation as a predicate for unfair competition law cause of action**. The California unfair competition law ("UCL") applies to activities that are "unlawful, unfair or fraudulent business act[s] or practice[s]" and "unfair, deceptive, untrue or misleading advertising" and provides consumers with a private right of action.[57] Plaintiffs have raised UCL claims by alleging that non-data breach violations of the CCPA are "unlawful, unfair, and/or fraudulent."[58] However, to date, there has not been a case where courts have been persuaded by this argument.[59]

B. Enforcement

CCPA enforcement began on July 1, 2020.[60] Businesses have a thirty-day right to cure the violation before the California attorney general may proceed with an enforcement action.[61] Since July 1, 2020, numerous notices of alleged noncompliance were issued across various industries, including online marketing and advertising services, social media networks, grocery retail, online dating, automotive, online gaming, and education technology.[62] Consumer complaints, social media, and business websites were elements the attorney general considered when evaluating businesses for CCPA non-compliance.[63]

While the central issues varied in scope, enforcement notices sent to businesses about privacy policies, opting out of the sale of personal information, and notice to consumers appeared the most frequent.[64] The attorney general paid particular attention to CCPA privacy policies and whether a business was in compliance with providing a consumer the means to opt out of the sale of personal information given the explicit inclusion of the opt-out provisions in the CCPA.[65] In particular, the attorney general examined non-compliant service provider contracts, untimely responses to requests, non-compliant privacy policies, lack of request methods, failing to provide a Do Not Sell link on the business webpage, and failing to provide notice of financial incentive to consumers in loyalty programs.[66]

The takeaway from the attorney general's curative efforts is that paying close attention to consumer-facing requirements may reduce a business' exposure to enforcement actions.

57. Cal. Bus. & Prof. Code §§ 17200-17210 (West, Westlaw through Ch. 145 of 2021 Reg. Sess.).

58. *See, e.g.*, Class Action Complaint at 34, Wesch v. Yodlee, Inc., No. 3:20-CV-05991 (N.D. Cal. Aug. 25, 2020).

59. *See, e.g.*, Wesch v. Yodlee, Inc., No. 20-cv-05991-SK, 2021 WL 1399291, at *6 (N.D. Cal. Feb. 16, 2021); *McCoy*, 2021 WL 405816, at *9.

60. Cal. Civ. Code § 1798.185(c) (2020).

61. *Id.* § 1798.155(b).

62. *CCPA Enforcement Case Examples*, Cal. Att'y Gen., https://oag.ca.gov/privacy/ccpa/enforcement (last visited Sept. 12, 2021) [hereinafter *CCPA Enforcement Case Examples*].

63. *CCPA Enforcement: Enter the AG*, IAPP Summit Sessions, https://www.youtube.com/watch?v=5uX1RkQpPUI (last visited Aug. 25, 2021) (including statements from California Supervising Deputy Attorney General Stacey Schesser).

64. *CCPA Enforcement Case Examples, supra* note 62.

65. Cal. Civ. Code §§ 1798.120, 1798.130(a)(5) (2020); Cal. Code Regs. tit. 11, §§ 999.306, 999.315 (2021).

66. *CCPA Enforcement Case Examples, supra* note 62.

The "New Abnormal"—The Emergence of Persistently Insecure Digital Systems

*By Roland L. Trope**

I. Introduction

Grid operators and owners have long recognized the need to secure digital communications and operations against "high-impact, low-frequency" ("HILF") event risks. As explained in a 2009 report prepared by the North American Electric Reliability Corporation ("NERC") and the U.S. Department of Energy, HILF event risks

> have the potential to cause catastrophic impacts on the electric power system, but either rarely occur, or, in some cases, have never occurred. Examples of HILF risks include *coordinated cyber . . . attacks*, . . . and major natural disasters like earthquakes, tsunamis, large hurricanes, *pandemics*, and geomagnetic disturbances caused by solar weather.[1]

Even so, critical infrastructure enterprises and their legal counsel may be challenged when a single HILF event occurs, especially if the infrequency and randomness of HILF event occurrence have lulled contingency planners into excluding HILF events from "worst-case" scenario planning.

Compared to customary "worst-case" scenarios, HILF events and their disruptive effects expand exponentially, often without awareness by enterprise officers, directors, and counsel until it's too late for them to make orderly adjustments in contingency plans and to keep the enterprise from succumbing.[2] HILF events may emerge with little or no warning (e.g., earthquakes, tsunamis), or with warning signs that go unnoticed or denied until it's too late to contain the exponential

* Roland Trope is a partner in the New York offices of Trope and Schramm LLP and an Adjunct Professor in the Department of Electrical Engineering and Computer Science at the U.S. Military Academy.

Disclaimer: The views expressed herein are solely Mr. Trope's, and should not be attributed to the U.S. Military Academy, Department of the Army, Department of Defense, or the U.S. Government. Mr. Trope can be contacted at: rltrope@tropelaw.com.

1. N. Am. Elec. Reliability Corp., High-Impact, Low-Frequency Event Risk to the North American Bulk Power System 8 (2010) (emphasis added), https://www.energy.gov/sites/default/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

2. *See id.* at 21 ("HILF events can occur very quickly and reach maximum impact with little warning or prior indication of an imminent risk. Effective response and restoration from HILF events require fast initiation and mobilization exercised through thorough prior planning.").

growth of the HILF event's disruptive effects. English mathematician Hannah Fry describes the belated detection and response challenges when the HILF event is a pandemic that spreads exponentially:

> "The thing you have to understand about exponential growth is that it feels like nothing is happening for ages and then it's like an unstoppable truck that's just slamming into a wall" . . . .
>
> Her favorite example is of an imaginary lily pad on a pond doubling its area every day. It starts growing in one minuscule corner and covers the whole surface of the pond after a month. By day 20, the lily pad is still almost invisible. By day 28, it covers a quarter of the pond, by day 29 it covers half, and by day 30 it covers it all.[3]

During the survey year, multiple overlapping HILF events revealed deficiencies in cybersecurity and contingency planning. The HILF events we experienced included:

- the global COVID-19 pandemic;
- a succession of ransomware attacks on critical infrastructure (e.g., Colonial Pipeline,[4] JBS USA Holdings, Inc.[5]); and,
- a massive series of state-sponsored advanced persistent threat ("APT") attacks on major tech companies (e.g., SolarWinds, Microsoft[6]).

Each APT was discovered months after initial intrusion, each with an indeterminate scope, and each requiring such extensive remediation that it may take years to rebuild the networks from scratch. Even then, we may discover the new components to be already compromised by malware. The net effect has been a *paradigm shift* from low- to high-impact disruptions. Low-impact disruptions (e.g., from thunderstorms or computer theft) tend to be relatively short (days, weeks). High-impact disruptions often persist for a long and uncertain period (many months or years). There has also been a *paradigm shift* from moderate to catastrophic disruptions with a demonstrable loss of enterprise resilience. Enterprises usually recover quickly and completely from low-impact disruptions. Enterprises often fail to fully recover from high-impact disruptions, and if they do, recovery tends to be slow and to require substantial reconstruction or replacement of equipment and systems. Many enterprises might find the recovery effort infeasible, or the disruptions so harmful they succumb to them.[7]

3. John Thornhill, *Mathematician Hannah Fry: "I'm Sure There's Lots of Tutting—But Not to My Face*," Fin. Times (July 30, 2021), https://www.ft.com/content/a5e33e5a-99b9-4bbc-948f-8a527c7675c3.

4. Allison Quinn, *Ransomware Attackers Stole Heaps of Data Before Gas Pipeline Shutdown*, Daily Beast (May 9, 2021), https://www.thedailybeast.com/ransomware-attackers-strike-the-jugular-of-us-gas-with-shut-down-of-colonial-pipeline?ref=topic.

5. Natalie Page, *The Second Wave of a Ransomware Pandemic*, Sec. Blvd. (July 19, 2021), https://securityboulevard.com/2021/07/the-second-wave-of-a-ransomware-pandemic/.

6. *See infra* Part II.

7. A Chatham House report uses the term "high-impact, law-probability events" instead of HILF and makes the following interesting observation about them:

The HILF events and the paradigm shifts they ushered in have rendered obsolete the concept of "new normal." The concept of a "new normal" after a disruptive incident reassuringly presumes there will be a complete post-event recovery, a prompt restoration of pre-event levels of services and operations, of the reliability, trustworthiness, and resilience of digital systems, and of the operations, augmented by artificial intelligence ("AI"), that rely upon such systems. That does not appear to be the prospect for enterprises in the wake of the 2020–21 HILF events and the shock waves of society-wide or jurisdiction-wide HILF event disruptions. The enterprises that survived did so by adapting, often by permitting or requiring personnel to work remotely. But whether caused by the pandemic, ransomware, or an APT attack, enterprises adapted by directing or authorizing personnel to work remotely and thus in locations not protected by the enterprise's security safeguards. Companies lost visibility over use of laptops by personnel. Personnel used work laptops increasingly for personal tasks and personal laptops for work tasks, all of which diminished security. As a result, "the perimeter has shifted from the network to the endpoint."[8] As explained in an HP-prepared report:

> Within a matter of weeks in early 2020, WfH [work from home] went from an occasional employee convenience to being the only way many organizations could continue to function. The scale of this change was extraordinary. A YouGov survey of global office workers commissioned for this report by HP . . . shows that 82% worked from home more since the start of the pandemic. . . . However, the danger is that organizations embrace WfH without assessing how this environment amplifies existing security threats. The volume of corporate data being accessed from home has risen substantially, . . . putting more information at risk. All the while, the number of endpoints—personal and employer provisioned—being used to access the corporate network from beyond the traditional network perimeter has exploded. . . . Often, endpoint devices such as laptops . . . and printers are left exposed, raising the chance that security incidents become invisible until damage is done.[9]

As the HP commissioned study demonstrates, most enterprises decided that in order to stabilize operations and survive they would leave their digital systems and networks unsecured and leave their sensitive data without many safeguards the enterprises had relied upon prior to the pandemic.

> The consequences of high-impact, low-probability events often spread rapidly and unevenly across sectors and borders. They pose particular threats to key industries—especially high-value manufacturing—and to the just-in-time business model. . . . In the face of persistent disruption, some businesses would start to impose big cuts in investment and jobs or to consider closing down.

BERNICE LEE & FELIX PRESTON, CHATHAM HOUSE, PREPARING FOR HIGH-IMPACT, LOW-PROBABILITY EVENTS: LESSONS FROM EYJAFJALLAJÖKULL 7, 11 (2012), https://www.chathamhouse.org/sites/default/files/public/Research/Energy,%20Environment%20and%20Development/r0112_highimpact.pdf.

8. HP WOLF SEC., BLURRED LINES AND BLINDSPOTS 4 (2021), https://threatresearch.ext.hp.com/wp-content/uploads/2021/05/BPS_Wolf-Security-Blurred-Lines-Report.pdf.

9. *Id.* at 1.

As enterprises adapted and re-adapted to HILF events, their cybersecurity environment increasingly turned into a "new *abnormal*." The cyber profile of many enterprises increasingly degraded into a condition of unreliable, insecure, and compromised cyber systems. Many enterprises going forward would be well-advised to presume that their cyber systems are *persistently* insecure and that their tech experts have not found all intruders or all malware the intruders may have secreted in digital systems. Henceforth, sensitive data may need to be kept off computer networks, servers, and digital storage media to prevent the APT attackers from subsequently accessing it to exfiltrate, destroy, or maliciously modify it. The possibility of that precarious *status quo*, and of the re-occurrence of HILF events prolonging or aggravating the "new abnormal" (including current APTs that may yet be detected), merits consideration. To facilitate that consideration, this essay will discuss:

- in Part II, the most significant known APTs during 2020–21;
- in Part III, an Indiana Supreme Court decision on whether payment of ransomware comes within insurance coverage for "use of any computer to fraudulently cause a transfer" of property or funds;[10]
- in Part IV, a U.S. Supreme Court decision on whether an individual who accesses a computer and certain directories and files—with authorization—and then misuses the accessed data in violation of a workplace rule or website term of use, thereby violates the Computer Fraud and Abuse Act ("CFAA"); and,
- in Part V, possible lessons for enterprises whose viability depends on cybersecurity and resiliency to HILF events.

II. SolarWinds Incident—Creation of Persistently Insecure, Digital-Based Systems

In mid-December 2020, software firm SolarWinds disclosed that its information technology platform, Orion, had been hacked an indefinite number of months earlier.[11] Malicious actors (reportedly of Russian intelligence service SVR[12]) had carried out a sophisticated, stealthy intrusion and remained undetected in targeted systems and networks for at least nine months. The intrusion included malware planted "in a routine software upgrade"[13] of SolarWinds' Orion program, which "keeps a watchful eye on all the various components in

10. G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 165 N.E.3d 82, 85 (Ind. 2021).

11. Jessica Shumaker, *Massive SolarWinds Breach Poses Risk to Law Firms, Courts as Well as Businesses*, LegalNews (Jan. 29, 2021), http://legalnews.com/detroit/1496019/.

12. Dina Temple-Raston, *A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

13. Sue Halpern, *After the SolarWinds Hack, We Have No Idea What Cyber Dangers We Face*, New Yorker (Jan. 25, 2021), https://www.newyorker.com/news/daily-comment/after-the-solarwinds-hack-we-have-no-idea-what-cyber-dangers-we-face.

a company's network,"[14] and affected customers located within SolarWinds' supply chain.

On December 13, 2020, the Department of Homeland Security Computer Readiness Team issued Emergency Directive 21-01 ("ED 21-01").[15] ED 21-01 appears to have been premised on several features of the incident: *first*, the unusual scope and severity of the attack ("over 17,000 organizations downloaded the infected back door"[16]); s*econd*, the lengthy period during which it continued without detection;[17] and *third,* a determination that the incident created "persistence in the [computer network] environment" with the result that it appears uncertain whether it will be possible to eradicate the malicious actors and the malware they secreted in targeted systems.[18] ED 21-01 cautioned: "SolarWinds Orion products . . . are *currently being exploited* by malicious actors. This tactic permits an attacker to gain access to network traffic management systems. *Disconnecting affected devices* . . . is the *only known mitigation measure* currently available."[19] Estimates (made in March 2021) predicted that agencies, attempting to rebuild their networks from scratch, may need "in the neighborhood of 12 to 18 months."[20]

Law firms whose clients included any of the affected enterprises might still be at risk through digital communications with such clients.[21] The electronic filing system that federal courts use was compromised.[22] In the immediate aftermath, some security experts viewed the attack as "an inflection point"[23] and believe it should be recognized as reflecting certain *paradigm shifts*, including:

- The attack methods show that the intruders understood in detail the step-by-step procedures that software companies use internally to initiate, build, test, and release updates; this fact will (or should) "change the way that large enterprises think about the software they install and think about how they handle updates."[24]

14. Temple-Raston, *supra* note 12. Orion enabled IT departments to "look on one screen and check their whole network . . . . [It] touches everything—which is why hacking it was genius." *Id.*

15. *Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise*, Dep't Homeland Sec. (Dec. 13, 2020), https://cyber.dhs.gov/ed/21-01/ [hereinafter ED 21-01].

16. Patrick Howell O'Neill, *Recovering from the SolarWinds Hack Could Take 18 Months*, MIT Tech. Rev. (Mar. 2, 2021), https://www.technologyreview.com/2021/03/02/1020166/solarwinds-brandon-wales-hack-recovery-18-months/.

17. Infiltration reportedly started in 2019, and detection did not occur until December 2020. *Id.*

18. ED 21-01, *supra* note 15.

19. *Id.* (emphasis added).

20. O'Neill, *supra* note 16.

21. Victoria Hudgins, *Spared Direct Hit, Law Firms Could Still Face SolarWinds Cyber Fallout*, Law.com (Jan. 21, 2021), https://www.law.com/legaltechnews/2021/01/21/spared-direct-hit-law-firms-could-still-face-solarwinds-cyber-fallout/?slreturn=20210025142438.

22. Dustin Volz & Robert McMillan, *Federal Judiciary's Systems Likely Breached in SolarWinds Hack*, Wall St. J. (Jan. 7, 2021), https://www.wsj.com/articles/federal-judiciarys-systems-likely-breached-in-solarwinds-hack-11610040175.

23. Temple-Raston, *supra* note 12.

24. Temple-Raston, *supra* note 12.

- And worse, enterprises now need to ask "What if the hackers planted the seeds of future attacks during that nine months they explored SolarWinds' customer networks—did they hide code for backdoors that will allow them to come and go as they please at a time of their choosing? . . . Will we find out later that the SolarWinds hack set the stage for something more sinister? . . . [N]ations are targeting [the] private sector . . . ."[25]

In early March 2021, Microsoft disclosed that certain users of its email and calendar program Exchange and the program's operational server had experienced a highly sophisticated cyberattack, reportedly executed by a malicious actor, known as Hafnium, that is located in the People's Republic of China, but that "conducts its operations primarily from leased virtual private servers (VPS) in the United States."[26] Microsoft explained that Hafnium has historically selected U.S. entities as its main targets, with the aim of exfiltrating data from enterprises in several industry sectors, including law firms.[27] The victims of the hack reportedly extended to upwards of 30,000 Microsoft customers, including federal agencies and private enterprises (particularly small and medium size businesses).[28]

The Hafnium attack started in January 2021, escalated in late February, and continued into March 2021.[29] In response, Microsoft released multiple security updates or "patches." When Microsoft observed that multiple bad actors continued to take advantage of unpatched systems "to attack organizations with on-premises Exchange Server," Microsoft endeavored to aid defenders in investigating the attacks by releasing a set of "observed indicators of compromise" in the form of "malware hashes and known malicious file paths"; a week later, Microsoft released a "new one-click mitigation tool . . . to help customers who do not have dedicated security or IT teams to apply security updates for Microsoft Exchange Server."[30]

However, due in part to limitations in technical expertise at many commercial victims, hundreds of servers remained vulnerable. In response, the Federal Bureau of Investigation ("FBI") sought and obtained judicial authorization to enter electronically many of the victims' computer networks, search for and locate the "web shells" lodged there by Hafnium, and execute code that would cause those shells to issue a command to the company's server that they be deleted.[31] As the FBI explained to the District Court:

25. *Id.*

26. Tom Burt, *New Nation-State Cyberattacks*, Microsoft (Mar. 2, 2021), https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

27. *Id.*

28. Kate Conger & Sheera Frenkel, *Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China*, N.Y. Times (Mar. 6, 2021), https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html.

