



Welcome to the October 2022 newsletter prepared by Arnold & Porter’s AdTech and Digital Media group. This newsletter includes legal and regulatory developments relevant to the AdTech and Digital Media industries, the state of venture investment activity in the AdTech industry and updates regarding Arnold & Porter’s activity in the space.

Supreme Court

Texas Law HB 20—5th Circuit blocks Texas social media law as parties turn to SCOTUS: On September 9, 2021, Texas passed House Bill 20 (HB 20), which creates civil liability for social media platforms (with more than 50 million monthly active users) that moderate, remove or label users’ content based on their “viewpoints,” unless considered illegal or “specifically authorized” under federal law. HB 20 also extends to email providers, forbidding them from censoring the content of emails unless it is illegal or obscene. Further, HB 20 requires social media platforms to disclose their content moderation policies and publish an acceptable use policy (AUP). Two trade groups, NetChoice and the Computer and Communications Industry Association (CCIA), challenged HB 20 on First Amendment grounds in *Netchoice v. Paxton*. In December 2021, US District Judge Robert Pitman (WDTX) preliminarily enjoined enforcement of the law. The United States Court of Appeals for the Fifth Circuit stayed the preliminary injunction on May 11, 2022. CCIA and NetChoice then asked the United States Supreme Court to vacate the stay, and on May 31, the court vacated the Fifth Circuit’s stay by a 5-4 vote. Texas subsequently appealed the district court’s ruling, and on September 16, 2022, a divided panel of the Fifth Circuit (Judges Edith Jones and Andrew Oldham, with Judge Leslie H. Southwick largely dissenting) reversed the ruling, thereby allowing HB 20 to take effect.

On October 12, 2022, the Fifth Circuit granted a request by the CCIA and NetChoice to stay enforcement of HB 20 pending Supreme Court review of the Fifth Circuit’s ruling. The CCIA and NetChoice have signaled their intention to file a petition for a writ of certiorari arguing that the Fifth Circuit’s position (upholding HB 20) conflicts with the Eleventh Circuit’s decision in *NetChoice v. Moody*. That decision struck down Senate Bill 7072, a similar anti-moderation bill enacted by the state of Florida in 2021, which imposed sweeping requirements on social-media providers. As a result of the Fifth Circuit’s stay, HB 20 will not take effect until

the Supreme Court has a chance to weigh in. The traction that the CCIA and NetChoice have gained thus far gives BigTech companies, such as Facebook, Google, and Twitter, some hope that the Supreme Court may ultimately strike down HB 20 and similar anti-moderation bills.

[Gonzalez v. Google, LLC](#)—*Whether immunity under Section 230 of the Communications Decency Act extends to recommendations by algorithms* (cert. granted Oct. 3, 2022): This case, which is expected to be heard this winter by the Supreme Court of the United States alongside *Taamneh v. Twitter*, addresses whether Section 230 of the Communications Decency Act of 1996 shields interactive computer services that use algorithms to target and recommend third-party content to users. The plaintiffs, the family of an American woman killed by an ISIS terrorist attack in Paris in 2015, allege that Google (as parent of YouTube) was partially responsible for the death of 23-year-old Nohemi Gonzalez because YouTube’s recommendation system led users to recruitment videos for ISIS. Google defended itself by relying on Section 230, which provides immunity for providers of third-party content (like YouTube) from (i) actions arising out of illegal content posted by its users and (ii) actions arising out of content moderation by the provider. The plaintiffs argued that algorithm-generated recommendations (like the one that allegedly contributed to the death of Ms. Gonzalez) are outside of the scope of Section 230, differentiating between providers removing content (e.g. YouTube removing ISIS videos) and providers promoting illegal content (e.g. YouTube promoting ISIS videos via algorithms).

The United States District Court for the Northern District of California ruled in favor of Google on August 15, 2018; and on June 22, 2021, the United States Court of Appeals for the 9th Circuit upheld that decision. On October 3, 2022, the United States Supreme Court granted certiorari (agreeing to review the decision and opine on the scope of Section 230 as it applies to algorithmic recommendations) alongside *Twitter, Inc. v. Taamneh*, a parallel case involving Section 230 and Anti-Terrorism Act claims. This pair of cases represents the first time the United States Supreme Court will assess the protections of Section 230 in the context of algorithmic recommendations, and it will likely have major implications for BigTech, the internet and related industries. Particularly if the Supreme Court rules against Google in *Gonzalez*—Google, and other electronic content providers, may find themselves operating in a world where they could be held liable for promotion by their algorithms (which are currently major drivers of revenue for BigTech) of illegal, defamatory or otherwise objectionable content created by third parties. *Taamneh* and *Gonzalez* are both expected to be heard this winter.

