BEACON POLICY ADVISORS
1701 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006
beaconpa.com

SPOTLIGHT REPORT

September 22, 2022

Every Step You Take, Every Move You Make: The Outlook for Data Privacy

What's Happening: The legislative and regulatory outlook for data privacy is heating up in Washington, DC and Sacramento, CA.

Why It Matters: It's a defining moment for the issue of data privacy on the federal and state levels. In the wake of the Cambridge Analytica scandal, Frances Haugen's whistleblowing, and other bad headlines for Big Tech in recent years, privacy has risen to the forefront for policymakers. **The American Data Privacy and Protection Act (ADPPA) is under consideration on Capitol Hill, though its prospects appear dim.** The ADPPA has encountered several obstacles in its path to passing Congress, including opposition from Californian officials, a lack of key support in the Senate, and a tight timeline in an election year. Nevertheless, the ADPPA is likely to remain relevant even after this Congress as it provides a benchmark for future congressional efforts to protect users' personal information online. Also under consideration in Congress this year is more narrowly tailored children's privacy legislation, but this too may not have a simple path to passage. **While the ADPPA is stalled in Congress, the Federal Trade Commission has begun weighing the proposal of new rules on "commercial surveillance." This rulemaking process could result in potentially wide-ranging standards and is perhaps the most likely comprehensive federal privacy reform to be enacted.** The ADPPA is the result of years of wrangling over thorny issues such as whether to allow Americans to sue for privacy violations and whether to preempt state laws, two questions that have historically divided the parties. If this opportunity to pass comprehensive privacy protections slips away, it's possible that Congress may not have another bite at the apple for a while. **This year, California has moved full steam ahead in toughening privacy protections, providing a model for policymakers elsewhere and potentially setting a de facto national standard for platforms that aim to simplify compliance by adopting California's rules for national operations.** Last week, Governor Gavin Newsom (D) signed the California Age-Appropriate Design Code Act into law, and the California Privacy Protection Agency (CPPA) continues work on a rulemaking process to implement the state's privacy laws.

What's Next: Both the CPPA and FTC rulemaking processes are ongoing. An update on the development of the CPPA rules is expected tomorrow when the

CPPA will hold a board meeting that will include discussion of rulemaking. The FTC's proposed rules are currently subject to a public comment period, which will end October 21st. **The contours of the data privacy debate in Congress next year will depend on the outcome of the midterm elections.** If Republicans take control of one or both chambers, as we expect them to do, passage of comprehensive data privacy protections may become more challenging. **In the absence of federal data privacy legislation, it's likely that state lawmakers will increasingly introduce their own bills once most 2023 state legislative sessions begin in January.** This would continue a trend from this year. According to the International Association of Privacy Professionals (IAPP), 25 states considered data privacy bills in 2022, and two passed them: Connecticut and Utah.

Congress

In June, we published a Spotlight Report with more details on the American Data Privacy and Protection Act. This month, we're focusing on the political dynamics surrounding the bill for the rest of this Congress and beyond. **Right now, the ADPPA's chance of passing Congress before year end looks weak, despite the landslide committee vote during the bill's July markup in the House. This assessment is due to three major reasons.**

1. ***Californian Concerns About Preemption***

Federal and state officials from California have expressed opposition to the ADPPA's preemption of their state's privacy laws, considered to be the toughest in the nation. This includes Newsom, who sent a letter to House Energy and Commerce Committee Chair Frank Pallone (D-NJ) advocating a carveout from federal preemption for California; Assembly Speaker Anthony Rendon, who sent a letter to House Speaker Nancy Pelosi (D-CA) opposing preemption; and the CPPA board, which voted at a special meeting in July to oppose the ADPPA. **California Democrats may not be alone in their concern about preemption of state laws.** Democratic attorneys general from Connecticut, Illinois, Maine, Massachusetts, Nevada, New Jersey, New Mexico, New York, and Washington joined California Attorney General Rob Bonta in calling on Congress to preserve state privacy laws. If the ADPPA passes, some privacy advocates fear that it would set a ceiling on data privacy protections at the state level, blocking more nimble state legislatures from passing new legislation as technology evolves. Notably, the two "no" votes in committee came from congresswomen representing California: Reps. Anna Eshoo (D-CA) and Nanette Barragán (D-CA).