29. *Id.*

30. *HAFNIUM Targeting Exchange Servers with 0-Day Exploits*, Microsoft (Mar. 2, 2021), https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

31. Mike Lennon, *FBI Agents Secretly Deleted Web Shells from Hacked Microsoft Exchange Servers*, SecurityWeek (Apr. 14, 2021), https://www.securityweek.com/fbi-agents-secretly-deleted-web-shells-hacked-microsoft-exchange-servers; Affidavit in Support of an Application Under Rule 41(b)(6)(B)

> most of these victims are unlikely to remove the remaining web shells because the web shells are difficult to find due to their unique file names and paths or *because these victims lack the technical ability to remove them on their own.*[32]

In short, without the knowledge of the affected enterprises, the FBI obtained a search warrant from a U.S. District Court "to seize and copy from Microsoft Exchange Servers located in the United States the web shells identified in [an attachment], and to delete the web shells from those servers."[33]

The FBI's novel and extraordinary action did not provide complete remediation for affected enterprises. Removal of the web shells did not identify or remove any other malware that Hafnium may have secreted in each targeted enterprise's servers and networks.[34] Moreover, whatever vulnerabilities Hafnium may have exploited, it's possible that the array of Microsoft's security patches (over twenty-five of which Microsoft released in March and early April 2021) might not have addressed all the Exchange Server zero-day vulnerabilities known to the Hafnium intruders. It's possible that the same or different intruders could "plant another web shell" and resume the intrusion, exfiltrate information, or modify key operational data to cause kinetic damage.[35]

III. G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.

When advising clients on responses to a ransomware attack, there are multiple uncertainties. They include:

- *Can we restore access to systems and data needed for resumption of at least degraded operations?* (Possibly, but the prolonged disruption of Colonial Pipeline[36] and other critical infrastructure targets of ransomware suggests many enterprises have not prepared sufficiently for that contingency.[37])
- *Can we negotiate a reduction in the demanded payment?* (Possibly. If the target is a hospital the attackers may be willing to consider reductions or even to "decrypt for free," as one ransomware group, DoppelPaymer,

for a Search Warrant at 4–6, *In re* Certain Microsoft Exchange Servers Infected with Web Shells, No. 4:21mj755 (Apr. 9, 2021), https://www.justice.gov/opa/press-release/file/1386631/download [hereinafter FBI Affidavit].

32. FBI Affidavit, *supra* note 31, at 6 (emphasis added).

33. *Id.* at 7.

34. Brian Barrett, *The FBI Takes a Drastic Step to Fight China's Hacking Spree*, WIRED (Apr. 14, 2021, 5:41 PM), https://www.wired.com/story/fbi-takes-drastic-step-to-fight-china-hacking-spree/.

35. *Id.*

36. *See* Scott Neuman, *What We Know About the Ransomware Attack on a Critical U.S. Pipeline*, NPR (May 10, 2021), https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline.

37. *See, e.g.*, Richard Tracy, *Turning Up the Heat: A Ransomware Attack on Critical Infrastructure Is a Nightmare Scenario*, Forbes (July 20, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/07/20/turning-up-the-heat-a-ransomware-attack-on-critical-infrastructure-is-a-nightmare-scenario/?sh=2dfb87d81da0.

says it will do,[38] but the FBI "advises victims to avoid negotiating with hackers, arguing that paying ransoms incentivizes criminal behavior."[39])

- *Can we lawfully pay the intruders?* (Possibly not, if there's reason to believe the payment, without a license from the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC") will violate any of the U.S. economic sanctions regulations.[40])
- *Can counsel's firm ethically pay or advise on making such payment to a criminal?* (Possibly, but it is peculiar that despite the multitude of ransomware attacks, no bar association in the United States has issued an ethics opinion that addresses that issue; apparently the sole ethics opinion to date comes from the Queensland Law Society, which addressed the issue of whether a law firm may ethically pay a ransom to recover access to client data in the *firm's computers*:

  > On balance, the clear obligation to protect client interests tends to outweigh the general public policy objection to paying criminals. Payment of the ransom is therefore an option available to the firm once all of the competing alternatives have been considered. . . . If lawful, we are entitled to make the decision based on what we think will lead to the best outcome for the client and our firm . . . .
  >
  > As an aside, if the attackers have had access to compromised systems there is a clear ethical duty to warn clients that this has occurred. So "pay up and keep quiet" is only possible where there is no way the intruders could have client data.[41]

- *If we pay, will the intruders release the encryption passwords or keys and restore our access to our data?* (Possibly, but they may demand additional amounts; and that risk raises an equally salient question: did intruders exploit their access to modify critical data randomly, rendering the data unreliable and potentially hazardous if utilized?)

For any enterprise considering making a payment to hackers, a key question may be whether the insurer will view the payment and the costs imposed by the

38. *Ransomware Groups Say They Won't Attack Hospitals*, VIRSEC, https://www.virsec.com/blog/maze-and-other-ransomware-groups-say-they-wont-attack-hospitals-during-covid19-outbreak-but-how-trustworthy-is-their-word (last visited Sept. 25, 2021).

39. Rachel Monroe, *How to Negotiate with Ransomware Hackers*, New Yorker (May 31, 2021), https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.

40. An OFAC advisory cautions companies to account for the risk "that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction," and thus expose the enterprise, its directors and officers and legal counsel to an OFAC enforcement action, as well as possible violations of "regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations." Dep't of Treasury, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments 1 (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

41. David Bowles, Is It Ethical (or Legal) for Law Firms to Pay Cyber-Ransom? 2 (Dec. 8, 2017), https://www.qls.com.au/getattachment/2ee73b54-fd00-4ad6-882a-54a5b2e88451/doc20171208_is_it_ethical_or_legal_for_law_firms_to_pay_cyber-ransom_final_djb.pdf.

disruption of operations as covered by the terms of the issued policy. The Supreme Court of Indiana, in a case of first impression, answered that question under Indiana law in *G&G Oil Co. of Indiana v. Continental Western Insurance Company*.[42]

In November 2017, hackers executed a ransomware attack on G&G Oil Co. of Indiana ("G&G").[43] Unable to access its servers and most workstations, G&G paid the demanded bitcoin ransom. But the hackers refused to restore G&G's control over its servers and demanded an additional payment.[44] G&G ultimately paid the additional ransom (for a total of $34,477.50) ("Ransom Payment"); the hackers sent passwords enabling G&G to decrypt and regain access to its servers.[45]

G&G submitted a claim to Continental Western Insurance Company, the issuer of its multi-peril commercial policy.[46] G&G relied on the policy's Computer Fraud clause ("Computer Fraud Clause"), which read:

> We will pay for *loss of or damages to "money" . . . and "other property"* resulting directly from the use of any computer to *fraudulently cause a transfer of that property* from inside the "premises" . . . .
>
> a. To a person . . . outside those "premises"; or
>
> b. To a place outside those "premises."[47]

Continental denied G&G's claim on two grounds. *First,* G&G had not purchased an optional Computer Virus and Hacking Coverage ("Hacking Coverage"). *Second*, Continental viewed the Ransom Payment as a loss that did not result directly from the "use of a computer to fraudulently cause a transfer of G&G's funds."[48]

G&G filed a complaint seeking a judgment to require Continental to indemnify G&G for the Ransom Payment loss.[49] The trial court granted Continental's cross-motion for summary judgment.[50] G&G appealed. The Court of Appeals of Indiana affirmed, adopting Continental's argument that the hacker did not commit an act that qualified as "fraud."[51] With no "fraud" committed, the Court of Appeals reasoned that the hacker's actions did not come within the Hacking Coverage for use of a computer to "fraudulently cause" a transfer of money, nor to "fraudulently cause" G&G to "purchase Bitcoin to pay as ransom."[52] The Court of Appeals seemingly viewed the hacker as an honest thief; although illegal, "there was no deception involved" in the hacker's ransom demand. No deception, no fraud,

42. 165 N.E.3d 82 (Ind. 2021).
43. G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 145 N.E.3d 842, 844 (Ind. Ct. App.), *rev'd & remanded*, 165 N.E.3d 82 (Ind. 2021).
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.* at 843–44 (emphasis added).
48. *Id.* at 844.
49. *Id.*
50. *Id.*
51. *Id.* at 847.
52. *Id.*

no coverage by the Computer Fraud Clause for loss caused by "use of any computer to fraudulently cause a transfer" of money.[53]

G&G appealed to the Supreme Court of Indiana, which reversed. The Supreme Court of Indiana found persuasive the Seventh Circuit's definition of "fraud" (albeit in the context of bankruptcy): "it includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated."[54] With that as a guide, the Supreme Court of Indiana construed the term "fraudulently cause a transfer" to mean "simply 'to obtain by trick.'"[55]

Applying that criterion, the court found neither party had demonstrated entitlement to summary judgment. G&G's evidence fell short, because not every ransomware attack is perforce fraudulent.[56] An enterprise's cybersecurity becomes a gauge of whether a hacker needed to resort to a "trick." As the court explained, "if no safeguards were put in place [by G&G], it is possible a hacker could enter a company's servers unhindered and hold them hostage. There would be no trick there."[57] Continental's evidence fell short for the same reason. The court found it unclear whether the hacker gained access to G&G's computer systems by "trick."[58]

The court then addressed whether the Ransom Payment loss was one "resulting directly from the use of a computer" as required by the Policy's Computer Fraud Clause.[59] Continental argued that G&G's "voluntary transfer of Bitcoin was an intervening cause that severed the causal chain of events" and thereby disconnected the Ransom Payment loss from a direct use of a computer.[60] The court disagreed, finding that G&G's Ransom Payment was only "voluntary" in the sense that G&G acted consciously. But the court sagaciously reasoned that "the payment more closely resembled one made under duress," and therefore it was "not so remote that it broke the causal chain" required for G&G's losses to have "resulted directly from the use of a computer."[61]

IV. *Van Buren v. United States*[62]

Georgia police sergeant Van Buren asked acquaintance Albo for a personal loan. Albo secretly recorded the request and shared it with a sheriff's office, alleging Van Buren tried to "shake him down" for cash.[63] The FBI received the recorded conversation and set up a "sting" operation: Albo would offer Van Buren about $5,000 to search the state law enforcement computer database for a license plate "purportedly belonging to a woman whom Albo had met at a local strip

53. *Id.* at 843.
54. G&G Oil Co. of Ind. v. Cont'l W. Ins. Co., 165 N.E.3d 82, 88 (Ind. 2021) (quoting McClellan v. Cantrell, 217 F.3d 890, 893 (7th Cir. 2000)).
55. *Id.* at 89.
56. *Id.*
57. *Id.*
58. *Id.*
59. *Id.* at 90.
60. *Id.*
61. *Id.* at 90–91.
62. 141 S. Ct. 1648, 1653 (2021).
63. *Id.* at 1653.

club."[64] Van Buren agreed. Operating his patrol-car computer, he used credentials that gave him authorized access to the law enforcement database of license plate data records.[65] Van Buren searched the database, found the requested license-plate entry (unaware the FBI had created it), and told Albo he could disclose it to him. Van Buren's use of the data violated his police department's prohibition on use of police computers for personal purposes.[66]

The federal government indicted Van Buren under the CFAA, alleging he accessed a computer while "exceed[ing] authorized access."[67] A jury convicted Van Buren and the Eleventh Circuit affirmed.[68] The U.S. Supreme Court granted certiorari to resolve the split among the circuit courts in interpreting the scope of liability under the CFAA's "exceeds authorized access" clause.[69]

Government and defendant agreed that defendant had authorization to access the subject computer when he "used his patrol-car computer and valid credentials to log into the law enforcement database."[70] They disputed whether defendant was "entitled *so* to obtain" the license-plate record—if not, defendant violated the CFAA.[71] Justice Barrett, writing the opinion of the Court (for a 6 to 3 majority), framed the issue as one of statutory construction: what did "so" mean in the context of that CFAA prohibition against exceeding "authorized access," which the CFAA defines as occurring when anyone accesses "a computer with authorization and . . . use[s] such access to obtain . . . information in the computer that the accesser is not entitled *so* to obtain."[72]

Defendant argued that the disputed phrase "is not entitled so to obtain" means that if a person is authorized to access information in a computer, there is no violation of the CFAA even if he accesses or uses that information for an unauthorized purpose. The government argued that the CFAA is violated if a person is authorized to access the information but does so for an unauthorized purpose.[73]

The Court agreed with the defendant. Explaining her conclusion, Justice Barrett offered a cogent spatial metaphor that referred to "access" and "authorization" as resembling a portcullis or gate "up-or-down." Justice Barrett reasoned that defendant's interpretation, unlike the government's, treated the "without authorization" and "exceeds authorized access" clauses consistently:

> Under Van Buren's reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system. And reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry.[74]

64. *Id.*
65. *Id.*
66. *Id.*
67. 18 U.S.C. § 1030(a)(2) (2018).
68. *Van Buren*, 141 S. Ct. at 1653–54.
69. *Id.* at 1654.
70. *Id.*
71. *Id.*
72. 18 U.S.C. § 1030(e)(6) (2018) (emphasis added).
73. *Van Buren*, 141 S. Ct. at 1654–55.
74. *Id.* at 1658–59.

By contrast, the government's reading would create an illimitable risk of criminalizing "every violation of a computer-use policy," turning "millions of otherwise law-abiding citizens" into criminals.[75]

The Court concluded that defendant "did not 'excee[d] authorized access' to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose."[76] The Court reversed the judgment of the Eleventh Circuit and remanded the case for further proceedings consistent with its opinion.

V. Conclusion—Pragmatic Lessons

When a HILF cyber event like SolarWinds occurs, the breached enterprises might never be able to determine with certitude whether the intruders have been expelled, their secreted malware contained, disabled, or eradicated, whether all adverse effects are over, or even whether the scope of the attack and damage have been ascertained. Henceforth, counsel and clients may need to assume the persistent presence of malware and even the continued presence of cyber actors in the enterprise until it can be verified reliably that intruders and malware have indeed been eradicated. But at this time, the possibility of verification that "all's clear" in a digital system remains uncertain.

In light of the emergence of HILF events, counsel might see if it can coax a client to "stress test" and reevaluate its cyber security safeguards. This may require reevaluation of steps the enterprise has taken that facilitate remote work during the pandemic, but that may have sacrificed data safeguards.

The *G&G Oil* decision suggests that an insured enterprise may be disqualified from recovering on a claim for losses resulting from a ransom payment or disruption of its operations if a court determines that the intruders gained access, not with a "trick," but through a security lapse or other security deficiency.

After *Van Buren*, enterprises can no longer rely on invoking the criminal prosecution under the CFAA to deter personnel from violating workplace policies on use of company data. If personnel have authority to access the computer, directory, and files containing the data, preventing insider threats and misuse of the data remains an enterprise responsibility.

Enterprise security is often designed to ask good people to do good things and relies on them to do it. Unfortunately, such security proves no match for when good people err, are tricked by a clever social engineering ploy, or when they sour and enlist their ingenuity to do bad things with sensitive data. We might do better to limit our trust to where the consequences of misplaced trust are trivial. But what are we do to about systems where misplaced trust would cause catastrophic disruptions and where experience of recent HILF events teaches us that such systems remain persistently insecure?

75. *Id.* at 1661.
76. *Id.* at 1662.

Developments in Digital "Wrap" Contracts

*By Nancy S. Kim**

I. Introduction

This essay covers cases involving digital wrap contracts,[1] which include browsewraps, clickwraps, sign-in wraps, and other variants. As was true last year, arbitration clauses involving gig economy companies dominate the cases this year and courts continue to provide greater guidance regarding how to apply the standard of "reasonable notice." The cases illustrate the careful attention of courts to context, including the nature of the interaction, user experience, and website design.

Part II focuses on the factors courts consider in applying the two-prong test of "reasonable notice" and "manifestation of assent." Part III focuses on specific terms in these contracts. One case finds that mandatory arbitration clauses are unenforceable against drivers engaged in food delivery services. Another sounds a cautionary note about the pitfalls of wrap contracts for the *drafter*. A third case involves terms in a privacy notice that are referenced in the company's Terms of Service to the company's chagrin. The survey ends, not with a case, but with a brief discussion of a wrap contract involving one of the world's biggest companies. It underscores that even though contract terms may be unilaterally drafted, they are mutually enforceable and can have unintended consequences.

II. The Totality of the Circumstances—Including the Nature of the Interaction —To Assess the Reasonableness of Notice

In *Kauders v. Uber Technologies, Inc.*, the Massachusetts Supreme Judicial Court for the first time considered what standard should be used to determine formation of online contracts.[2] Significantly, the court recognized that although the "fundamentals of online contract formation should not be different from ordinary contract formation," the experience of contracting online *is* different from

* Michael Paul Galvin Chair in Entrepreneurship and Applied Legal Technology, Chicago-Kent College of Law, Illinois Institute of Technology.