[Twitter, Inc. v. Taamneh](#)—*Potential aiding and abetting liability of social media platform under US Anti-Terrorism Act* (cert. granted Oct. 3, 2022): This case stems from a mass murder in an ISIS-directed terrorist attack on a nightclub in Turkey. The US relatives of one of the victims brought an action against Twitter, Facebook and Google, alleging that they were liable under the Anti-Terrorism Act (ATA) for aiding and abetting terrorist acts. The ATA provides a basis for US nationals injured by acts of terrorism, or their families, to recover treble damages in civil claims against a person who “aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism.” The district court in *Taamneh* held that plaintiffs failed to plausibly allege two of the three requirements for aiding-and-abetting liability under the ATA, and so did not reach the argument that plaintiffs’ claims were barred under Section 230 of the Communications Decency Act. The Ninth Circuit reversed. In its petition for certiorari, Twitter’s presented questions ask whether social media companies (1) can be deemed to be “knowingly” providing substantial assistance for purposes of the ATA when they regularly work to prevent terrorist use of their services and (2) can be liable under the ATA even if their platforms were not used in the specific act of international terrorism at issue.

At issue in *Taamneh* is the scope of the ATA, not the scope of Section 230 immunity, which the Ninth Circuit declined to address because it had not been considered by the district court. Given the similarity of the claims with the *Gonzalez* litigation, however, the *Taamneh* litigants stipulated that if the Supreme Court denied the *Gonzalez* certiorari petition, then *Tamneeh* would be automatically dismissed. In other words, for plaintiffs to ultimately prevail in *Tamneeh*, they will have to get a favorable ruling from the Supreme Court on the ATA issues described above, and the Supreme Court will also have to rule in *Gonzalez* that Section 230 immunity does not shield the social media companies in that case. The *Taamneh* and *Gonzalez* pair of cases, which are both expected to be heard this winter by the Supreme Court, are ones to watch, as rulings against BigTech could open the floodgates for ATA and Section 230 claims against social media companies, resulting in a sea of change in the liability landscape for the social media industry.

FTC Developments

[FTC Exploring Rulemaking Targeting Fake Online Reviews](#): On October 20, 2022, the FTC issued an [Advance Notice of Proposed Rulemaking](#) relating to fake online reviews and other deceptive reviews and endorsements. The proposed rule would expand the FTC’s ability to target fake online reviews by giving it the ability to impose monetary fines. As noted in our September newsletter, there have been a number of FTC enforcement actions and private litigations targeting fake reviews.

[FTC hosted event on “Protecting Kids From Stealth Advertising in Digital Media”](#): On October 19, 2022, the FTC held a virtual event to analyze the ways in which children are targeted by stealth advertising and the effect such targeting has on them. The event included opening remarks from Lina Khan, Chair of the FTC, closing remarks by Serena Viswanathan, Associate Director, Division of Advertising Practices at the FTC, and panelists from a self-regulatory organization, academia, the medical profession, advocacy groups, and industry. During the event, Chair Khan warned social media companies that the FTC is considering taking action to protect children from “stealth” digital advertising that is “designed specifically to exploit insecurities for commercial gain.” Unboxing videos and memes were two common examples of stealth advertising discussed that influence children, whether they realize it or not.

Case Law Development

[Does 1-6 v. Reddit—CDA Section 230 Immunity](#): The Ninth Circuit in *Does 1-6 v. Reddit* issued an important ruling resolving a split among district courts within the circuit regarding the scope of an exception to CDA Section 230 immunity for civil claims based on violations of federal sex trafficking laws. The Section 230 exception, enacted as part of 2018’s Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), allows litigants to bring civil claims against “interactive computer services” for violation of 18 USC § 1595 “if the conduct underlying the claim constitutes a violation of [the criminal statute] section 1591.” District courts were split on whether this exception covered all claims that could be brought under Section 1595 or was limited to a narrower sub-category of claims that met the stricter requirements for criminal liability under Section 1591. Some courts have required plaintiffs to establish the elements of a criminal violation of Section 1591, i.e., that the defendant engaged in conduct that specifically furthered the sex trafficking, received a benefit causally connected to that conduct and had actual knowledge of the sex trafficking. Other courts have applied a civil standard derived from Section 1595, which requires only that the defendant knowingly received a benefit from participating in a venture that the defendant knew or should have known violated sex trafficking law.