Given the size of California in Democrats' House majority and the state's preeminent role within the party, the Golden State's ADPPA qualms are hard for Democratic leadership to ignore. Accordingly, the House Energy and Commerce Committee released an updated draft of the bill before the July markup. This apparently wasn't enough to satisfy Golden State critics of the ADPPA, who found a powerful ally earlier this month in another Californian: Pelosi. "With so much innovation happening in our state, it is imperative that California continues offering and enforcing the nation's strongest privacy rights," Pelosi said in a statement. "California's landmark privacy laws and the new kids

age-appropriate design bill, both of which received unanimous and bipartisan support in both chambers, must continue to protect Californians."

2. ***A Lack of Key Support in the Senate***

The chair of the Senate Commerce Committee, Maria Cantwell (D-WA), thus far has declined to back the ADPPA, and her support is crucial to the bill's chances of advancing in the upper chamber. In a July interview with Spokane, WA newspaper the Spokesman-Review, Cantwell didn't mince words in throwing cold water on the bill, whose approach to enforcement she deems insufficient. "The problem is it's taking the House a long time to come to reality about what strong enforcement looks like," Cantwell said. "If you're charitable, you call it ignorance. If you think that it's purposeful, it literally won't pass the House because they just won't meet the test of what a strong federal bill looks like." **In response to one question, Cantwell articulated her position on the ADPPA as "Don't take the bait on a weak bill."** The updated July draft of the bill reduced the wait time for the private right of action to kick in and further restricted forced arbitration, but Cantwell hasn't publicly changed her stance.

3. ***A Ticking Clock***

"In the days ahead, we will continue to work with Chairman Pallone to address California's concerns," Pelosi said in her September 1st statement, but the limited time remaining in Congress' legislative session this year will make that difficult. The political environment of the midterms precludes work on major legislation like the ADPPA before Election Day, and lawmakers will have their hands full with other priorities such as the must-pass National Defense Authorization Act, appropriations, and confirmation of judicial and executive branch nominees during the lame duck session, particularly if Senate control is set to change come the new year.

Future prospects for privacy legislation will be shaped by the outcome of the midterm elections. In our view, Republicans are likely to gain control of both chambers of Congress. Some future version of the ADPPA could potentially emerge from a GOP-controlled House, though there is no guarantee it would make it through a new farther right Republican majority. The bill passed out of the House Energy and Commerce Committee this summer by a vote of 53-2 with substantial GOP support, and the committee's ranking member, Rep. Cathy McMorris Rodgers (R-WA), who is likely to chair the panel next year, released a statement earlier this month reaffirming her support for the bill. The GOP focus on supposed anti-conservative bias by tech platforms has the potential to throw sand in the gears of negotiations, though.

Data privacy legislation would face lower chances in a GOP Senate, however. If Republicans retake the Senate majority, the Senate Commerce Committee ranking member, Roger Wicker (R-MS), is expected to take the chairmanship of the Armed Services Committee instead. On the basis of seniority, Senator Ted Cruz (R-TX) is next in line to be the top Republican on the Commerce Committee. The deeply conservative Cruz is unlikely to back data privacy reforms. If Democrats retain Senate control, any data privacy bill would need to earn Cantwell's support, and it's difficult to imagine a bill that could pass a GOP House and pass muster with Cantwell. **Regardless, any future data**

privacy bill is likely to look towards the ADPPA as a baseline, and the basic principles of this legislation may return in future proposals.

Children's Data Privacy

If or when it becomes clear that the ADDPA doesn't have the votes to pass this year, lawmakers could decide that they still want to get something done on data privacy and turn to children's privacy instead. Senate Ed Markey (D-MA), who sponsored a children's privacy bill this session, said as much in a July statement quoted by the Hill. "If we can't protect every American online right now, I'm calling on my colleagues in the Senate to at least step up to protect our children." Though Cantwell has not brought up the ADPPA for consideration, she did hold a markup of two bipartisan bills, the Children and Teens' Online Privacy Protection Act and the Kids Online Safety Act. **The political dynamics around children's online privacy have shifted since California passed the Age-Appropriate Design Code Act last month.** This bill introduces new requirements for platforms to protect children's privacy and safety on the internet. It could make passage of a federal bill on this subject more challenging, however, due to the classic issue of preemption. It's not clear whether federal children's privacy legislation would replace California's new law. Californians would likely oppose preemption, while others may want a single national standard for children's online privacy.