1. I am disinclined to use the term "electronic contracts" because that term also includes contracts that are electronically signed using software such as Docusign, which are not the subject of this essay.

2. 159 N.E.3d 1033, 1048 (Mass. 2021) ("We have not previously considered what standard a court should use when considering issues of contract formation for online contracts.").

paper transactions and reasonable Internet users may not realize that they are entering into a contractual relationship.[3]

Plaintiff Christopher Kauders sued Uber, alleging that several drivers refused to provide him with rides because he was blind and accompanied by a guide dog.[4] Uber moved to compel arbitration pursuant to the terms and conditions that it claimed applied to users such as the plaintiff.

The court considered Uber's registration process at length. During the process of registering to use the Uber app Kauders filled out information on several screens, with the final screen containing the words LINK PAYMENT. The user was required to enter credit card information on this page. The court explained:

> Under the box, white, boldface text stated "scan your card" and "enter promo code." In the middle of the screen, below the word "OR" in white text, there was a large, dark button labeled "PayPal" that provided another mechanism for entering payment information.
>
> At the bottom of the screen, there was white text that stated, "By creating an Uber account, you agree to the Terms & Conditions and Privacy Policy."[5]

The court observed that the terms were "extremely favorable" to Uber and touched on a "wide variety of topics." Furthermore, the terms stated that Uber could amend them at any time without notice.[6]

The court adopted the standard of "reasonable notice of the terms" and "reasonable manifestation of assent to those terms" to determine online contract formation.[7] It noted that "[s]etting out these general fundamental contract principles is not, however, the difficult part of analysis"; rather, the difficulty lay in how to *apply* the standard to a given situation. Actual notice would satisfy the first prong. In the absence of actual notice, however, "the totality of the circumstances must be evaluated" to determine whether the user received reasonable notice.[8]

According to the court, this "fact-intensive inquiry" required consideration of several factors, including the "form of the contract," meaning whether the presentation appears to be contractual, as well as "the nature, including the size, of the transaction, whether the notice conveys the full scope of the terms and conditions, and the interface by which the terms are being communicated."[9]

"For Internet transactions," the court continued, "the specifics and subtleties of the 'design and content of the relevant interface' are especially relevant in evaluating whether reasonable notice has been provided."[10] The examination of the

3. *Id.* at 1048–49.
4. *Id.* at 1039.
5. *Id.* at 1040.
6. *Id.* at 1041.
7. *Id.* at 1049.
8. *Id.*
9. *Id.* at 1049–50.
10. *Id.* at 1050 (quoting Meyer v. Uber Techs., Inc., 868 F.3d 66, 75 (2d Cir. 2017)).

interface should include evaluating the "clarity and simplicity of the communication of the terms" by considering such factors as:

> Does the interface require the user to open the terms or make them readily available? How many steps must be taken to access the terms and conditions, and how clear and extensive is the process to access the terms? Ultimately, the offeror must reasonably notify the user that there are terms to which the user will be bound and give the user the opportunity to review those terms.[11]

The second prong, reasonable manifestation of assent, required considering the "specific actions" necessary to manifest assent. For example, the interface could require a user to check a box to indicate agreement to terms and conditions. Actions the user takes in the context of clickwraps are the "clearest manifestations of assent."[12] The court explained the "several important purposes" of requiring an affirmative act of assent:

> It puts the user on notice that the user is entering into a contractual arrangement. This is particularly important regarding online services, where services may be provided without requiring compensation or contractual agreements, and the users may not be sophisticated commercial actors. Without an action comparable to the solemnity of physically signing a written contract . . . we are concerned that such users may not be aware of the implications of their actions where agreement to terms is not expressly required. . . . Requiring an expressly affirmative act, therefore, such as clicking a button that states "I Agree," can help alert users to the significance of their actions. Where they so act, they have reasonably manifested their assent.[13]

The task of determining assent is more difficult in the absence of any requirement that the user take an express action, such as clicking, and the court was disinclined to find assent through inference:

> Where the connection between the action taken and the terms is unclear, or where the action taken does not clearly signify assent, it will be difficult for the offeror to carry its burden to show that the user assented to the terms.[14]

The court examined Uber's interface at length. It noted many deficiencies, including that Uber did not require the user to scroll or select terms and did not require the user to click the link to the terms and conditions (even though the user did have to click the "Done" button), and that the connection between account creation and the terms was "oddly displayed" and not prominent enough.[15]

The court found that Uber's terms and conditions did not constitute a contract because the registration process did not provide users with "reasonable notice." It contrasted Uber's registration process for users with that for its drivers, which required that the driver click twice, once to indicate agreement, and again to

11. *Id.*
12. *Id.*
13. *Id.* at 1050–51.
14. *Id.* at 1051.
15. *Id.* at 1052.

indicate receipt and review of ALL THE DOCUMENTS and ALL THE NEW CONTRACTS.[16] It concluded that in the absence of reasonable notice, "a contract cannot have been formed here."[17]

In *Emmanuel v. Handy Technologies, Inc.*,[18] the plaintiff, Maisha Emmanuel, filed a class action lawsuit claiming that Handy, the operator of an online platform that connected individuals with house cleaners, had misclassified her and other class members as independent contractors rather than employees in violation of state and federal laws.[19] Handy filed a motion to compel arbitration claiming that Emmanuel was bound by its Independent Contractor Agreement.

Emmanuel had completed Handy's online application form and then checked a box next to the words "I agree to Handy's Terms of Use"[20] with the words "Terms of Use" displayed as a blue hyperlink.[21] If the link was clicked, the mandatory arbitration clause was visible only by scrolling on the screen.[22] When Emmanuel used an assigned personal identification number to access Handy's app, she saw a screen with bulleted statements indicating that she was an independent contractor, and not an employee.[23] She was required to click a blue button labeled Confirm below the bulleted statements or a button labeled "Click here to return to portal home and see the newest jobs," which would have refreshed the screen and returned her to the page with the bullet points.[24] Emmanuel selected Confirm, and a second screen appeared that required acceptance of an Independent Contractor Agreement.[25] Only a portion of that agreement was visible without scrolling.[26] A blue button labeled Accept at the bottom of the screen partially obscured the Agreement and was visible even without scrolling through the rest of the Agreement. The only other option was to click a gray button that was again labeled, "Click here to return to portal home and see the newest jobs," which resulted in the screen being refreshed.[27] Visible only by scrolling was the arbitration clause. Emmanuel testified that she did not scroll through the terms but clicked Accept.[28]

The district court held that under Massachusetts law, Emmanuel had entered into an arbitration agreement with Handy. The First Circuit agreed, stating that the precedent established in *Kauders v. Uber Technologies, Inc.* compelled it to do so.[29] According to the court, the "reasonable notice of the terms" and the "reasonable manifestation of assent to those terms" standard articulated in *Kauders*

16. *Id.* at 1055.
17. *Id.* at 1054.
18. 992 F.3d 1 (1st Cir. 2021).
19. *Id.* at 3.
20. *Id.*
21. *Id.* at 3.
22. *Id.*
23. *Id.* at 4.
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.* at 4–5.
28. *Id.* at 5.
29. *Id.* at 7.

was satisfied. Notably, the court chose to focus its analysis, not on whether the plaintiff clicked the box next to the link to the Terms of Use, but on her selection of the Accept button on the screen containing the initial sentences of the Agreement.[30] The court noted that although only part of the Agreement was visible without scrolling, the portion that was visible "made clear" that there was additional text.[31] Furthermore, the court stated that a website does not have to require a user to scroll through the entire Agreement for the manifestation of assent to be valid.[32] More significantly, the court distinguished the facts in *Kauders* by noting that Emmanuel did not "simply download the app and open it," but instead went through a multi-step screening process that included an online application, a telephone interview, a background check, and an in-person training session.[33]

Thus, based upon the "totality of the circumstances," the court found that a contract was formed. However, rather than focusing solely on a single moment of contract formation such as an isolated instance of clicking a button, it considered the multiple interactions Emmanuel had with Handy—which included, but were not limited to, the online contracting process. The case indicates that even if the precise moment of contract formation is unclear, a court may consider the "totality of the circumstances" to determine whether there was reasonable notice and manifestation of consent.

In *HomeAdvisor, Inc. v. Waddell*,[34] appellees sued HomeAdvisor under the Texas Deceptive Trade Practices Act when contractors they found through the website abandoned jobs before they were completed. HomeAdvisor filed a motion to compel arbitration which the trial court denied. HomeAdvisor appealed, arguing that there was a valid agreement to arbitrate between it and the appellees.[35]

The Court of Appeals agreed with HomeAdvisor and reversed the trial court's order, stating as the governing standard that "an agreement to arbitrate exists where notice of the arbitration provision was reasonably conspicuous and manifestation of assent is unambiguous."[36] It noted that HomeAdvisor had submitted the declaration of its vice president of software development which stated that each of the appellees had created an account with HomeAdvisor and had submitted service requests through its website. To complete their service requests, the declaration continued, appellees must have clicked an orange button immediately below which appeared an express statement that the use of HomeAdvisor's services was subject to its Terms & Conditions.[37] The court characterized this as a sign-in wrap.[38] The declaration included screenshots of each submittal page,

30. *Id.* at 15.
31. *Id.* at 9.
32. *Id.*
33. *Id.* at 10.
34. No. 05-19-00669-CV, 2020 WL 2988565 (Tex. App. June 4, 2020).
35. *Id.* at *1–3.
36. *Id.* at *4.
37. *Id.* at *2.
38. *Id.* at *4.

an image of which the court included in its opinion. The declaration also stated that there was a hyperlink to the Terms and Conditions on "nearly every webpage" of the website.[39]

The court applied the standard of a "reasonably prudent computer or smartphone user" to determine whether the terms were conspicuous, stating that to meet this standard it was not necessary for the terms themselves to appear on the page where the user indicates assent: "it is enough that the page contains a conspicuous hyperlink."[40] The court noted that the submittal page was "uncluttered" with only a "few spaces" to enter information and that the hyperlinked text was "dark against a bright white background, clearly legible, and the same size" as the other text on the screen. Furthermore, the "entire screen is visible at once with no scrolling necessary" and the user may click on the hyperlink and view the terms before submitting a request for service.[41]

The Terms and Conditions contained an arbitration provision, which the court reproduced in its opinion. The words **ARBITRATION AND GOVERNING LAW** and other important terms, such as **YOU GIVE UP YOUR RIGHT TO GO TO COURT**, were in bold and all-caps, which distinguished them from the surrounding text.[42] The court stated that the provision was "prominently noted with bolded and capitalized print" and that there was "nothing misleading or confusing" about the presentation of its user agreement.[43] Furthermore, the appellees' assent was "unambiguous" because they clicked the submit button which was "temporally coupled" with the receipt of the company's services and they were "clearly advised" that clicking the orange button indicates assent.[44] The court stated, "the reasonably prudent user would have understood that they could only receive HomeAdvisor's referral services by agreeing to the company's terms and conditions."[45]

Thus, the court considered the issue of reasonable notice and contract formation not by examining any single factor in isolation, but by considering the presentation of the terms and the entire contracting experience from the vantage point of the "reasonably prudent" user. Finally, the court held that the issue of unconscionability was delegated to the arbitrator pursuant to the arbitration agreement.[46]

The Texas court's approach regarding what constitutes reasonable notice contrasts with that adopted by a New Jersey court. In *C.D. v. Massage Envy Franchising, LLC*,[47] the plaintiff alleged that a massage therapist committed assault and battery during a massage, and in doing so breached the contract between the parties which prohibited such conduct. Massage Envy claimed that the plaintiff

39. *Id.* at *2.
40. *Id.* at *4.
41. *Id.*
42. *Id.* at *2.
43. *Id.* at *4.
44. *Id.* at *5.
45. *Id.*
46. *Id.*
47. No. ESX-L-3263-19, 2020 N.J. Super. Unpub. LEXIS 2382 (Dec. 3, 2020).

agreed to arbitration when she clicked "agree" on a check box at the bottom of an electronic consent form which Massage Envy presented to plaintiff on a tablet device when she arrived for the service.[48] The check box was at the end of a multi-page General Consent form and next to the words "I agree and assent to the *Terms of Use Agreement*," with the italicized words being a hyperlink.[49] Tapping on the hyperlink opened a new screen that presented a ten-page document titled Terms and Conditions. The Terms and Conditions contained a mandatory arbitration clause. Underneath the check box was a signature line where the plaintiff signed her name and then tapped a box that said CONTINUE.[50] Massage Envy argued that the claim should be submitted to arbitration. The court disagreed, finding that the General Consent form failed to clearly direct the plaintiff to the Terms and Conditions which was where the arbitration lurked.

The court framed the question as "whether or not the arbitration clause presented here was done so 'unfairly' or 'with a design to conceal or de-emphasize its provisions,'"[51] defining "design" in a footnote as "arrangement, or format, or layout" and not "intent, a plan, or a state of mind."[52] It found that the design was defective but clarified that it was not holding that clickwrap agreements as a form of contract were unenforceable; rather, it was that "this particular arbitration provision" was unenforceable

> because its placement, within a lengthy electronic document reached only by a hyperlink, which was accessible only adjacent to a signature line, which signature line followed a lengthy list of rules and disclaimers contained on an extended series of screens through which the user was required to scroll, was not under any fair analysis placed in such a way so as to give the plaintiff notice that there was more to consider in agreeing to the defendants' membership rules.[53]

The court's conclusion reflects how "notice" is affected by the design of the website which, in this case, negatively affected the plaintiff's inclination to read the terms:

> While it is undisputed that plaintiff did not read the electronic agreement reachable only by hyperlink, that is attributable, in this court's opinion, not to laziness, disinterest, or blithe indifference, but rather to an objectively confusing, nay misleading, design of the website. As a result, plaintiff's ignorance of the document's terms cannot fairly be ascribed to anything she did wrong.[54]

These cases indicate that a finding of notice and manifestation of consent for purposes of contract formation may, depending upon the context, require more than an overt act in connection with a statement that acknowledges that terms and conditions apply to the transaction. In other words, the standard of

48. *Id.* at *2–3.
49. *Id.* at *3.
50. *Id.* at *3–4.
51. *Id.* at *25.
52. *Id.* at *25 n.11.
53. *Id.* at *26–27.
54. *Id.* at *28.

reasonable notice should not be equated with a single presentation of a conspicuous notice; rather, courts will consider and evaluate the context of the transaction, the interaction of the user and the company, and the contracting process. Where a user is presented with notice of terms multiple times or on multiple occasions (for example, at account creation and then each time an order or request is made), a court is more likely to find reasonable notice and contract formation. By contrast, a single presentation of terms, even if prominent, will require evidence of deliberate or specific assent in order for a court to find contract formation.

III. Problems with the Substance of Terms

A. Class Action Waivers and Food Delivery Drivers

In *Archer v. GrubHub, Inc.*,[55] the plaintiffs were delivery drivers who sued Grubhub alleging that it unlawfully retained delivery charges and failed to reimburse them for travel expenses.[56] Each plaintiff electronically signed a statement acknowledging that she had "read, understand[s], and/or agree[s] to be bound by the terms" of the Arbitration Agreement.[57]

Grubhub moved to compel arbitration and the plaintiffs opposed, claiming that they did not agree to arbitration because the electronic pages did not "specifically reference" the arbitration agreement and did not "unambiguously reference" consent to arbitration.[58] The court disagreed with the plaintiffs, finding that each signature page was time- and date-stamped and explicitly referenced the Arbitration Agreement and informed the signor that the signor was agreeing to be bound by the "conspicuous terms" of the Arbitration Agreement.[59]

However, the court agreed with the plaintiff's second argument that the Arbitration Agreement was not enforceable under section 1 of the Federal Arbitration Act ("FAA") because the action relates to "contracts of employment of . . . workers engaged in . . . interstate commerce."[60] Furthermore, it concluded that because the FAA did not apply, the Massachusetts state policy against class action waivers was *not* preempted by federal law. Accordingly, the class action waiver provision in GrubHub's Arbitration Agreement was unenforceable because it was against public policy.[61]

B. Drafters Arguing Against Their Own Terms

In *Stover v. Experian Holdings, Inc.*,[62] Rachel Stover purchased Experian's credit score subscription and assented to its terms and conditions. The terms included

55. No. 1984-CV-03277, 2021 WL 832132 (Mass. Super. Ct. Jan. 13, 2021).
56. *Id.* at *1.
57. *Id.* at *2 (alterations by the court).
58. *Id.* at *5.
59. *Id.*
60. *Id.* at *7.
61. *Id.* at *9.
62. 978 F.3d 1082 (9th Cir. 2020).

an arbitration provision, a class action waiver, and a change-of-terms provision stating that each time she accessed the website she was manifesting assent to the "then current" terms.[63] Stover cancelled her subscription in 2014 and accessed it again only in 2018, at which time the arbitration provision had been changed to include a carve-out for disputes arising out of the Fair Credit Reporting Act ("FCRA").[64] Stover subsequently filed a class action complaint alleging violation of the FCRA and Experian moved to compel arbitration.[65] The district court granted Experian's motion, finding that the 2018 agreement applied but that Stover's claims were not within the FCRA carve-out. Stover appealed claiming that the agreement was unenforceable under California law. Experian, too, argued against the district court's order but on the grounds that "a mere website visit" was not enough to "activate" a change in terms.[66] In other words, Experian was in the interesting position of arguing that its unilaterally modified updated terms did not apply to Stover.