The Ninth Circuit held that FOSTA's abrogation of Section 230 immunity for sex trafficking was limited to claims that met the more rigorous criminal standard of Section 1591. It held that Reddit's alleged receipt of advertising revenue on webpages that users had reported as containing child sexual abuse material could only establish acquiescence or "turning a blind eye" to wrongdoing, not actual participation in sex trafficking as required for liability under Section 1591. Furthermore, because Reddit did not actively participate in sex trafficking, the benefits it received from advertising were not sufficiently connected to sex trafficking to establish liability.

The Ninth Circuit's decision provides much needed clarity for interactive computer services regarding the scope of the FOSTA exception to Section 230 immunity.

[Washington State Attorney General seeks \\$25M penalty from Meta over election ads](#): Attorney General Bob Ferguson of Washington State announced on October 13 that he filed a motion seeking the maximum penalty of \$24.6 million against Facebook's parent company, Meta, over 822 alleged intentional violations of Washington's campaign finance transparency law. Washington's commercial advertiser law requires any company that provides political advertisements to disclose information such as the identity of the party sponsoring the ad, dates services were rendered and names of candidates supported and opposed. "We have penalties for a reason," Ferguson said. "Facebook is a repeat, intentional violator of the law. It's a sophisticated company. Instead of accepting responsibility and apologizing for its conduct, Facebook went to court to gut our campaign finance law in order to avoid accountability. If this case doesn't warrant a maximum penalty, what does?"

Healthcare

On September 28, 2022, the international and European self-regulatory bodies for the research-based pharmaceutical industry (IFPMA, International Federation of Pharmaceutical Manufacturers and Associations and EFPIA, European Federation of Pharmaceutical Industries and Associations) published a Note for Guidance to assist member companies with their use of social media and digital channels. See [Arnold & Porter's BioSlice Blog](#) for details.

Other Developments

[The White House's Blueprint for an AI Bill of Rights](#): As discussed in our [Advisory](#), on October 4, 2022, the White House Office of Science and Technology Policy published its Blueprint for an AI Bill of Rights. The Blueprint for an AI Bill of Rights is a nonbinding framework that sets forth five principles and several definitions that aim to guide the use and design of automated systems with the ultimate goal of protecting privacy and civil rights and liberties. This framework calls for digital regulation of AI, and includes five principles:

1. **Safe and Effective Systems:** Automated systems should be safe and effective. They should be evaluated independently and monitored regularly to identify and mitigate risks to safety and effectiveness. Results of evaluations, including how potential harms are being mitigated, should be "made public whenever possible."
 2. **Algorithmic Discrimination:** Automated systems should not "contribute to unjustified different treatment" or impacts that disfavor members of protected classes. Designers, developers and deployers should include proactive equity assessments in their design processes, use representative data sets, watch for proxies for protected characteristics, ensure accessibility for people with disabilities, and test for and mitigate disparities throughout the system's life cycle.
-

3. **Data Privacy:** Individuals should be protected from abusive data practices and have control over their data. Privacy engineering should be used to ensure automated systems include privacy by default. Automated systems' design, development and use should respect individuals' expectations about their data and the principle of data minimization, collecting only data strictly necessary for the specific context. OSTP stresses that consent should be only used where it can be appropriately and meaningfully provided, limited to specific use contexts and unconstrained by dark patterns; moreover, notice and requests for consent should be brief and understandable in plain language. Certain sensitive data (including data related to work, home, education, health, and finance) should be subject to additional privacy protection, including ethical review and use prohibitions.
4. **Notice and Explanation:** Operators of automated systems should inform people affected by their outputs when, how and why the system affected them. This principle applies even "when the automated system is not the sole input determining the outcome." Notices and explanations should be clear and timely and use plain language.
5. **Human Alternatives, Consideration and Fallback:** People should be able to opt out of decision-making by automated systems in favor of a human alternative, where appropriate. Automated decisions should be appealable to humans.