Data Privacy and the FTC

Last month, the FTC proposed a significant rulemaking on data privacy. In a press release, the agency announced that it was considering developing new rules on "harmful commercial surveillance and lax data security." The FTC defined "commercial surveillance" as the "business of collecting, analyzing, and profiting from information about people." **According to a fact sheet released by the FTC, some specific areas of interest for the agency include inadequate data security practices, the impact of commercial surveillance on children, consumer-unfriendly data collection practices, inaccurate and discriminatory effects of algorithms, and dark patterns.** If the FTC ultimately proposes rules that cover all of this ground, the agency's standards could have a major impact on Silicon Valley. In a statement, FTC Commissioner Alvaro Bedoya noted that in his view, the FTC's advance notice of proposed rulemaking (ANPR) on data privacy will not conflict with the ADPPR. "This ANPR will not interfere with that effort. I want to be clear: Should the ADPPA pass, I will not vote for any rule that overlaps with it. There are no grounds to point to this process as reason to delay passage of that legislation."

FTC Chair Lina Khan's public comments suggest that the FTC in its rulemaking could take a new, stricter approach to consent. In an April speech at the IAPP Global Privacy Summit, Khan said that she is "concerned that present market realities may render the 'notice and consent' paradigm outdated and insufficient" and "Going forward, I believe we should approach data privacy and security protections by considering substantive limits rather than just procedural protections." She reiterated this concern in a press release last month on the ANPR.

The proposed rulemaking came as data privacy has increasingly become a focus for the FTC in recent weeks and months. In remarks delivered at the National Advertising Division Annual Conference this week, Bedoya described privacy as "a basic, vital necessity" and emphasized the need not only to address data collection practices but also the use and processing of Americans' personal information. In July, President Biden in his executive order on abortion access called on the FTC "to protect consumers' privacy when seeking information about and provision of reproductive healthcare services." Soon after, the commission published a blog post focused on the enforcement of federal law regarding sensitive data, including location and health information. **"The Commission is committed to using the full scope of its legal authorities to protect consumers' privacy. We will vigorously enforce the law if we uncover illegal conduct that exploits Americans' location, health, or other sensitive data," said Kristin Cohen, acting associate director of the FTC Division of Privacy and Identity Protection.** She also highlighted deceptive data anonymization practices and misuse of consumer data as areas of interest for the FTC.

Not long after the rulemaking was announced, the FTC sued Kochava, a data broker, for selling sensitive geolocation data. The data in question related to people's visits to locations including reproductive health facilities, places of religious worship, shelters for people facing homelessness or domestic violence, and addiction treatment centers. In its case, the FTC argues that Kochava allowed its buyers to identify the specific users tied to certain data. **The agency's crackdown on Kochava suggests that any data privacy rules that emerge from the agency's rulemaking process could be strict.**

The FTC is accepting public comments on the proposed rules until October 21st. Final rules are not likely to be released before next year. The next release of the Biden administration's unified regulatory agenda, expected in December, may provide an update on the status of the rulemaking. **With the ADDPA looking unlikely to pass this year, the FTC rulemaking may be the more likely pathway for comprehensive federal data privacy protections to be enacted in the near future.**

Data Privacy in California

California has made progress in strengthening data privacy protections on the legislative and regulatory fronts this year. **Last week, Governor Newsom signed into law the bipartisan California Age-Appropriate Design Code Act.** Major components of the bill include high default privacy settings for children, mandatory Data Protection Impact Assessments for products used by children, and restrictions on the collection and use of children's personal data. Notably, the bill sets an age threshold of 18 years old, higher than the limit of 13 years old set by the federal Children's Online Privacy Protection Act (COPPA). **This bipartisan, widely supported bill could provide inspiration for other state lawmakers in red and blue states alike to pursue tightening rules on children's privacy in next year's legislative sessions.**