The Ninth Circuit agreed with Experian, noting that Stover assented "only once" to a single contract that Experian modified without notice, and that she had "no obligation to investigate" whether there were new terms if she was not provided with notice. "Indeed," continued the court,

> the opposite rule would lead to absurd results: contract drafters who included a change-of-terms provision would be permitted to bind individuals daily, or even hourly, to subsequent changes in the terms. The absence of limits on the frequency or substance of changes in terms subverts the basic rule of contract law that "[a] contract exists where the parties assent to the same thing in the same sense, so that their minds meet."[67]

The court held that "in order for changes in terms to be binding pursuant to a change-of-terms provision in the original contract, both parties to the contract—not just the drafting party—must have notice of the change in contract terms."[68]

This case reflects the limits of a company's ability to impose a unilateral modification clause, even in those jurisdictions that enforce them (and not all do). In order to bind a user, notice of upcoming changes should be presented to that user *each time* there is a change to the terms. As this case demonstrates, a unilateral modification clause is *not* notice of that change; rather, it is a notice that the company *may* change terms in the future. Accordingly, a company should not expect that a unilateral modification clause will bind existing users to subsequent changes unless there is specific advance notice of that subsequent change and a manifestation of the user's assent to the new terms.

In *Calhoun v. Google, LLC*,[69] the plaintiffs alleged that Google collected their personal data when they used the Chrome browser even when they chose not

63. *Id.* at 1084.
64. *Id.*
65. *Id.* at 1085.
66. *Id.*
67. *Id.* at 1086 (quoting 17A Am. Jur. 2d *Contracts* § 30 (Aug. 2020 update)).
68. *Id.*
69. No. 20-CV-05146-LHK, 2021 WL 1056532 (N.D. Cal. Mar. 17, 2021).

to use the "sync" feature, in violation of various state and federal laws.[70] They argued that Google expressly promises to Chrome users that their personal information will not be sent to Google unless the user chooses to store that data in the user's Google account by turning on sync.[71] Google argued that it explicitly disclosed the data collection in its Privacy Policy which was incorporated by reference into its Terms of Service, and that the plaintiffs consented to Google's data collection because they consented to the Terms of Service.[72]

The court, however, disagreed and found that the disclosure was insufficient.[73] It noted that there were four relevant documents: (1) Google's Terms of Service; (2) Google's Privacy Policy; (3) Chrome's Terms of Service; and (4) Chrome's Privacy Notice. As of March 31, 2020, the Terms of Service explicitly *excluded* the Privacy Policy by stating that "[a]lthough it's not part of these terms, we encourage you to read" the Privacy Policy.[74] According to the court, a "reasonable user consenting to Google's Terms of Service on or after March 31, 2020 might have concluded that she was not consenting to Google's Privacy Policy."[75]

Furthermore, the court stated that the Chrome Privacy Notice made "specific representations that could suggest to a reasonable user that Google would not engage in the alleged data collection," including "*You don't need to provide any personal information to use Chrome*," and "*The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google account by turning on sync*."[76] Thus, a "reasonable user could have concluded that if he or she used Chrome without sync, his or her personal information would not be sent to Google."[77] Accordingly, "Google cannot show that Plaintiffs expressly consented to Google's collection of data."[78]

In addition, the court denied Google's motion to dismiss plaintiffs' breach of contract claim. Google had claimed that the Chrome Privacy Notice was *not* contractual but merely "informational."[79] The court disagreed and found that the Terms of Service state that "by using our services, you're agreeing to these terms," and that the terms explicitly incorporated the Chrome Privacy Notice.[80] Consequently, the court found that "rather than being an informational resource, the Chrome Privacy Notice is part of the contract between Plaintiffs and Google."[81] Finally, it denied Google's motion to dismiss plaintiffs' claim for breach of the implied covenant of good faith and fair dealing because the allegations

70. *Id.* at *1–5.
71. *Id.* at *2.
72. *Id.* at *7–8.
73. *Id.* at *8.
74. *Id.* at *3.
75. *Id.* at *8.
76. *Id.*
77. *Id.* at *9.
78. *Id.* at *10.
79. *Id.* at *19.
80. *Id.*
81. *Id.*

went beyond the breach of contract claim and alleged that Google acted in bad faith by, for example, circumventing cookie blockers.[82]

C. Revisiting Arbitration Clauses

One of the most notable changes to digital wrap contracts took place outside of the courtroom. Amazon quietly dropped its mandatory individual arbitration clause from its Conditions of Use. While the May 2018 version of Amazon's Conditions of Use[83] contained multiple paragraphs providing that all disputes and claims are subject to binding individual arbitration, the current version eliminates those provisions and substitutes a clause stating that the state and federal courts in King County, Washington, are the exclusive forums for adjudication of disputes and that both parties waive their right to a jury trial. An article in the *Wall Street Journal* speculated that the change may have come about because the company received "more than 75,000" individual arbitration demands on behalf of Amazon Echo users who were suing over various privacy-related claims.[84] These hefty arbitration filing fees were discussed in last year's survey of digital contracts.[85]

IV. Conclusion

Courts continue to provide more clarity about what it means for notice to be "reasonable" for purposes of online contract formation. Although the font and presentation of the terms themselves are relevant, the courts focus more sharply on the nature of the transaction and the totality of the user's interaction with the company; they do not limit their attention to the moment when the terms are presented. Courts also take into account the nature of the relationship between the parties and the type of dispute. Thus, where a user is alleging assault and battery (as in *C.D. v. Massage Envy Franchising, LLC*) or discrimination (as in *Kauders v. Uber Technologies, Inc.*), courts may require specific notice and evidence of deliberate and intentional manifestations of consent.

In addition to the *form* of the terms, the *substance* was at issue in several notable cases. Terms may have unintended consequences for companies, even when unilaterally drafted. Companies should assess whether voluminous boilerplate terms actually serve their interests before imposing them upon website visitors as these terms can be used against them. If they have multiple documents containing digital adhesive terms, companies should consider how the terms interact with each other.

82. *Id.* at *19–20.

83. The version of the Conditions of Use that was in effect prior to May 21, 2018, is no longer available on Amazon's website but is accessible via the Internet Archive's Wayback Machine, at https://web.archive.org/web/20180503110140/https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=508088 (copy on file with author).

84. Sara Randazzo, *Amazon Allows Customers to Sue*, Wall St. J., June 2, 2021, at A1.

85. Nancy Kim, *New Developments in Digital and Wrap Contracts*, 76 Bus. Law. 349, 359–60 (2020).

Developments in the Laws Affecting Electronic Payments and Financial Services

By Stephen T. Middlebrook,[*] Sarah Jane Hughes,[**] Tom Kierner,[***] and Peter Maskow[****]

I. Introduction

The past year proved to be a busy period for the regulation of electronic payments and financial services. In this year's survey, we discuss rulemakings, enforcement actions, and other litigation that has significantly impacted the law governing payments and financial services. Part II addresses the ongoing fight between federal and state authorities over which should properly regulate FinTech entities and describes some new steps the Office of the Comptroller of the Currency ("OCC") has taken to assert its authority in this area. Part III details an enforcement action that California regulators took against a FinTech company they determined had misrepresented its relationship with its banking partner. Efforts by both federal and state regulators to assert their authority over virtual currency, including a relatively new form of virtual currency called a stablecoin, are discussed in Part IV. The decision of a federal judge upholding the application of the District of Columbia's money transmission statute to a virtual currency business is addressed in Part V. Part VI covers much-needed guidance from the Consumer Financial Protection Bureau regarding Earned Wage Access products while Part VII discusses the Bureau's loss of a court challenge to part of its regulations governing prepaid accounts. In Part VIII, we address a warning from the Federal Trade Commission ("FTC") to businesses employing artificial intelligence that the use of algorithms that discriminate based on race or other protected classes is a violation of federal law. Section IX provides our thoughts on what business lawyers may expect to see in the next year or two.

* Stephen T. Middlebrook is a principal at Middlebrook LLC. Previously, he was general counsel to two FinTech companies and senior counsel at the U.S. Department of the Treasury. Steve can be reached at Steve@Middlebrook-LLC.com.

** Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at Indiana University's Maurer School of Law. She can be reached at sjhughes@indiana.edu.

*** Tom Kierner is senior staff counsel at Fiserv and previously served as assistant general counsel at a payments company. He can be reached at Tom.kierner@fiserv.com.

**** Peter Maskow is Director, Consumer Litigation at Bluegreen Vacations in Boca Raton, Florida. Pete can be reached at peter.maskow@bluegreenvacations.com.

II. A Busy Year for the Regulators, FinTechs, Assignees of Loans, and Digital Assets Entities

In 2020 the OCC finalized two rules that deftly would have provided FinTechs with many benefits of Special Purpose National Bank Charters ("SPNBCs") without corresponding charter obligations. These rules were the Permissible Interest on Loans that Are Sold, Assigned, or Otherwise Transferred Rule[1] ("Valid-When-Made Rule") and an ill-fated National Banks and Federal Savings Associations as Lenders Rule[2] ("True Lender Rule"). The OCC also continued defending its SPNBC plans against the challenge brought by the New York State Department of Financial Services ("DFS").[3] This Part describes these developments and the FDIC's companion Valid-When-Made Rule.[4]

On July 31, 2018, the OCC announced its plans to take applications for SPNBCs from FinTechs.[5] DFS challenged the OCC's plans on September 14, 2018, arguing that the OCC lacked authority to charter entities that did not take deposits, absent express statutory authority to do so.[6] DFS prevailed in the trial court.[7] The OCC appealed and, as the survey year closed, the Second Circuit decided in favor of the OCC on standing and ripeness grounds and remanded the action to the district court.[8]

The Valid-When-Made Rule clarified that assignees of bank-originated obligations may charge interest "permissible before the transfer . . . after the transfer."[9] The OCC cited National Bank Act authority under 12 U.S.C. § 24 to make loans, enter into contracts, and sell loans made and to transfer obligations under contracts made.[10] The rights of assignees to enforce contract terms including interest rates was the issue in *Madden v. Midland Funding, LLC*,[11] in which the buyer of consumer credit-card obligations bought from a Delaware national bank sought to collect from a New York resident. The consumer argued that the purchaser

1. Office of the Comptroller of the Currency, Permissible Interest on Loans that Are Sold, Assigned, or Otherwise Transferred, 85 Fed. Reg. 33530 (June 2, 2020) (to be codified at 12 C.F.R. §§ 7.4001 & 160.110) [hereinafter Valid-When-Made Rulemaking].

2. Office of the Comptroller of the Currency, National Banks and Federal Savings Associations as Lenders, 85 Fed. Reg. 68742 (Oct. 30, 2020) (to be codified at 12 C.F.R. § 7.1031) [hereinafter True Lender Rulemaking].

3. Complaint for Declaratory and Injunctive Relief, Vullo v. Office of the Comptroller of the Currency, No. 18-cv-8377 (S.D.N.Y. Sept. 14, 2018).

4. Fed. Deposit Ins. Corp., Federal Interest Rate Authority, 85 Fed. Reg. 44146 (July 22, 2020) (to be codified at 12 C.F.R. § 331.1–4).

5. Press Release, Office of the Comptroller of the Currency, OCC Begins Accepting National Bank Charter Applications for FinTech Companies (July 31, 2018), https://www.occ.gov/news-releases/nr-occ-2018-74.

6. Complaint, *supra* note 3, at paras. 4, 5 & 7.

7. Vullo v. Office of the Comptroller of the Currency, 378 F. Supp. 3d 271 (S.D.N.Y. 2019).

8. Lacewell v. Office of the Comptroller of the Currency, 999 F.3d 130, 134 (2d Cir. 2021).

9. Valid-When-Made Rulemaking, *supra* note 1, at 33530. The rule itself states: "Interest on a loan that is permissible under 12 U.S.C. 85 shall not be affected by the sale, assignment, or other transfer of the loan." 12 C.F.R. § 7.4001(e) (2021). The companion rule for federal thrifts is at 12 C.F.R. § 160.110(d) (citing 12 U.S.C. § 1463(g)(1)).

10. Valid-When-Made Rulemaking, *supra* note 1, at 33531 (citing 12 U.S.C. § 24 (Seventh)).

11. 786 F.3d 246 (2d Cir. 2015) (vacating the holdings on preemption and denial of class certification, finding that the district court erroneously analyzed the preemption issue).

was entitled not to the interest rate allowed by the agreement but to a lower rate provided for under New York's usury law.[12] The Valid-When-Made Rule constituted a regulatory work-around—or rejection— of the Second Circuit's position that assignees were not covered by the preemption of state usury ceilings that national banks and federal thrifts that originated the loans enjoy under federal laws.[13]

The FDIC promulgated its own Valid-When-Made Rule on July 22, 2020.[14] The FDIC relied on section 27 of the FDI Act[15] to allow *state* banks (the OCC rule applies to *national* banks) to export interest at rates permissible in the state where the bank is located.[16] Seven states challenged the rule on August 20, 2020.[17] The action was pending as this survey year ended.

The OCC's later-repealed True Lender Rule could have resolved legal uncertainty about which entity—the chartered depository institution or its non-bank partners—originated loans and, consequently, whether federal or state interest-rate laws govern these loans.[18] The Rule provided that the lender is the bank that either (1) is named in the loan agreement as the lender or (2) funded the loan.[19] The Rule also provided that "[i]f, as of the date of origination, one bank is named as the lender in the loan agreement for a loan and another bank funds that loan, the bank that is named as the lender in the loan agreement makes the loan."[20] The party that is the lender on this basis is responsible for compliance with federal laws for the loans.[21]

On May 11, 2021, the Senate passed a resolution[22] to repeal the True Lender Rule under the Congressional Review Act,[23] which also enjoins subsequent promulgation of the same or a similar rule unless specifically authorized by a law enacted after the disapproval.[24] After this survey year closed, the House passed the resolution and the President signed it.[25] Thus, the opportunity that the Rule would have provided to FinTechs is dead.

12. *Id.* at 248.
13. *Id.* at 249.
14. Fed. Deposit Ins. Corp., Federal Interest Rate Authority, 85 Fed. Reg. 44146 (July 22, 2020) (to be codified at 12 C.F.R. § 331.1–4).
15. 12 U.S.C. § 1831(d) (2018).
16. 12 C.F.R. § 331.4(a) (2021).
17. Complaint for Declaratory and Injunctive Relief, California v. FDIC, No. 20-CV-5860 (Aug. 20, 2020).
18. True Lender Rulemaking, *supra* note 2, at 33530.
19. 12 C.F.R. § 7.1031(b) (2021).
20. *Id.* § 7.1031(c).
21. *Id.*
22. S.J. Res. 15, 117th Cong. (2021), https://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=117&session=1&vote=00183 (Roll Call; Vote Summary).
23. 5 U.S.C. §§ 801–808 (2018).
24. *Id.* § 801(b)(2).
25. *Remarks by President Biden Signing Three Congressional Review Act Bills into Law*, WHITE HOUSE (June 30, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/30/remarks-by-president-biden-signing-three-congressional-review-act-bills-into-law-s-j-res-13-s-j-res-14-and-s-j-res-15/ (referring to the Rule's allowance of "rent-a-bank schemes").

This survey year also produced the first sanctions imposed by the Treasury Department's Office of Foreign Assets Control ("OFAC") against digital asset firms. The first of these actions involved BitGo, a provider of technology that enables digital currency transactions.[26] The 183 "apparent violations"—all between March 10, 2015, and December 11, 2019—involved digital currency transactions by persons in Crimea, Cuba, Iran, Sudan, and Syria for which BitGo allegedly had "reason to know" of the users' locations. BitGo settled the claims for $98,830.[27] On February 8, 2021, OFAC announced that a second similar action, against BitPay, Inc., was settled for $507,375.[28]

In a February 2021 regulatory filing with the Securities and Exchange Commission, Coinbase disclosed that certain of its transactions were "under review" by OFAC.[29] The two settlements and the regulatory filing make clear that sanctions compliance for digital assets entities is a growing part of OFAC's work.

III. California Settles Claims Against FinTech Company for Misrepresenting Banking Services

FinTech providers were also under scrutiny at the state level. In March 2021, the California Department of Financial Protection and Innovation ("DFPI") entered into a settlement agreement with Chime regarding Chime's use of the words "bank" and "banking" in marketing the company's products.[30] Chime is a FinTech that works with bank partners to offer consumer bank accounts online. It manages the programs on behalf, and with the oversight, of the bank partners. But Chime is not a bank, and according to the DFPI Chime was not clear enough about this fact. Its principal website domain was chimebank.com, and its marketing efforts contained language that, according to the DFPI, could lead consumers to think they were banking with Chime.[31]

Chime escaped without financial penalty, but was required to make significant changes to its marketing efforts. Chime agreed to cease using its domain "chimebank.com," beef up its internal marketing compliance program, and clearly disclose that it is not a bank and that banking services are being provided by Chime's bank partners.[32] Much has been written over the last few years about

26. Enforcement Release, U.S. Dep't of the Treasury, OFAC Enters into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions (Dec. 30, 2020), https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.

27. *Id.*

28. Enforcement Release, U.S. Dep't of the Treasury, OFAC Enters into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions (Feb. 18, 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf.

29. Kyle Brasseuer, *OFAC Crypto Crackdown: Coinbase Disclosures Under Review*, Compliance Week (Mar. 5, 2021, 9:38 AM), https://www.complianceweek.com/sanctions/ofac-crypto-crackdown-coinbase-disclosures-under-review/30115.article.

30. Settlement Agreement, *In re* Comm'r of Fin. Prot. & Innovation v. Chime Fin., Inc. (Cal. Dep't of Fin. Prot. & Innovation Mar. 29, 2021), https://dfpi.ca.gov/wp-content/uploads/sites/337/2021/04/Admin.-Action-Chime-Financial-Inc.-Settlement-Agreement.pdf.

31. *Id.* at 2.

32. *Id.* at 3–4.

the rise of so-called "neobanks" and their disruption of the traditional consumer financial services market. However, these companies, like Chime, are often not banks at all. The Chime settlement agreement with DFPI is a good reminder that FinTech companies, in their quest to create a cohesive brand strategy, should be careful not to misrepresent their role.