[Clearview AI \(a facial recognition company\), facing \\$20 million fine and ordered to delete biometric data in connection with allegations of noncompliance with GDPR by the French Privacy Authority.](#) Following similar sanctions imposed on Clearview in [Italy](#) and the [UK](#), the CNIL (France's data protection authority) imposed a financial penalty of 20 million euros and ordered the AI company to stop collecting and delete the images and biometric data of French citizens collected from Facebook, other social media and from scouring the web.

The fine comes after the company failed to address a notice in which the French data protection regulator urged Clearview to change its practices of collecting images and other data of French citizens in violation of the GDPR by scraping social media web sites. Additionally, according to CNIL, the company further violated the GDPR by not providing French citizens with the ability to access or erase their personal data.

[State court deals blow to apps using clickwrap—recent state court's decisions and legal tactics raise new concerns about the inclusion of arbitration terms.](#) In a recent split decision marking a departure from federal precedents, the Pennsylvania Superior Court invalidated an arbitration clause, arguing that the notice mobility company Uber gave to a customer who later sued the company was not substantial enough to show that the plaintiff had agreed to arbitrate her claims. Notably, the court based its decision on the alleged violation of the party's right to a jury trial recognized by the Pennsylvania Constitution and the argument that, in the context of internet contracts, a stricter standard should be applied when testing the validity of consumers' consent to waive a state constitutional right, such as the right to a jury trial. The Pennsylvania court's ruling could be the first of a progeny of decisions by the courts of those states where the right of jury trial is granted constitutional ranking and this type of ruling could ultimately trigger forum shopping strategies by the plaintiffs' bar.

While the Pennsylvania court's decision raises concerns about the enforceability of certain arbitration clauses embedded in the terms of use, a petition recently filed in the Northern District of Illinois by tens of thousands of consumers against tech giant Samsung exposes an emerging legal tactic and raises different type of concerns.

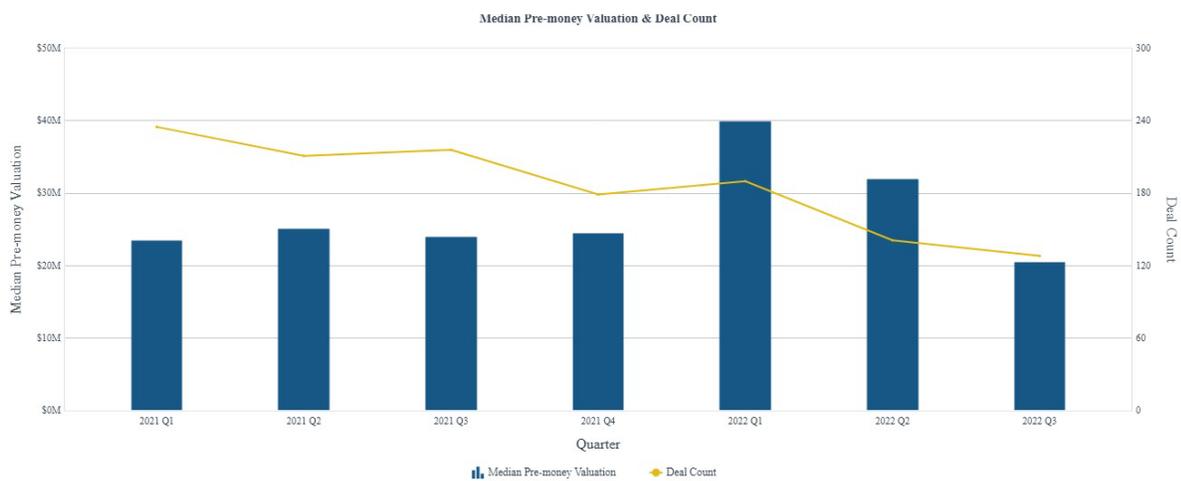
Nearly 50,000 users of Samsung Galaxy devices filed a [petition](#) and motion to compel arbitration alleging that Samsung violated the Illinois' Biometric Information Privacy Act by collecting and storing biometric data through the use of facial-recognition technology on the photos taken by petitioners with their smart phones. Given the high

number of users who are separately pursuing arbitration, Samsung faces millions of dollars in initial arbitration filing fees alone. The company has so far refused to pay such fees due to alleged deficiencies in the filings. This type of use of mass arbitration for alleged violations of privacy statutes (especially in light of its potential financial implications) is likely to be another factor that could reasonably prompt companies to reevaluate whether their terms of service should include mandatory arbitration clauses.