The Golden State's top privacy regulator, the California Privacy Protection Agency, is continuing apace with its first rulemaking implementing the state's privacy laws. The proposed rules released by the agency cover consumer rights for opt-out and requests to access or correct information, dark patterns, and the CPPA's enforcement powers. **The CPPA will hold a public board meeting tomorrow afternoon, and its ongoing rulemaking process is on the agenda.** CPPA Board Members Lydia de la Torre and J. Christopher Thompson are set to discuss "the course of action for [the] current rulemaking process." According to a slide deck released by the CPPA in advance of tomorrow's meeting, the agency's staff are currently going over input received from the public during the comment period this summer. After the next version of the initial rules formally proposed in July are released, there will be another public comment period. **The CPPA has not given an indication of when the rulemaking process will be complete.**

The CPPA faced a statutory deadline to finish rulemaking by July 1st, six months before the California Privacy Rights Act (CPRA) takes effect on January 1st, 2023. This deadline, however, was not met. In February, the CPPA executive director, Ashkan Soltani, said at a board meeting that the agency planned to finish rulemaking in the third or fourth quarter of this calendar year. Under Soltani's timeline, the formal rulemaking was slated to start in the second quarter and continue in the third quarter. The notice of proposed rulemaking was not ultimately released until July, though, suggesting that completion of the rules might slip later than estimated. **Tomorrow's meeting could offer greater clarity on the CPPA's timeline for completing this rulemaking. The next few months will likely be key for the agency as regulators seek to finalize rules in anticipation of the CPRA's implementation date.**

CFPB Regulation of Consumer Financial Data

The Consumer Financial Protection Bureau (CFPB) recently released a report entitled "The Convergence of Payments and Commerce: Implications For Consumers" as a precursor to additional reports, rulemakings, and likely enforcement actions as part of its attempt to prevent further monetization of consumer financial data and its use in commerce. **Investors with an interest in Big Tech's foray into the payment system; buy now, pay later (BNPL); and the impact of consumer finance on retailers should look for a proposal on control of personal financial data from section 1033 of the Dodd-Frank Act as well as further comments from Director Rohit Chopra on how the bureau intends to participate in the aforementioned FTC rulemaking on consumer data surveillance, particularly how he plans to enforce those rules as they apply to consumer finance companies.**

Additionally, at any time during these lengthy processes, there could also be an enforcement action against one or more of the largest players in these sectors with the bureau attempting to impose its rules on that company and others while the larger rulemakings play out in the background.

Past CFPB Actions

The rulemaking to implement section 1033 of the Dodd-Frank Act concerning personal financial data began in 2020 under the Trump administration. Since then, it has been amended in scope to serve as a vehicle for the bureau to create rules designed to undermine super apps and to help mitigate the entrance of Big Tech into consumer finance. The CFPB has also released an interpretive rule aimed at digital marketing companies to warn them of the risks of using consumer financial data in their work and that they may fall afoul of consumer protection and civil rights laws.

Embedded Commerce

The term embedded commerce is very broad and can mean anything from clicking on a QR code to using a link from a BNPL provider at checkout to being able to purchase a product while on an unrelated social media app with one click. **All of these elements are areas of concern for the CFPB not because the regulator is against convenience and an enhanced consumer experience, but because the bureau believes this type of commerce can put consumers at risk of making poor financial decisions, promotes the monetization of consumer data, skirts regulations based on product design, and for the largest companies, they can increase their power over consumers' financial and commercial lives.**

The bureau believes that the super apps of China, WeChat and Alipay, are not a desirable policy outcome and it is attempting to prevent such apps from being created and most importantly, from being successfully adopted, in the United States. The bureau's Payments and Commerce report claims that the United States already has what is termed "bank in an app" where a variety of financial, payment, and commerce functions can be accessed altogether, but the fear is that this grows or that one of the Big Tech companies that are currently mostly commerce or social media focused also are able to add a "bank in an app" so they would get closer to the ubiquity of a WeChat.

The report states that the **PayPal (PYPL)** wallet is the closest US equivalent to a super app. It writes, "PayPal's vision of the super app is a digital wallet that allows a consumer to aggregate their financial activity into a single app, including their credit and debit cards, investment and savings information, purchase information, and discounts and coupons derived from the consumer's previous purchase behavior." Apple Pay is another example of a financial services super app, with its digital wallet and recent announcements that it plans to offer BNPL-like credit to finance purchases from other retailers.