IV. Regulatory Guidance and Challenges Related to Virtual Currency and the Adoption of Stablecoins for Payment Activity

A. OCC Issues Interpretive Letter Permitting the Use and Creation of Stablecoins by Banks, But for How Long?

In January 2021, the OCC issued an interpretive letter allowing banks to use Independent Node Verification Networks ("INVNs") and stablecoins for payment activities.[33] An INVN is "a shared electronic database where copies of the same information are stored on multiple computers."[34] Stablecoins are assets "designed to maintain a stable value relative to an identified fiat currency."[35] The letter expanded upon prior statements permitting banks to facilitate cryptocurrency and fiat currency exchange transactions,[36] and encouraging them to hold "reserves" for stablecoins on at least a one-to-one basis.[37]

The OCC drew on precedent authorizing a national bank to offer an electronically stored value ("ESV") system, characterizing ESV as the electronic equivalent of paper payment systems and likening ESV's functionality to services already provided by banks.[38] The OCC observed that the distinction between stablecoins and cards with ESV used to facilitate cashless payments is merely "technological in nature."[39] The letter also noted stablecoins' efficiency in the retention, transfer, transmission, and exchange of fiat currency value and their particular usefulness in cross-border transfers.[40]

The OCC found that banks possess the requisite expertise to facilitate exchange, settle transactions, and manage their position as a financial intermediary.[41] These factors, coupled with the demand for banks to use INVNs and stablecoins, led the OCC to conclude that banks may "validate, store, and record

33. *See* Office of the Comptroller of the Currency, Interpretive Letter No. 1174 (Jan. 4, 2021), https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf [hereinafter OCC IL 1174].

34. *Id.* at 1.

35. President's Working Grp. on Fin. Mkts., Statement on Key Regulatory and Supervisory Issues Relevant to Certain Stablecoins, Treas. SM-1223 (Dec. 23, 2020), https://home.treasury.gov/system/files/136/PWG-Stablecoin-Statement-12-23-2020-CLEAN.pdf.

36. *See* Office of the Comptroller of the Currency, Interpretive Letter No. 1170, at 8 n.39 (July 22, 2020), https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf.

37. *See* Office of the Comptroller of the Currency, Interpretive Letter No. 1172 (Sept. 21, 2020), https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf.

38. OCC IL 1174, *supra* note 33, at 6–7.

39. *Id.* at 7.

40. *Id.* at 3–4, 7–8.

41. *Id.* at 2–3.

payments transactions by serving as a node on an INVN,"[42] and to approve the use of INVNs and stablecoins for permissible payment activities.[43] Finally, the letter permits banks to "buy, sell, and issue stablecoin to facilitate payments."[44]

The OCC acknowledged risks concomitant with stablecoins, including difficulty in verifying parties to a transaction and the need to safeguard reserve assets, maintained on a one-to-one ratio, to ensure satisfaction of liquidity needs and to cover potential losses. Moreover, it cautioned that cryptocurrency payment activities increase risks associated with Bank Secrecy Act and anti-money laundering compliance,[45] and that stablecoin issuance requires conformity with applicable securities regulations.[46]

Acting Comptroller Michael Hsu has asked OCC staff to review the agency's cryptocurrency actions.[47] Hsu expressed concern that the OCC's cryptocurrency positions lacked "full coordination with all stakeholders" and were not part of a broader regulatory strategy.[48]

B. New York Resolves Regulatory Action Against Stablecoin Issuer and Cryptocurrency Exchange

Demonstrating that concerns about stablecoin reserves are well-founded, the New York Attorney General ("NYAG") investigated a cryptocurrency exchange platform, Bitfinex, and the issuer of the stablecoin Tether.[49] The NYAG found that Tether's disclosures about the reserves claimed to back the stablecoin were misleading.[50] Specifically, the NYAG found that Tether included in its "reserves" money lent to Bitfinex, failed to announce changes made to its reserve disclosures (despite the disclosures' referencing "other assets and receivables from loans" as a component of reserves), and failed to disclose Bitfinex's capital liquidity issues resulting from its loss of control of approximately $850 million.[51] While neither Bitfinex nor Tether admitted the findings, they agreed to pay the State of New York a penalty of $18.5 million, to publish the categories of assets backing its reserves for two years, and to discontinue future activities with New York residents and businesses.[52]

42. *Id.* at 4.
43. *Id.* at 9.
44. *Id.* at 7.
45. *Id.* at 9.
46. *Id.* at 6 n.27.
47. *See* Michael J. Hsu, Acting Comptroller of the Currency, Statement Before the Committee on Financial Services, U.S. House of Representatives 13 (May 19, 2021), https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-wstate-hsum-20210519.pdf.
48. *Id.* at 11.
49. Settlement Agreement, *In re* iFinex Inc. (Feb. 18, 2021), https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf.
50. *Id.* at 2–9.
51. *Id.* at 5–6, 9.
52. *Id.* at 2, 9–12.

C. FinCEN Issues Notice of Proposed Rulemaking to Track Cryptocurrency Transactions

To enhance the ability of law enforcement agencies to track the flow of money in convertible virtual currency ("CVC") or digital assets with legal tender status ("LTDA"), the Financial Crimes Enforcement Network ("FinCEN") issued a proposed rulemaking pursuant to the Bank Secrecy Act.[53] Specifically, the proposed rule would require reporting, record keeping, and verification in connection with transactions greater than $3,000 involving either un-hosted wallets or wallets that are "otherwise covered."[54] The proposed rule would require banks and money services businesses to report transactions to FinCEN within fifteen days of their occurrence, and to keep records related to their customer, their customer's CVC or LTDA transactions, and the counterparties to such transactions.[55] FinCEN's second notice of the proposed rulemaking identified additional authority under the Anti-Money Laundering Act and supplemented information on the reporting.[56]

V. Bitcoin Is "Money" for Purposes of Money Transmission Laws in the District of Columbia

In 2019, Larry Dean Harmon was charged in federal court in the District of Columbia with engaging in money transmission without a license in violation of the D.C. Money Transmitters Act ("MTA") and with money laundering and operating an unlicensed money transmitting business in violation of 18 U.S.C. §§ 1956 and 1960.[57] The allegations against Harmon related to the operation of a Bitcoin "tumbler"—a service that for a fee would transmit Bitcoin through a series of transactions in an effort to mask the (illegal) origins of the virtual currency.[58] Harmon moved to dismiss the two counts related to money transmission on the grounds that Bitcoin is not money for purposes of the MTA and, thus, his tumbler service was not engaged in money transmission.[59] Although the MTA does not define the term "money," the court held that the word is commonly understood to mean "a medium of exchange, method of payment, or store of value" and that Bitcoin fell within that definition.[60] Defendant noted that the D.C. Department of Insurance, Securities and Banking ("DISB"), which has authority to enforce the MTA, had indicated on its webpage that virtual currencies were unregulated and consumers should be aware of the increased risks they

53. FinCEN, Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83840, 83840–41 (Dec. 23, 2020).

54. *Id.* at 83842–43 ("Otherwise covered wallets" are those "hosted by a foreign financial institution not subject to effective anti-money laundering regulation.").

55. *Id.* at 83843.

56. FinCEN, Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 3897, 3897 (Jan. 15, 2021).

57. United States v. Harmon, 474 F. Supp. 3d 76, 80 (D.D.C. 2020).

58. *Id.* at 82–83.

59. *Id.* at 87.

60. *Id.*

pose.[61] The court was not persuaded by the DISB webpage, which it viewed as a consumer alert and not an official interpretation of the law,[62] and denied the motion to dismiss.

Subsequently, prosecutors made the court aware of a nonpublic letter DISB had sent to a company that had inquired about the need to obtain a money transmitter license for a virtual currency project.[63] DISB informed the company that it would not need a money transmitter license because virtual currency services do not involve the transmission of money.[64] Based on this new information, the defendant moved for reconsideration.[65] The court denied the motion, holding that the DISB letter was legally not entitled to deference and, even if it was, the reasoning set forth in the letter was entirely unpersuasive.[66] In particular, the court opined that the DISB letter misinterpreted and misapplied guidance on virtual currencies issued by FinCEN.[67] The *Harmon* decision signals that courts are increasingly capable of sophisticated analysis of virtual currency issues and will not always defer to litigants or administrative agencies when applying the law to virtual currency businesses.

VI. CFPB Issues Advisory Opinion and Guidance on Earned Wage Access Products

On December 10, 2020, the Consumer Financial Protection Bureau ("CFPB") issued an advisory opinion[68] regarding Earned Wage Access ("EWA") products. The advisory opinion primarily addresses the question of if and when an EWA program is covered by the Truth in Lending Act ("TILA") and Regulation Z. EWA products provide workers with access to funds that they have earned but that have not yet been paid to them.[69] The advisory opinion concludes that EWA programs that meet certain requirements are not an "extension of credit" and not subject to TILA or Regulation Z.[70]

The advisory opinion builds upon commentary included in regulations regarding payday lending[71] issued in 2017. Those regulations suggested that an

61. *Id.* at 95.
62. *Id.*
63. United States v. Harmon, No. 19-CR-395 (BAH), 2020 WL 7668903, at *2 (D.D.C. Dec. 24, 2020).
64. *Id.* at *2–3.
65. *Id.* at *3.
66. *Id.* at *8–10.
67. *Id.* at *10–12.
68. Truth in Lending (Regulation Z); Earned Wage Access Programs, 85 Fed. Reg. 79404 (Dec. 10, 2020) [hereinafter EWA Advisory Opinion].
69. Telis Demos, *The Wait for Payday Doesn't Have to Be So Long*, Wall St. J. (Aug. 10, 2019), https://www.wsj.com/articles/the-wait-for-payday-doesnt-have-to-be-so-long-11565429401; Stephen T. Middlebrook, *What Business Lawyers Need to Know About Wage Advance Products*, Bus. L. Today (Sept. 5, 2019), https://businesslawtoday.org/2019/09/business-lawyers-need-know-wage-advance-products.
70. EWA Advisory Opinion, *supra* note 68, at 79406–08.
71. Payday, Vehicle Title, and Certain High-Cost Installment Loans, 82 Fed. Reg. 54472 (Nov. 17, 2017) [hereinafter Payday Rulemaking].

EWA product that allows an employee to draw accrued wages ahead of a scheduled payday recoups the advance through payroll deduction, and does not provide recourse against the employee might not be a form of lending.[72] Relying on the 2017 regulations, the CFPB concluded that EWA programs that "provide access to the consumer's own funds" through transactions that are "limited to the accrued cash value of employee wages" are not an extension of credit for purposes of Regulation Z.[73]

Under CFPB's advisory opinion, an EWA product qualifies as a Covered EWA Program which is not an extension of credit and not subject to Regulation Z if it meets all of the following criteria:

1. The provider contracts with the employer.
2. The advance does not exceed the amount of earned wages verified by the employer.
3. The employee pays no fee, voluntary or otherwise, for the service. The advance must be sent to an account of the employee's choice. If the account receiving the advance is a prepaid account offered by the provider, then certain additional fee restrictions apply to the prepaid account.
4. The provider recovers the advance only through payroll deduction from the next paycheck. One additional deduction may be attempted if the first deduction fails for technical reasons.
5. If the advance can't be collected through the payroll deduction, the provider can't otherwise collect from the employee.
6. The provider must make certain warranties to employee, including that there will be no fees, no recourse against the employee, and no debt collection activities.
7. The provider may not conduct a credit assessment or credit reporting.[74]

EWA products that do not verify an employee's earned wages with the employer, do not recoup the funds through payroll deduction, or that otherwise do not meet these criteria would still potentially be subject to Regulation Z.

CFPB also issued an approval order for an EWA program.[75] Through this type of order, CFPB grants an entity a safe harbor from legal liability regarding a certain product or practice if it follows certain conditions prescribed in the order. The approval order describes one of the entity's EWA programs and

72. EWA Advisory Opinion, *supra* note 68, at 79407 n.33 (citing Payday Rulemaking, *supra* note 71, at 54547).

73. *Id.* at 79407.

74. *Id.* at 79405–06.

75. Press Release, Consumer Fin. Prot. Bureau, Consumer Financial Protection Bureau Issues an Approval Order to Facilitate Employee Access to Earned but Unpaid Wages (Dec. 30, 2020), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-issues-an-approval-order-to-facilitate-employee-access-to-earned-but-unpaid-wages/.

concludes that the EWA product at issue is not an extension of credit.[76] The approved EWA program differs from criteria for a Covered EWA Program in some respects. The EWA program does provide a method to access the EWA payment without a fee, but it also offers other methods of accessing EWA funds that do involve a fee.[77] In addition, while the advisory opinion allows an EWA provider to make a single additional attempt at recoupment if the first attempt fails for technical reasons, the approval order permits the provider to re-present the deduction in the two subsequent paychecks if the initial recoupment fails.[78] CFPB does not explain why the approval order varies from the criteria set forth in the advisory opinion. We expect CFPB will issue additional approval orders or other forms of guidance regarding EWA products in the future.

VII. PayPal Succeeds in Invalidating Parts of the CFPB's Prepaid Account Rule

The D.C. District Court sided with PayPal in its challenge to two provisions of the CFPB's Prepaid Account Rule ("Rule").[79] The provisions, effective on April 1, 2019, were: (i) the highly prescriptive short-form disclosure requirement and (ii) the prohibition on linking credit features to an account for thirty days.

Under the Rule, financial institutions that offer prepaid accounts must generally provide certain pre-acquisition disclosures to consumers.[80] One such disclosure is a tabular short form disclosure that lists the most common fees assessed in connection with the account being issued.[81] The Rule prescribes use and location of disclaimers, pixel and font size, color, and content, among other things.[82] According to PayPal, following the prescriptive tabular format caused confusion and led many customers to believe that PayPal had begun to assess fees for services that were performed for free.[83]

The Rule also requires card issuers to wait thirty days after a consumer registers a prepaid account before linking certain credit features to that account.[84] As applied to PayPal, this prohibited PayPal from allowing consumers to attach their own separate credit products that they've had for years to PayPal's digital wallets for the first thirty days after they have acquired the digital wallet product. The court concluded the CFPB had exceeded its statutory authority with regard to both challenged provisions, granted PayPal's motion for summary judgment,

76. Consumer Fin. Prot. Bureau, Approval Order (Dec. 30, 2020), https://files.consumerfinance.gov/f/documents/cfpb_payactiv_approval-order_2020-12.pdf.
77. *Id.* at 3.
78. *Id.*
79. PayPal, Inc. v. CFPB, 512 F. Supp. 3d 1 (D.D.C. 2020), *appeal docketed*, No. 21-5057 (D.C. Cir. Mar. 10, 2021).
80. 12 C.F.R. § 1005.18(b) (2021).
81. *Id.* § 1005.18(b)(2).
82. *Id.* § 1005.18(b).
83. Complaint at 2–7, PayPal v. CFPB, No. 19-cv-3700 (D.D.C Dec. 11, 2019).
84. 12 C.F.R. § 1026.61(c)(1)(iii) (2021).

and vacated both provisions.[85] The CFPB has filed an appeal,[86] so the longer-term status of the Rule is unknown.

The court, however, did not consider PayPal's argument that the Rule violated PayPal's First Amendment rights, which is unfortunate. There is growing interest in the intersection of financial disclosure regulations and freedom of speech, and we have previously covered how courts apply First Amendment principles to the "the pervasive and extremely detailed disclosure requirements that regulators frequently impose on electronic financial products and services."[87]

VIII. FTC Issues Warning Related to the Sale and Use of Artificial Intelligence

The FTC staff announced through an April 2021 blog post that selling or using algorithms that are biased on the basis of race or other protected classes violates federal law.[88] Citing the agency's experience in enforcing the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act against developers and users of artificial intelligence ("AI"), the FTC offered guidance on how to use AI in a compliant way. When developing algorithms, businesses should ensure that data that the algorithm is built on does not exclude information from particular populations. Once the algorithm is developed, it should be tested, both before initial use and periodically thereafter, to identify and avoid discriminatory outcomes. The blog post also advised businesses to consider using transparency frameworks and independent standards so biases may come to light, and cautioned against making untruthful statements about what the algorithm can do and how the data is used. New technology is never perfect, but the FTC reminds businesses that a practice is unfair if it causes more harm than good.

Financial institutions and FinTechs heavily rely on AI, such as to authenticate customer identity, detect suspicious transactions, prevent fraud, enable better and more efficient customer service, and for many other purposes. This FTC blog post is a good reminder for electronic payment companies to examine existing AI systems to evaluate their risk of noncompliance. After all, as the FTC warned, companies need to hold themselves accountable "or be ready for the FTC to do it for you."[89]

85. *PayPal*, 512 F. Supp. 3d at 12.

86. Notice of Appeal, PayPal, Inc. v. CFPB, No. 19-cv-3700 (D.D.C. Mar. 1, 2021).

87. Stephen T. Middlebrook, Sarah Jane Hughes & Tom Kierner, *Two Steps Forward, One Step Back: Developments in the Law Affecting Electronic Payments and Financial Services*, 73 Bus. Law. 277, 281 (2018).

88. Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC.gov (Apr. 19, 2021, 9:43 AM), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

89. *Id.*

IX. Conclusion

As in past years, we continue to see regulators struggle to deal with new and evolving financial products. We anticipate that federal and state agencies will continue to fight over which should have primary authority over the FinTechs. Business lawyers should also expect to see additional regulations and enforcement actions in the area of virtual currency. We note that Federal Reserve Chair Jerome Powell has already announced that in the near future the Federal Reserve Board will publish a paper discussing use of new technology in payments, including the possibility of issuing a central bank digital currency.[90] The Board has also issued proposed rules governing the use of FedNow, its new instant payment system which it expects to be available in 2023.[91] As the regulatory framework for real-time payment networks evolves, we expect to see additional actions from CFPB and states with regard to new financial products like Earned Wage Access which are made possible by these new payment networks.