Markets

Based on data provided by PitchBook, both the median deal value and the deal count for venture investments in AdTech & MarTech in the US are trending down (see figure 1 below). The same is also happening for the US, Europe and Asia combined (see figure 2 below).

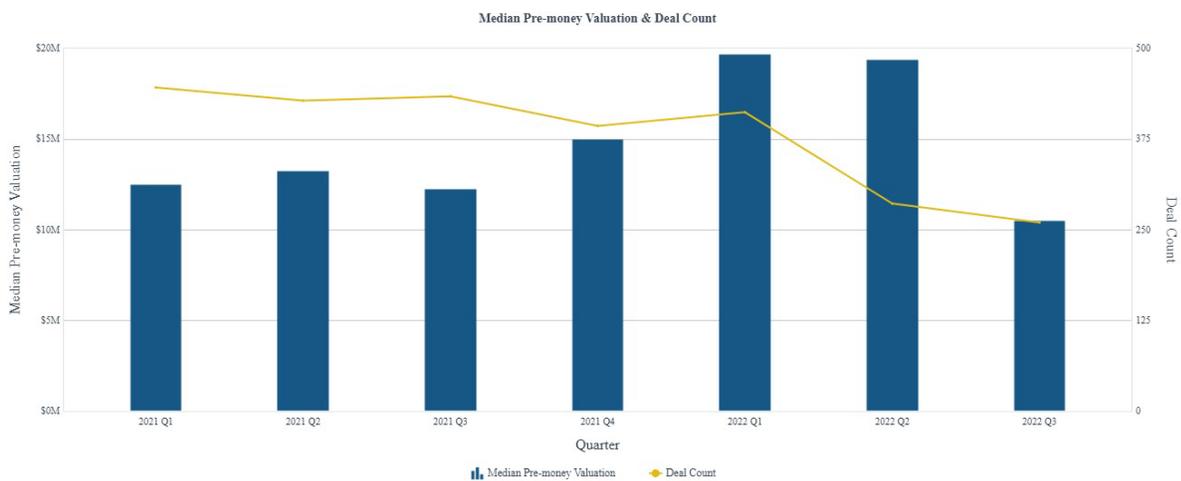
Annex A (US Only)



Created on 22-Oct-2022 | Source: PitchBook Data

PitchBook

Annex B (US, Europe, Asia)



Arnold & Porter Updates

- See our [alert](#) on the FTC’s recent lawsuit against Kochava Inc., an Idaho-based digital marketing and analytics company, alleging that the company violated Section 5 of the FTC Act by selling precise geolocation data that revealed customers’ visits to “sensitive locations” such as abortion clinics, places of worship and homeless shelters. As described in our August [newsletter](#), Kochava previously sued the FTC for allegedly improperly threatening to sue Kochava by mischaracterizing its business and practices. The lawsuit represents an expansion of the FTC’s prior focus on whether data collection was “deceptive,” to consideration of substantive limits on data collection, which in this case was to curb potentially dangerous collection and use of geolocation data.
- See our [Advisory](#) on the Whitehouse’s Blueprint for an AI Bill of Rights (also summarized above under “Other Developments”).

Please see Arnold & Porter’s [AdTech and Digital Media webpage](#) for additional publications summarizing developments in AdTech and Digital Media.

Questions/Comments?

Contact a member of our Editorial Committee



Nicholas O’Keefe

Partner
Silicon Valley



Tom A. Magnani

Partner
San Francisco



Jami Vibbert

Partner
New York



Nancy L. Perkins

Counsel
Washington, DC



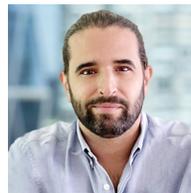
Isaac Chao

Senior Associate
San Francisco



Francesco DeProspero

Senior Associate
Silicon Valley



Joshua Blank

Senior Attorney
New York