Embedded commerce also creates opportunities for merchants to collect and sell transaction data without consumer awareness or acceptance and this can be monetized as well as used to market certain products and services (or not) in a discriminatory or risky manner. Additionally, as Big Tech and other large players enter into this space, a concentrated market could result in smaller merchants having to pay excessive fees to the larger payment or super app companies, which has already been shown to happen with existing payment networks (Visa, Mastercard, American Express, etc.) increasing their swipe fees for merchants.

Section 1033 Rulemaking

The CFPB has not yet published extensive information on what will be in the bureau's consumer financial data rulemaking, but Director Chopra has spoken at length about this topic. The key points for investors to consider are that the rulemaking is meant to give consumers "power" over their data and that it can be standardized and ported between providers with permission of the consumer.

It is also meant to prevent selling and monetization of that data in what Chopra calls an "underworld" by consumer finance companies and retailers. In the recent report on Payments and Commerce, the bureau describes this phenomenon: "Increasingly, many firms are moving from seeing their customer's value as generating revenue from using that company's financial products, to the customer as a source of behavioral and financial data to be leveraged and potentially sold to create an additional revenue stream." The mandate for portability is meant to ensure that one single firm cannot hold a monopoly over a consumer's data and it can also be controlled by the consumer.

The Payments and Commerce report goes on to state: "As consumers interact online, they leave a path of behaviors that can readily be converted into a digital version of their analog lives and life choices. Social media companies leverage this wealth of information to provide users with a richer and more valuable experience. However, they can also use this information to generate incremental revenue by targeting ads and offers for the benefit of third parties or they may even sell consumers' information to other organizations without their explicit consent…Given the prevalence of machine learning and algorithmic optimization in modern business, companies increasingly have the capability to leverage consumer financial data to achieve outcomes that may take significant financial advantage of consumers that may result from automated decision-making with limited transparency."

We expect that a Small Business Regulatory Enforcement Fairness Act (SBREFA) hearing will be scheduled and occur this fall and that will outline what the bureau is likely to propose in a formal proposed rule either by year end or in early 2023.

Digital Surveillance and BNPL Report

Immediately after issuing the report on Commerce and Payments, the bureau issued its long-awaited report on BNPL companies. In his remarks about that report, Chopra takes great pains to detail how he believes most BNPL companies are building their businesses around what the bureau calls "digital surveillance."

Chopra says: "In some ways, these firms aren't just lenders, they are also advertisers and virtual mall operators. Because they are deeply embedded as a payment mechanism for e-commerce, Buy Now, Pay Later lenders can gather extraordinarily detailed information about your purchase behavior, in a way traditional cards cannot. Buy Now, Pay Later has mimicked parts of Big Tech's surveillance model to harvest and monetize data in ways that banks and credit unions have typically avoided. Many of these firms have created their

own gateways and digital, app-driven marketplaces, powered by personalized behavioral data, to lure their users into buying more products financed through a Buy Now, Pay Later loan. Increasingly, Buy Now, Pay Later firms can leverage data and user interface design to gamify shopping and lending, promoting repeat usage and further revenue generation."

The potential for these companies to use digital dark patterns and pricing based on consumer behavior is too risky for Chopra and we expect that he will use rulemaking authority to squelch these practices for any company that offers credit as a consumer finance company. He cites the fact that in the US there is a long history of a separation between commerce and banking and we expect that he will attempt to return to the status quo ante.

Specifically, Chopra has tasked bureau staff with "identify[ing] the data surveillance practices that Buy Now, Pay Later providers engage in that may need to be curtailed." He goes on to mention demographic, transactional, and behavioral data that is used outside of a lending decision and links these practices to wider concerns with Big Tech companies. **Chopra then goes even further and cites the ongoing FTC rule on commercial surveillance and says the bureau will participate in drafting this rule and will be responsible for enforcing it for financial services firms — effectively using the legal authority of another agency to curb the business practices of a whole industry.**

This announcement means that investors with an interest in BNPL should also pay close attention to the FTC rulemaking on commercial surveillance that was released in August, as it will have a significant impact on the future lines of business that BNPL companies can conduct.

Based on this report, it appears that the BNPL sector and its partner retailers have reached their high-water mark and multiple significant changes will be coming for all of its practices and lines of business in the near future, particularly those that rely on a consumer's financial data.