90. Press Release, Fed. Reserve Bd., Federal Reserve Chair Jerome H. Powell Outlines the Federal Reserve's Response to Technological Advances Driving Rapid Change in the Global Payments Landscape (May 20, 2021), https://www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm.

91. Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, 86 Fed. Reg. 31376 (June 11, 2021).

Intermediary Liability and Section 230 Developments

*By Chase J. Edwards**

I. Introduction

The service provider immunity provision of the Communications Decency Act ("CDA")[1] is nothing less than a cornerstone of the modern Internet Age. The Act was passed in 1996 in an effort to stem the tide of lawsuits against early Internet platforms based on content created by third parties. It provides an "interactive computer service"[2] ("ICS") with immunity against lawsuits stemming from information provided by third parties.[3] Colloquially known by its section number in Title 47 of the U.S. Code, Section 230 allowed the Internet to grow into its current form by shielding platforms from most federal claims[4] and preempting conflicting state claims.[5] Over the years, courts have confirmed that Section 230's immunity clause covers virtually all forms of third-party content published by platforms of all types (e.g., social media, e-commerce, dating) even if the information is patently inaccurate, illegal, or intended to deceive others.

The developments included in this survey relate to a wide array of business law topics, including facial recognition software (Part II.B), product liability suits against Amazon (Part II.D), and cryptocurrency (Part II.E).

The future of Section 230 is uncertain due to controversy surrounding content moderation by major platforms including warning labels, user bans, and deplatforming. This survey concludes with a discussion of several proposed and

* Associate Professor of Business Law, Associate Director of the Center for Critical Infrastructure Cybersecurity, University of Louisiana at Lafayette.

1. Pub. L. No. 104-104, § 509, 110 Stat. 56, 137 (1996) (codified as amended at 47 U.S.C. § 230 (2018)).

2. The CDA defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2).

3. *Id.* § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."). An "information content provider" is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." *Id.* § 230(f)(3).

4. Certain federal claims are excluded from the preemptive effect of Section 230. *Id.* § 230(e)(1), (2), (4) & (5).

5. *Id.* § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.").

enacted legislative reforms that resulted from an unprecedented groundswell of criticism of Section 230 (Part IV). Given the wide-ranging application of Section 230's immunity clause to companies that constitute a significant portion of the economy, all business lawyers should monitor its current applications and potential future.

II. Applications of Section 230

A. Negligent Design

The past several years have seen several opinions regarding the liability of Snap, Inc. for the design of its popular app Snapchat. Two cases, *Maynard v. Snapchat, Inc.*[6] and *Lemmon v. Snap, Inc.*,[7] were discussed in last year's survey.[8] Both cases resulted from young users attempting to drive at breakneck speeds while using Snapchat's "speed filter." Filters are designed by the company and added to Snapchat to overlay a variety of information onto a user's pictures. In the case of the "speed filter," the app used a phone's GPS information to overlay the current speed of the person taking the photo. Surprising no one, several people were killed or grievously injured in crashes involving users posting pictures showing themselves driving at over 100 miles per hour.

In its initial decision in the *Maynard* case, the trial court ruled in favor of Snap on Section 230 grounds. On appeal, the Georgia Court of Appeals held that Snap was not entitled to Section 230 immunity because the claim was based on negligent design of Snap's software and not on any third-party speech.[9] On remand, the trial court held that Section 230 was not applicable and conducted a standard duty/breach analysis, finding that Snap did not have a duty to prevent this injury. The Georgia Court of Appeals affirmed.[10]

In *Lemmon*, three young men were killed in an automobile accident caused by users' attempts to log an entry in Snapchat at more than 100 miles per hour. Shortly before the car crashed into a tree at about 113 miles per hour, one of the passengers posted a Snapchat entry documenting the vehicle traveling at 123 miles per hour.[11] The Ninth Circuit, reversing the trial court, held, like the Georgia court in *Maynard*, that Section 230 immunity was unavailable because the negligent-design claim was not based on any third-party speech.[12]

B. Facial Recognition

The use of facial recognition software has proliferated in both government and private sectors. In an interesting case involving this emerging and controversial technology, Vermont's Attorney General sued one of the leading companies in

6. 816 S.E.2d 77 (Ga. Ct. App. 2018).
7. 440 F. Supp. 3d 1103 (C.D. Cal. 2020), *rev'd & remanded*, 995 F.3d 1085 (9th Cir. 2021).
8. Chase J. Edwards, *Developments in Intermediary Liability*, 76 Bus. Law. 339, 344–45 (2020).
9. *Maynard*, 816 S.E.2d at 81.
10. Maynard v. Snapchat, Inc., 851 S.E.2d 128 (Ga. Ct. App. 2020).
11. *Lemmon*, 995 F.3d at 1088.
12. *Id.* at 1093–94.

the industry, Clearview AI, for violating Vermont's Consumer Protection Act and its Fraudulent Acquisition of Data law.[13] Clearview AI attempted to use Section 230 as a shield, but the court denied Section 230 immunity because the state's claims were not based on any third-party content. Instead, they were "based on the means by which Clearview acquired the photographs, its use of facial recognition technology to allow its users to easily identify random individuals from photographs, and its allegedly deceptive statements regarding its product."[14]

C. Soliciting Content for a Shared Document

Elliott v. Donegan[15] provided an interesting look at the applicability of Section 230 to the web-based apps and tools that have become increasingly popular since the pandemic forced the world into remote working arrangements. The defendant in this case created a #MeToo-inspired, publicly available Google spreadsheet called "Shitty Media Men" and encouraged the anonymous reporting of misbehaving men in the media. The plaintiff sued for defamation after he found his name on the list with notations that multiple women had accused him of sexual violence.

The defendant sought to use Section 230 as a shield on the grounds that the spreadsheet operated like a message board. The court agreed that the creator of the spreadsheet qualified as an ICS, but did not dismiss the complaint because plaintiff alleged that defendant herself had created the allegedly defamatory content, making her an "information content provider."[16] However, the court's analysis provides for Section 230 protection as long as all of the information contained in the spreadsheet was contributed by third parties.[17]

D. Amazon and Product Liability Laws

When a product it sells causes injury, an intermediary like Amazon may seek to avoid liability by arguing that its role in the transaction places it outside the scope of the state product liability law. These laws generally impose liability on the "seller." Courts have reached differing conclusions on whether Amazon has acted as a "seller" in a particular transaction.

For instance, in *Bolger v Amazon.com, LLC,*[18] the court held that "Amazon's own involvement in the distribution of an allegedly defective product supports strict liability."[19] The court distinguished products that are sold through the "fulfilled by Amazon" feature from those that are shipped from the supplier wherein Amazon serves solely as the marketplace platform. Likewise, in *Loomis v. Amazon.com LLC*, after an extensive evaluation of liability stemming from an

13. State v. Clearview AI, Inc., No. 226-3-20 Cncv (Vt. Super. Ct. Sept. 10, 2020).
14. Slip op. at *8.
15. 469 F. Supp. 3d 40 (E.D.N.Y. 2020).
16. *Id.* at 57.
17. *Id.* at 57–59.
18. 267 Cal. Rptr. 3d 601 (Ct. App. 2020).
19. *Id.* at 626.

exploding hoverboard incident, the court discussed the vertical integration of the Amazon supply chain and determined that in this case Amazon was subject to California's strict liability law. The factors that the court found relevant included Amazon's "1) interacting with the customer, 2) taking the order, 3) processing the order to the third party seller, 4) collecting the money, and 5) being paid a percentage of the sale."[20]

However, state tort laws vary. Another Amazon hoverboard case reached a different conclusion and held that Amazon was not a "seller" within the scope of the Illinois product liability law. In *Great Northern Insurance Co. v. Amazon.com, Inc.*,[21] the court explained that "the Supreme Court of Illinois has consistently conveyed that the key criterion for being a seller is exercising control over the *product*, not over the *purchasing process*."[22]

In *Oberdorf v. Amazon.com Inc.*,[23] the Third Circuit held that Amazon was a "seller" under the Pennsylvania product liability law. But after rehearing the case en banc, the full court vacated the panel decision and certified the question of state law to the Pennsylvania Supreme Court.[24] The Pennsylvania court agreed to consider the issue, which it phrased as: "Under Pennsylvania law, is an e-commerce business, like Amazon, strictly liable for a defective product that was purchased on its platform from a third-party vendor, which product was neither possessed nor owned by the e-commerce business?"[25] The Pennsylvania Supreme Court's determination should provide a definitive resolution of the issue under Pennsylvania law.

E. Hijacked YouTube Channels

The sheer number of cryptocurrencies available to investors has increased dramatically over the past few years despite many open questions about important issues such as taxation, jurisdiction, and remedies.[26] Further complicating the matter is the manner in which the asset is held. While many major brokerages have expanded their offerings to include a few major cryptocurrencies, owners can choose to hold their "coins" or "tokens" in a "crypto wallet."

Ripple Labs, the creator of a cryptocurrency called XRP, was the target of an online scam that used videos posted on hijacked YouTube channels to dupe users into transferring their XRP to an account that they believed belonged to

20. 277 Cal. Rptr. 3d 769, 780 (Ct. App. 2021).

21. No. 19 C 684, 2021 WL 872949 (N.D. Ill. Mar. 9, 2021).

22. *Id.* at *4. The Fourth Circuit had previously reached the same conclusion in its analysis of Maryland law. Erie Ins. Co. v. Amazon.com, Inc., 925 F.3d 135 (4th Cir. 2019).

23. 930 F.3d 136 (3d Cir. 2019), *opinion & judgment vacated on reh'g en banc*, 936 F.3d 182 (3d Cir. 2019).

24. Oberdorf v. Amazon.com, Inc., 818 F. App'x 138 (3d Cir. 2020), *certified question accepted*, 237 A.3d 394 (Pa. 2020).

25. Oberdorf v. Amazon.com, Inc., 237 A.3d 394 (Pa. 2020).

26. *See Cryptocoins Are Proliferating Wildly. What Are They All For?*, Economist (June 12, 2021), https://www.economist.com/finance-and-economics/2021/06/10/cryptocoins-are-proliferating-wildly-what-are-they-all-for ("Fully 10,000 are listed on CoinMarketCap, a website, nearly twice as many as a year ago.").

Ripple. In *Ripple Labs Inc. v. YouTube LLC*, Ripple sued YouTube alleging that it failed to adequately respond to takedown notices, thus exacerbating the loss to both users and the company.[27] The court threw out Ripple's claims predicated on California's right of publicity and unfair competition laws. It held that since YouTube did not upload the videos or materially contribute to the scam, YouTube could claim the protection of Section 230.[28]

III. FOSTA

A federal law known as FOSTA[29] was enacted to combat sex trafficking by rolling back Section 230 immunity for websites that intentionally or recklessly host user-generated advertisements promoting that practice. Its preamble states that Section 230 "does not prohibit the enforcement against providers and users of interactive computer services of Federal and State criminal and civil law relating to sexual exploitation of children or sex trafficking."[30] In the three years since its passage, neither federal law enforcement nor the state attorneys general have expanded prosecution under the FOSTA criminal provision and few, if any, victims of trafficking have successfully availed themselves of the federal remedies provided in the amendment.[31]

In at least two cases, plaintiffs failed to recover because they pursued their claims under state laws that FOSTA did not exempt from Section 230.[32] Both courts held that FOSTA does not include an exemption for state law civil claims.

IV. Legislative Efforts to Modify Section 230

Last year's survey[33] covered President Trump's Executive Order[34] entitled Preventing Online Censorship, which targeted Section 230 for major reform. President Biden revoked that order soon after taking office.[35] Elsewhere in government, the push to modify Section 230 has never had more momentum. Eighteen bills were introduced in the 116th Congress and some were reintroduced in the 117th Congress along with others that aim to limit the scope, change the application of, or outright repeal Section 230.[36]

27. No. 20-cv-02747-LB, 2020 WL 6822891, at *2 (N.D. Cal. Nov. 20, 2020).
28. *Id.* at *6–7.
29. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018) (codified at 47 U.S.C. § 230(e)(5) (2018)).
30. *Id.*
31. U.S. Gov't Accountability Off., GAO-21-385, Sex Trafficking: Online Platforms and Federal Prosecutions 25 (2021), https://www.gao.gov/products/gao-21-385.
32. M.L. v. Craigslist Inc., No. C19-6153 BHS-TLF, 2020 WL 6434845 (W.D. Wash. Apr. 17, 2020), *report & recommendation adopted*, No. C19-6153 BHS-TLF, 2020 WL 5494903 (W.D. Wash. Sept. 11, 2020); J.B. v. G6 Hosp., LLC, No. 19-cv-07848-HSG, 2020 WL 4901196 (N.D. Cal. Aug. 20, 2020), *reh'g denied*, 2020 WL 7260057 (N.D. Cal. Dec. 10, 2020).
33. Edwards, *supra* note 8, at 345–47.
34. Exec. Order No. 13925, 85 Fed. Reg. 34079 (May 28, 2020).
35. Exec. Order No. 14029, 86 Fed. Reg. 27025 (May 14, 2021).
36. Kiran Jeevanjee et al., *All the Ways Congress Wants to Change Section 230*, Slate (Mar. 23, 2021, 5:45 AM), https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html.

However, the State of Florida is not waiting for Congress to act. In a move that brought about an immediate legal challenge,[37] Governor Ron DeSantis signed Florida's Transparency in Technology Act[38] into law. The law purports to create a right of action for private citizens against "Big Tech" and imposes fines of up to $250,000 per day for deplatforming political candidates.[39] As amicus briefs pile up and legal scholars pick apart the flaws in the legal arguments,[40] the one thing that seems certain is that some sort of change is on the horizon for Section 230.

37. NetChoice LLC v. Moody, No. 4:21cv220-RH-MAF (N.D. Fla. filed May 27, 2021).

38. S.B. 7072, 2021 Sess. (Fla. 2021).

39. Press Release, State of Fla., Governor Ron DeSantis Signs Bill to Stop the Censorship of Floridians by Big Tech (May 24, 2021), https://www.flgov.com/2021/05/24/governor-ron-desantis-signs-bill-to-stop-the-censorship-of-floridians-by-big-tech/.

40. Eric Goldman, *31 Bogus Passages from Florida's Defense of Its Censorship Law*—NetChoice v. Moody, Tech. & Mktg. L. Blog (June 24, 2021), https://blog.ericgoldman.org/archives/2021/06/31-bogus-passages-from-floridas-defense-of-its-censorship-law-netchoice-v-moody.htm.

Developments in Copyright and Trademark Law

*By John A. Rothchild**

I. Introduction

During the survey year, the U.S. Supreme Court issued one blockbuster decision involving copyrights on software and another significant decision involving trademark law applied to domain names. Part II discusses the Court's decision ending a dispute between Oracle and Google over software code used in the Android mobile platform, as well as some cases on the volitional-conduct requirement and the making-available right. Part III addresses the Court's decision about the eligibility for trademark registration of domain names having the form "generic.com" and a Sixth Circuit case about the circumstances under which an online marketplace may be directly liable for trademark infringement occurring in transactions it facilitates.

II. Copyright Law Developments

A. Copying of Application Programming Interface Procedure Names Is Fair Use

In *Google LLC v. Oracle America, Inc.*,[1] the U.S. Supreme Court resolved a long-running dispute between two behemoths of the computing industry, and placed its imprimatur on a type of copying that is aimed at making it easier for programmers to create new software.

The dispute arose when Google set about developing a software platform, called Android, that would run on mobile telephones. One element of the platform was a set of ready-made routines that software developers could incorporate, free of charge, into their own programs designed to run on Android phones. Using these routines would save them the effort they would otherwise need to expend to code standard and relatively low-level functions. These routines constitute what is called an application programming interface ("API").[2]

When Google began working on Android, there was an existing API with which millions of programmers were already familiar, associated with the Java SE programming language, which was used to write programs that ran on

* Professor, Wayne State University Law School.

1. 141 S. Ct. 1183 (2021).

2. *Id.* at 1191.

desktop and laptop computers.[3] Google decided to design its Android API so that Java programmers could use it without learning a new programming language. To accomplish this, the Android API's routines had to be organized and named in the same way as those in the Java API. The Java API organized the routines hierarchically. The individual routines, called "methods," were grouped together into "classes," and the classes were grouped into "packages." Each method was also given a name. To access a particular method, a programmer would call it up using a statement reflecting both the organizational hierarchy and the method's name. For example, to call a method that determines which of two integers is larger, the programmer would write a statement that includes the string "java.lang.Math.max," where "java.lang" designates the package where the routine is found, "Math" designates the applicable class within that package, and "max" is the name of the method that does the job.[4]

To mirror in the Android API the organizational and naming conventions of the Java API, Google copied about 11,500 lines of what is called "declaring code." This is not the code that constitutes the routine and performs the desired task (such as determining which of two integers is larger), but only the code that names the routines and allows them to be called up, corresponding to thirty-seven of the Java API's packages.[5] Google did not copy the code that runs when a Java routine is called up, but rather wrote its own implementing code from scratch. The implementing code amounted to 2.86 million lines. The code that Google copied therefore represented only a small proportion of the code constituting the Java API.[6]

Oracle was the successor to Sun Microsystems, the creator of Java, and owned the copyright to the code that constituted it. Oracle sued Google, claiming that Google infringed its copyright both by copying the literal declaring code and by replicating the hierarchical structure of the Java API. After a jury trial, the district court held that the API was not protected by copyright, as it constituted a "system or method of operation" beyond the scope of the Copyright Act.[7] On appeal, the Federal Circuit reversed, holding that both the declaring code and its organizational structure were protected.[8] After a second trial, the jury found that Google's copying of these elements of the Java API was fair use. On a second appeal, the Federal Circuit once again reversed, holding that, as a matter of law, the use was not fair.[9]

The U.S. Supreme Court granted certiorari and held that the Federal Circuit had erred in its determination that Google's use was not fair. The Court declined to decide the threshold issue of whether the Java API code or organizational

3. *Id.* at 1190.
4. *Id.* at 1191–93.
5. *Id.*
6. *Id.* at 1205.
7. *Id.* at 1194 (quoting 17 U.S.C. § 102(b)); Oracle Am., Inc. v. Google Inc., 872 F. Supp. 2d 974, 977 (N.D. Cal. 2012), *rev'd & remanded*, 750 F.3d 1339 (Fed. Cir. 2014).
8. Oracle Am., Inc. v. Google Inc., 750 F.3d 1339, 1354 (Fed. Cir. 2014).
9. Oracle Am., Inc. v. Google LLC, 886 F.3d 1179, 1210 (Fed. Cir. 2018), *rev'd*, *Google*, 141 S. Ct. at 1209.

structure was protected by copyright. Instead, it assumed that the API was protected, and held that Google's use of it was fair.[10]

In its analysis of fair use, the Court applied the familiar four-factor test from section 107 of the Copyright Act.[11] But in a departure from the usual judicial exposition of the factors,[12] the Court began with, and accorded substantial significance to, the second factor, which considers "the nature of the copyrighted work."[13] The Court observed that the nature of the work in question, namely the declaring code, differs from ordinary computer code (such as the implementing code that actually performs the function for which a method is called) in that it is "inextricably bound up" with elements of the Java API that all agree are not protected by copyright: the "general system" of computing tasks, the "idea" of organizing software routines hierarchically, and the use of particular method calls.[14] Likewise, it is "inextricably bound up" with the implementing code, which is protected by copyright, but which Google did not copy.[15] On account of these features, the Court found, "the declaring code is, if copyrightable at all, further than are most computer programs (such as the implementing code) from the core of copyright."[16] This factor accordingly tends to support a finding of fair use.

On the other fair use factors too, the Supreme Court disagreed with the Federal Circuit. The Federal Circuit found that Google's use of the copied code was not "transformative" under the first factor,[17] because, among other things, Google's Android API served the same function as the Java API.[18] But the Court held that the Android API "provided a new collection of tasks operating in a distinct and different computing environment," which "were carried out through the use of new implementing code (that Google wrote) designed to operate within that new environment."[19] The Court also disagreed with the Federal Circuit's application of the third factor, "the amount and substantiality of the portion used in relation to the copyrighted work as a whole."[20] The Federal Circuit found that Google had copied too much, because "the parties stipulated that only 170 lines of code were necessary to write in the Java language," but Google had copied 11,500 lines, and Google's desire "to meet the expectations of intended

10. *Google*, 141 S. Ct. at 1197.
11. 17 U.S.C. § 107.
12. *See, e.g.*, Authors Guild v. Google, Inc., 804 F.3d 202, 220 (2d Cir. 2015) ("The second factor has rarely played a significant role in the determination of a fair use dispute.").
13. 17 U.S.C. § 107(2).
14. *Google*, 141 S. Ct. at 1201.
15. *Id.*
16. *Id.* at 1202.
17. Oracle Am., Inc. v. Google LLC, 886 F.3d 1179, 1198–99 (Fed. Cir. 2018) (quoting Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994)), *rev'd*, *Google*, 141 S. Ct. at 1202–04; *see* 17 U.S.C. § 107(1) (setting forth, as the first factor regarding "fair use," "the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes").
18. *Oracle Am.*, 886 F.3d at 1200.
19. *Google*, 141 S. Ct. at 1203.
20. 17 U.S.C. § 107(3).

customers" did not justify such a large appropriation.[21] But the Court said that the relevant criterion was the ratio between the number of lines of the Java API that Google copied (11,500) and the number it did *not* copy (2.86 million), namely 0.4 percent.[22]

The Court's analysis suggests that courts will be more open to finding fair use in the context of computer programs when the purpose of the copying was to promote the creation of new computer programs.

B. The Volitional-Conduct Requirement

Since the early days of the commercial Internet, courts have held that a provider of online services can be held directly liable for copyright infringement only if the conduct alleged to be infringing is "volitional."[23] Two district courts arrived at different conclusions on the issue of whether a website operator acted volitionally when it allowed users to upload copyrighted materials.

In *Sid Avery & Associates, Inc. v. Pixels.com, LLC*,[24] the court found that the defendant did not engage in volitional conduct when it operated a website that allowed users to upload photographs that others could purchase as prints or have printed on items, such as coffee mugs and tote bags. Relying on a Ninth Circuit decision, the court explained that, to demonstrate volitional conduct, the plaintiff had to show that the defendant "exercised control (other than by general operation of [its website]); selected any material for upload, download, transmission, or storage; or instigated any copying, storage, or distribution" of the photographs.[25] Because defendant did not select the images to be uploaded (its uploading users did), or determine which items were purchased (its purchasers did), and because it in fact prohibited the uploading of infringing content and took down such content as soon as possible, the alleged infringement did not result from defendant's volitional conduct and defendant could not be held directly liable.[26]

In *Atlantic Recording Corp. v. Spinrilla, LLC*,[27] a court reached the opposite result on somewhat similar facts by applying a notably different analysis. The website in question allowed approved users to upload mp3 files of hip-hop songs and "mixtapes" consisting of multiple songs. Other users could select from the uploaded music files and listen to them streamed via the Internet. The defendant had a policy of removing music files once notified they were infringing. The court relied on prior decisions to conclude that the website operator engaged

21. *Oracle Am.*, 886 F.3d at 1206–07.

22. *Google*, 141 S. Ct. at 1204–05.

23. The seminal case is *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995). Later opinions addressing this requirement have clarified that conduct will be deemed "volitional" if it is the proximate cause of the harm. *See, e.g.*, Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 666 (9th Cir. 2017).

24. No. CV-18-10232, 2021 WL 736258 (C.D. Cal. Feb. 24, 2021).

25. *Id.* at *3 (quoting VHT, Inc. v. Zillow Grp., Inc., 918 F.3d 723, 732 (9th Cir. 2019)).

26. *Id.*

27. 506 F. Supp. 3d 1294 (N.D. Ga. 2020).

in volitional conduct when it allowed music to be streamed from the site.[28] Because the streaming constituted an unauthorized public performance of copyrighted sound recordings, the website operator was directly liable for the infringement.[29]

C. Latest Case on the Making-Available Right

A district court in Washington State became the latest court to hold that merely making a copyrighted work available to the public, without actually distributing copies of it, does not infringe the public distribution right.

In *SA Music, LLC v. Amazon.com, Inc.*,[30] the copyright owners of numerous musical works composed between the 1920s and the 1960s (including jazz standards such as *Stormy Weather* and the music of the 1939 motion picture *The Wizard of Oz*) charged that defendants made unauthorized copies of the songs, compiled them into albums accompanied by copies of the original album artwork, and made the recordings available to purchase via digital download on Amazon's online music store. Amazon, which was named as a defendant, moved to dismiss the claim that it infringed the plaintiffs' public distribution right[31] merely by making the unauthorized copies available for purchase. The court agreed with Amazon, holding "that distribution of a copyrighted work under § 106(3) requires 'actual dissemination' of the copyrighted work and, in the context of a digital music store, actual dissemination means the transfer (or download) of a file containing the copyrighted work from one computer to another."[32]

III. Trademark Law Developments

A. Registering "generic.com" as a Trademark

Booking.com is a website that enables its users to make vacation rentals and other travel arrangements. The operator of the website sought to register "Booking.com" as a trademark for the services it offers. The U.S. Patent and Trademark Office ("USPTO") refused to issue the registration on the ground that the proposed mark is generic. A generic mark is one that refers to a *type of* good or service rather than the *source of* a particular good or service. For example, "beer" is a generic term for a type of beverage, while "Bell's Two Hearted Ale" is a trademark that distinguishes a particular beer that comes from a particular source. Trademark law provides that a generic mark cannot be registered.[33]

28. *Id.* at 1307–16 (citing, among other cases, Am. Broad. Cos. v. Aereo, Inc., 573 U.S. 431 (2014); Spanski Enters., Inc. v. Telewizja Polska, S.A., 883 F.3d 904 (D.C. Cir. 2018)).

29. *Id.* at 1316 (citing 17 U.S.C. § 106(6) (addressing the exclusive right of public performance by means of digital audio transmission)).

30. No. 20-CV-00105, 2020 WL 3128534 (W.D. Wash. June 12, 2020).

31. 17 U.S.C. § 106(3).

32. *SA Music*, 2020 WL 3128534, at *7 (quoting Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007); *In re* Napster, Inc. Copyright Litig., 337 F. Supp. 2d 796, 802 (N.D. Cal. 2005)).

33. *See, e.g.*, Savannah Coll. of Art & Design, Inc. v. Sportswear, Inc., 983 F.3d 1273, 1282 (11th Cir. 2020).

The district court and the Fourth Circuit held that the USPTO's analysis was erroneous, and, in *U.S. Patent & Trademark Office v. Booking.com B.V.*,[34] the U.S. Supreme Court agreed. The USPTO based its analysis on a nineteenth-century case in which the U.S. Supreme Court held that "a generic corporate designation added to a generic term does not confer trademark eligibility."[35] Thus, a brewery called "Beer Company" could not successfully argue that, while "Beer" is unregistrable as generic, the addition of the word "Company" made the name distinctive and therefore registrable. The Court held that it is different with domain names: The addition of a generic top-level domain (like ".com") to a generic name (like "beer") *may* result in a distinctive designation that is eligible for registration. Because "only one entity can occupy a particular Internet domain name at a time," consumers may associate a domain name with a particular source of goods or services.[36]

Whether a domain name of the form "generic.com" actually is distinctive depends on consumer perception. What counts is "[t]he primary significance of the registered mark to the relevant public."[37] The lower courts determined that consumers do in fact perceive "Booking.com" as indicating a particular online source of travel-related services, rather than as a *type* of travel-service providers: Nobody would ever say "Travelocity is my favorite Booking.com."[38]

The Court thus rejected a per se rule that a domain name of the form "generic.com" is ineligible for registration as a trademark. Whether a particular domain name is registrable will depend on how consumers perceive it.

B. Liability of an Online Platform for Facilitating Trademark-Infringing Transactions

Redbubble operates an online marketplace that allows artists to upload images they create and allows consumers to order items (such as clothing, wall art, and jigsaw puzzles) that display those images. Some artists uploaded designs that included trademarks owned by Ohio State University ("OSU"), and consumers purchased items bearing those designs. OSU sued Redbubble for trademark infringement. The district court granted summary judgment to Redbubble, finding that its role in the transactions was too limited to render it directly liable for the resulting trademark infringement.

In *Ohio State University v. Redbubble, Inc.*,[39] the Sixth Circuit held that the district court should not have granted summary judgment. The appellate court began its analysis by noting that, in previous cases, courts have determined

34. 140 S. Ct. 2298 (2020), *aff'g* 915 F.3d 171 (4th Cir. 2019), *aff'g* 278 F. Supp. 3d 891 (E.D. Va. 2017).

35. *Id.* at 2305 (referencing Goodyear's India Rubber Glove Mfg. Co. v. Goodyear Rubber Co., 128 U.S. 598 (1888)).

36. *Id.* at 2306.

37. *Id.* at 2304 (quoting 15 U.S.C. § 1064(3)).

38. *See id.* at 2304–05; *Booking.com, B.V.*, 915 F.3d at 180–87; *Booking.com, B.V.*, 278 F. Supp. 3d at 901–18.

39. 989 F.3d 435 (6th Cir. 2021), *rev'g* 369 F. Supp. 3d 840 (S.D. Ohio 2019).

that some online marketplaces, including Amazon (to the extent that it hosts third-party sellers) and eBay, are not directly liable for trademark infringement occurring by virtue of sales that they facilitate.[40] Such platforms employ a hands-off business model. Their role is to connect willing buyers with willing sellers, earning commissions from the transactions. On the other hand, the manufacturers of trademark-infringing items, and the retail stores (online or brick-and-mortar) that sell them, are generally held liable. These entities may therefore be placed on a "spectrum," with Amazon and eBay at one end and retailers and manufacturers at the other end.[41] The question that the court addressed was where Redbubble falls on this spectrum. More generally, "what level of involvement and control must a defendant exercise over the creation, manufacture, or sale of offending goods to be considered akin to a 'seller' or 'manufacturer'" and therefore potentially directly liable for the resulting infringement?[42]

Redbubble has a greater involvement in the transactions it facilitates than do Amazon and eBay. When a consumer places an order, "Redbubble automatically contacts the artist and arranges the manufacturing and shipping of the product with independent third parties."[43] Is this degree of involvement enough to render Redbubble liable? The appellate court determined that "one key distinction" relevant to this question "is the degree to which the party represents itself, rather than a third-party vendor, as the seller, or somehow identifies the goods as its own."[44] The record included some findings of relevance to this criterion. For example, the goods that consumers order "often arrive in Redbubble packaging and contain Redbubble tags."[45] These facts created a triable issue on the degree of Redbubble's involvement, making the district court's grant of summary judgment erroneous.

40. *Id.* at 446 (citing, as one example, Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010)).
41. *Id.* at 447.
42. *Id.*
43. *Id.* at 440.
44. *Id.* at 448.
45. *Id.* at 440–41.

Developments in Advertising and Consumer Protection

*By Richik Sarkar**

I. Introduction

This survey begins with several cases involving the Telephone Consumer Protection Act ("TCPA"): the impact of the U.S. Supreme Court's decision last year in *Barr v. American Association of Political Consultants* and a new U.S. Supreme Court decision determining what constitutes an "automatic telephone dialing system" under the same statute (Part II). It continues with cases concerning account ownership and publicity rights in the context of social media (Part III). The U.S. Supreme Court and lower courts reviewed the scope of the Computer Fraud and Abuse Act ("CFAA") (Part IV). The survey concludes with cases involving deceptive business practices (Part V) and cybersecurity (Part VI).

II. TCPA Litigation

A. Fallout from *Barr*

Before 2015, the TCPA prohibited almost all robocalls to cell phones in the United States.[1] In 2015, as part of the Bipartisan Budget Act, Congress lifted the robocall restriction for calls "made solely to collect a debt owed to or guaranteed by the United States."[2] In 2020, the American Association of Political Consultants filed a lawsuit challenging the government-debt exception and seeking to invalidate the TCPA as a whole.[3] As reported in last year's survey, in *Barr v. American Association of Political Consultants, Inc.*, the U.S. Supreme Court held that the government-debt exception was unconstitutional but that the provision was severable, thus leaving the rest of the statute in place.[4] Ironically, the U.S. Supreme Court's resolution of this issue led to a new split among federal courts, focusing on the question: can courts consider claims that arose between the nascence of the 2015 exception and its severance in *Barr*?

* Richik Sarkar is a commercial litigation partner at Dinsmore & Shohl LLP. Richik spearheads commercial, consumer, and cybersecurity cases and projects for small, middle-market, and Fortune 500 companies. Richik thanks Nathan J. Hall, Washington University School of Law, J.D. candidate 2022, for his immense contribution to this survey.

1. Barr v. Am. Ass'n of Political Consultants, Inc., 140 S. Ct. 2335, 2344 (2020).
2. 47 U.S.C. § 227(b)(1)(A)(iii) (2018).
3. *Am. Ass'n Political Consultants*, 140 S. Ct. at 2345.
4. Richik Sarkar, *Developments in Advertising and Consumer Protection*, 76 Bus. Law. 313, 317–18 (2020).

In *Creasy v. Charter Communications, Inc.*,[5] the U.S. District Court for the Eastern District of Louisiana found that it did not have jurisdiction to adjudicate TCPA claims based on robocalls made between the passage of the 2015 exception and the 2020 *Barr* decision.[6] The court based its decision on "the timeless principle that '[a]n unconstitutional law is void, and is as no law.'"[7] The Northern District of Ohio found similarly in *Lindenbaum v. Realgy, LLC*,[8] saying that it "cannot wave a magic wand and make that constitutional violation disappear. Because the statute at issue was unconstitutional at the time of the alleged violations, this Court lacks jurisdiction over this matter."[9] However, the U.S. Court of Appeals for the Sixth Circuit reversed in *Lindenbaum v. Realgy, LLC*[10] because severance is not a remedy, and prospective application could only happen through a legislative act, the *Barr* decision could not impact the plaintiff's already pending claim as the U.S. Supreme Court determined that the government-debt-collector exception was automatically displaced from the start and then interpreted what the statute has always meant in its absence.[11]

This Sixth Circuit decision was in line with other district courts. In *LaGuardia v. Designer Brands, Inc.*,[12] the Southern District of Ohio held that the TCPA, with the exception of the invalidated provision, remained effective between 2015 and 2020. The court concluded that the effect of the U.S. Supreme Court's decision "is as if the amendment had never happened and the pre-2015 statute's enforceability is unaffected by the amendment."[13] District courts in the Eighth,[14] Ninth,[15] and Eleventh[16] Circuits have also held that they may enforce violations of the constitutional provisions of the TCPA that occurred between 2015 and 2020.

B. Definition of ATDS—U.S. Supreme Court's Decision in *Facebook, Inc. v. Duguid*

The U.S. Supreme Court resolved a circuit split by deciding *Facebook, Inc. v. Duguid*,[17] clarifying what kinds of automatic telephone dialing systems are subject to the TCPA. The TCPA restricts the use of an automatic telephone dialing system ("ATDS"), defined in the statute as a piece of equipment that has the

5. 499 F. Supp. 3d 499 (E.D. La. 2020).
6. *Id.* at 504.
7. *Id.* at 505 (quoting *Ex Parte* Siebold, 100 U.S. 371, 376 (1879)).
8. 497 F. Supp. 3d 290 (N.D. Ohio 2020).
9. *Id.* at 298–99.
10. 20-4252, 2021 U.S. App. LEXIS 27159 (6th Cir. Sept. 9, 2021).
11. *Id.* at *8–9.
12. No. 2:20-cv-2311, 2021 U.S. Dist. LEXIS 97396 (S.D. Ohio May 24, 2021).
13. *Id.* at *5.
14. *See, e.g.*, Burton v. Fundmerica, Inc., No. 8:19-CV-119, 2020 U.S. Dist. LEXIS 139299 (D. Neb. Aug. 5, 2020).
15. *See, e.g.*, Schmidt v. AmerAssist A/R Sols. Inc., No. CV-20-00230-PHX-DWL, 2020 U.S. Dist. LEXIS 193358 (D. Ariz. Oct. 19, 2020).
16. *See, e.g.*, Moody v. Synchrony Bank, No. 5:20-cv-61 (MTT), 2021 U.S. Dist. LEXIS 57853 (M.D. Ga. Mar. 26, 2021).
17. 141 S. Ct. 1163 (2021).

ability "to store or produce telephone numbers to be called, using a random or sequential number generator," and "to dial such numbers."[18] Duguid sued Facebook over text messages notifying him that someone was attempting to access his Facebook account from a different device.[19] Duguid never had a Facebook account, and he sued Facebook as part of a putative class under the TCPA, alleging that Facebook stored users' phone numbers and automatically messaged them without their consent.[20] The U.S. District Court for the Northern District of California dismissed the suit, finding that Duguid had failed to allege that Facebook sent randomly or sequentially generated text messages. The Ninth Circuit reversed, holding that to qualify as an ATDS a system only needed the capacity to store and dial numbers automatically.[21]

The U.S. Supreme Court granted certiorari to resolve a circuit split on this issue. It reversed the Ninth Circuit, holding that to be an ATDS a system had to use a random or sequential number generator.[22] Applying various canons of statutory construction, the Court concluded that the definition in the TCPA excluded any equipment that did not have this feature.[23] It proceeded to reject Duguid's non-textual arguments that Congress had a goal of broad privacy protection when it enacted the TCPA and that this decision would result in a "torrent of robocalls."[24]

III. Social Media Litigation

JLM Couture, Inc. v. Gutman was brought by JLM Couture, a clothing design firm, against Hayley Paige Gutman, the lead designer for JLM's bridal collection before her resignation.[25] The dispute was over the control of Gutman's social media accounts. In Gutman's contract with JLM, she signed over rights to the intellectual property in her name and designs.[26] The history of her accounts showed high levels of cooperation between herself and JLM, promoting products, lines, and JLM itself.[27] JLM moved for a preliminary injunction to prevent Gutman from making any changes to social media or using any of the intellectual property associated with her name or designs, on the grounds that she had breached her contract.[28] The U.S. District Court for the Southern District of New York granted JLM a preliminary injunction prohibiting Gutman from changing or using the social media accounts.[29] However, the court refused to enjoin Gutman from publicly disparaging JLM, inasmuch as she had not

18. 47 U.S.C. § 227(a)(1) (2018).
19. *Duguid*, 141 S. Ct. at 1168.
20. *Id.*
21. *Id.*
22. *Id.* at 1168–69.
23. *Id.* at 1170.
24. *Id.* at 1171–73.
25. No. 20 CV 10575-LTS-SLC, 2021 U.S. Dist. LEXIS 40953, at *1 (S.D.N.Y. Mar. 4, 2021).
26. *Id.* at *5–10.
27. *Id.* at *10–19.
28. *Id.* at *21–26.
29. *Id.* at *74–75.

contractually waived her right to speak about JLM, and given the First Amendment rule against prior restraints.[30]

In *Takeguma v. Freedom of Expression LLC*,[31] plaintiffs were models whose images were used, without their permission, in social media advertising for a strip club owned and operated by the defendant.[32] Plaintiffs asserted claims for misappropriation of likeness, violations of the Lanham Act, and false light invasion of privacy.[33]

In deciding the cross-motions for summary judgment, the court first found that the false light tort was time-barred because the statute of limitations began to run with the initial publication of the social media advertisements.[34] Not time-barred, however, were plaintiffs' common law right of publicity claims. The court began by finding a common law right of publicity in Arizona based on a combination of state decisional and statutory law.[35] The court then found that the right of publicity in Arizona was a property claim, not a libel or slander claim, and thus was subject to a two-year, not a one-year, statute of limitations.[36] Lastly, the court found that triable issues remained in deciding plaintiffs' false association claims under the Lanham Act.[37] On the other hand, the court granted summary judgment to defendant on the false advertising claims, finding that plaintiffs' claimed injuries were not within the "zone of interests" protected by the Lanham Act and that the alleged wrong was not the proximate cause of plaintiffs' injuries.[38]

IV. Computer Fraud and Abuse Act Cases

The Computer Fraud and Abuse Act of 1986 imposes criminal penalties against one who "intentionally accesses a computer without authorization or exceeds authorized access."[39] How to determine when someone "exceeds authorized access" has been problematic for courts because the intricacies of computer programs have expanded with time and the lines of authority and permitted access have blurred.[40] In *Van Buren v. United States*,[41] the U.S. Supreme Court shed some light on the meaning of that term.

Van Buren was a former police sergeant who ran a license-plate search in a state law enforcement database in exchange for $5,000, despite being aware that he was only allowed to use the database for law enforcement purposes.[42]

30. *Id.* at *65–69.
31. No. CV-18-02552-PHX-MTL, 2021 U.S. Dist. LEXIS 25834 (D. Ariz. Feb. 10, 2021).
32. *Id.* at *1–2.
33. *Id.* at *2.
34. *Id.* at *27–28.
35. *Id.* at *28–30.
36. *Id.* at *32–33.
37. *Id.* at *45.
38. *Id.* at *47–50.
39. 18 U.S.C. § 1030(a)(2) (2018).
40. *See* Andrea M. Matwyshyn, *The Law of the Zebra*, 28 Berkeley Tech. L.J. 155, 164–65 (2013).
41. 141 S. Ct. 1648 (2021).
42. *Id.* at 1653.

The government charged Van Buren with a felony violation for "exceed[ing] authorized access" of the computer system.[43] The Eleventh Circuit found that Van Buren's misuse of the computer was a violation of the CFAA because he had accessed the license plate database for an "inappropriate reason."[44] However, because other circuits had taken a narrower view of what it meant to exceed authorized access, the Court granted certiorari to settle the issue.[45]

The Court reversed the Eleventh Circuit and held that Van Buren did not violate the CFAA.[46] Even though he had an improper purpose for obtaining the data, he did not "exceed[] authorized access" because he had access to the database and was authorized to use it to retrieve license plate information.[47] In dicta, the Court said that it *would have been* a violation if Van Buren had authorization to access the computer but then accessed folders, files, or databases that were off-limits to him.[48] Commentators have said that the Court adopted a "gates up or down" approach to the CFAA, meaning that to violate the provision, a person must "bypass a gate that is down that the person isn't supposed to bypass."[49]

In *United States v. Eddings*, the U.S. District Court for the Eastern District of Pennsylvania relied on the "gates up or down" approach to decide a case where an ex-employee who retained password access to her former employer's computers accessed documents from the company's e-mail server and sent them to donors and media members as part of an extortion plot.[50] Her defense was simple: the gate was up, so she could not have violated the CFAA.[51] The court, however, found that mere possession of a password was not enough to make access "authorized," citing instances of password trafficking which are forbidden by the CFAA, and distinguishing *Van Buren*.[52] The same court relied on *Van Buren* in deciding *KBS Pharmacy, Inc. v. Patel*.[53] The facts more closely resembled those in *Van Buren*; pharmacy employees who had authorized access to the pharmacy's database misused the information in starting their pharmacy nearby.[54] The court found that the CFAA claim should be dismissed because, as in *Van Buren*, the defendants had access to the database at the time and only later misused the information.[55]

In *United Federation of Churches LLC v. Johnson*, the plaintiff, perhaps better known as the Satanic Temple, brought claims against former members who

43. *Id.*
44. *Id.* at 1654.
45. *Id.* at 1653.
46. *Id.* at 1662.
47. *Id.*
48. *Id.*
49. Mark Walsh, *Supreme Court Takes a Byte Out of Computer Crime Law*, ABA J. (June 24, 2021), https://www.abajournal.com/web/article/supreme-court-takes-a-byte-out-of-computer-crime-law (quoting Orin S. Kerr).
50. No. 5:19-cr-00535, 2021 U.S. Dist. LEXIS 114796, at *2–3 (E.D. Pa. June 21, 2021).
51. *Id.* at *12.
52. *Id.* at *13.
53. No. 21-1339, 2021 U.S. Dist. LEXIS 107779 (E.D. Pa. June 9, 2021).
54. *Id.* at *2–4.
55. *Id.* at *5–7.

hijacked two of its Facebook pages.[56] Collectively, the two Facebook pages have over 17,500 followers.[57] Access to the Facebook pages was controlled by the Church and limited to approved administrators who were subject to a code of conduct.[58] The defendants in the case had been authorized administrators.[59] After they renounced their membership in the Church, they took control of the Facebook pages and posted manifestos on the pages about what they claimed were abuses of the Church.[60]

The Church brought several claims against the defendants, including claims under the CFAA, the Anti-Cybersquatting Consumer Protection Act ("ACPA"), and defamation.[61] The court held that plaintiff failed to state a claim under the CFAA because it did not allege it had revoked the defendants' authorization to access the Facebook pages.[62] It also held that a post-domain path (i.e., "TheSatanicTempleWashington" in facebook.com/TheSatanicTempleWashington) is not a "domain name" and therefore use of plaintiff's trademark in that path is not a violation of the ACPA.[63] Lastly, it declined to rule on the defamation claim, invoking the doctrine of "ecclesiastical abstention" and finding it "may not resolve the defamation claim without delving into doctrinal matters."[64]

V. Deceptive Business Practices

MoviePass, a subscription service launched in 2011, allowed members to watch as many movies as they wanted at any theater they wanted. According to the complaint issued by the Federal Trade Commission ("FTC") in 2018, MoviePass realized that it was facing a significant cash deficit and decided to implement fraudulent business practices. For the subscribers using MoviePass most frequently, MoviePass implemented "password disruption," a practice that invalidated the passwords of 75,000 subscribers and forced them to reset their passwords. It also imposed ticket verification requirements on 20 percent of users, which obstructed the use of the product due to problems with the software. MoviePass also failed to protect its customer data from unauthorized access. These practices, the FTC alleged, violated the FTC Act, and the negative option subscription plan violated the Restore Online Shoppers' Confidence Act.[65] MoviePass settled the claims with the FTC in exchange for promises to refrain from misrepresentations and comply with mandated security programs and third-party monitoring. MoviePass was bankrupt at the time of the consent order and unable to pay any money judgment.[66]

56. No. 2:20-cv-00509-RAJ, 2021 U.S. Dist. LEXIS 36717, at *1 (W.D. Wash. 2021).
57. *Id.* at *2–3.
58. *Id.* at *3.
59. *Id.*
60. *Id.* at *4.
61. *Id.* at *6–7.
62. *Id.* at *12.
63. *Id.* at *15–20.
64. *Id.* at *28.
65. Complaint, *In re* MoviePass, Inc., File No. 192 3000 (F.T.C. 2021).
66. Agreement Containing Consent Order, *In re* MoviePass, Inc., File No. 192 3000 (F.T.C. 2021).

Randon Morris, through a group of companies that he controlled, initiated millions of robocalls to households throughout the United States, promising work-from-home positions that would pay hundreds of dollars a day and falsely claiming to be associated with Amazon.com. People who paid defendants to create a website that would purportedly allow them to earn commissions from Amazon were left with a useless and occasionally defunct website with no way to recover their money. The FTC alleged that they had violated the FTC Act and the Telemarketing Sales Rule.[67] Defendants stipulated to an order banning them from using robocalls or offering work-from-home business schemes and requiring them to pay over $2 million to settle the claims.[68]

Flo is a popular and accessible smartphone app that allows consumers to track their menstrual cycles and gives them predictive information about ovulation and general gynecological health. Given the nature of the app, women must input sensitive health data to use it. In its privacy policy, Flo assured users that information shared with third parties did not include data related to the user's menstrual cycle, pregnancy, or symptoms. However, Flo allegedly did share some of this information with third parties, including Facebook and Google.[69] The *Wall Street Journal* broke the story that Facebook could use snippets of code to intercept a user's sensitive health information transmitted from apps like Flo.[70] The FTC alleged that Flo made numerous misrepresentations about privacy of users' data, in violation of section 5 of the FTC Act.[71] Flo agreed to a consent order prohibiting it from making misrepresentations about privacy and requiring it to instruct third parties to delete its users' personal data.[72]

Everalbum is a photo storage company and app that used facial recognition technology as part of its service. It allowed users to tag faces that its software would then group with similar faces. The FTC alleged that the facial recognition service was turned on by default despite Everalbum's representations that it required affirmative action to use. When users deactivated their accounts, the app informed them that Everalbum would delete their photos. However, Everalbum allegedly retained photos in deactivated accounts indefinitely. The FTC alleged that through these misrepresentations Everalbum had violated section 5 of the FTC Act.[73] Everalbum entered into a consent decree with the FTC, which requires deletion of photos on deactivated accounts and prohibits misrepresentations.[74]

67. Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Nat'l Web Design, LLC, No. 2:20-cv-00846-TS (D. Utah Nov. 30, 2020).

68. Order Granting Stipulated Motion for Permanent Injunction and Monetary Judgment, FTC v. Nat'l Web Design, LLC, No. 2:20-cv-00846-RJS (D. Utah Mar. 12, 2021).

69. Complaint at 3–6, *In re* Flo Health, Inc., No. C-4747 (F.T.C. June 17, 2021).

70. Jeff Horwitz, *Facebook Blocks Collection of Sensitive Data Through Apps Following New York Probe*, Wall St. J. (Feb. 18, 2021), https://www.wsj.com/articles/facebook-blocks-collection-of-sensitive-data-through-apps-following-new-york-probe-11613691592.

71. Complaint at 9–10, *In re* Flo Health, Inc., No. C-4747 (F.T.C. June 17, 2021).

72. Decision and Order, *In re* Flo Health, Inc., No. C-4747 (F.T.C. June 17, 2021).

73. Complaint, *In re* Everalbum, Inc., Docket No. C-4743 (F.T.C. May 6, 2021).

74. Decision and Order, *In re* Everalbum, Inc., Docket No. C-4743 (F.T.C. May 6, 2021).

VI. Cybersecurity

Drizly, an alcoholic beverage delivery company, faced a class-action lawsuit in Massachusetts that alleged that a data breach had occurred, leading to customer information (including e-mail addresses, dates of birth, phone numbers, and IP addresses) being leaked to third parties on the "dark web." Drizly agreed to a settlement with the class, paying $7.1 million in total. Each member of the class is anticipated to get around $14. The settlement agreement benefitted both sides: Drizly could have faced massive exposure had the suit been allowed to continue, and the plaintiffs might have had difficulty overcoming hurdles such as standing and proving injury.[75]

Skymed sells emergency travel and medical evacuation services. Skymed's website displayed a very prominent "HIPAA compliance" seal. Skymed admitted that the seal should not have been on the website and removed it in April 2019. The company allegedly failed to secure customers' data leading to a security incident in May 2019. The FTC alleged that Skymed violated the FTC Act by misrepresenting its compliance with HIPAA and failing to secure customers' data.[76] The company agreed to a consent order requiring it to adopt a comprehensive security plan to prevent future incidents.[77]

Ascension is an analytics company that provides mortgage data to other companies. One of its vendors, OpticsML, received mortgage information that contained the personal information of tens of thousands of consumers. Ascension was required to vet the security measures of OpticsML but failed to do so. OpticsML allegedly allowed the information to sit on an insecure server, allowing approximately fifty-two unauthorized IP addresses to access the information, some tied to Russia and China.[78] The FTC alleged that this was a violation of the Gramm-Leach-Bliley Act Safeguards Rule. Ascension agreed to settle the claims in exchange for a mandated data protection plan.[79]

VII. Conclusion

The survey period has provided numerous decisions with far-reaching implications. Practitioners should monitor the continuing evolution of the TCPA and CFAA as case law continues to limit liability. Considering the dramatic increase in online commerce, the FTC will undoubtedly continue to police cyber business practices. Similarly, disputes involving social media accounts will continue to proliferate.

75. Kristin L. Bryan, *No Happy Hour Here: $7.1 Million Settlement Reached in Alcohol Delivery Data Breach Class Action Litigation, Class Members Anticipated to Get $14 Cash Payout*, Nat'l L. Rev. (May 17, 2021), https://www.natlawreview.com/article/no-happy-hour-here-71-million-settlement-reached-alcohol-delivery-data-breach-class.

76. Complaint, *In re* Skymed Int'l, Inc., No. C-4732 (F.T.C. Jan. 26, 2021).

77. Decision and Order, *In re* Skymed Int'l, Inc., No. C-4732 (F.T.C. Jan. 26, 2021).

78. Complaint, *In re* Ascension Data & Analytics, LLC, File No. 192 3126 (F.T.C. 2021).

79. Agreement Containing Consent Order, *In re* Ascension Data & Analytics, LLC, File No. 192 3126 (F.T.C. 2021).