The Next Move

Regulatory and policy developments in tech — December 2023

CFPB proposal targets digital wallet and payment apps

By Jim Russell, Jacob Sciandra, Vivek Parikh, David Durovy

2

California advances prescriptive cyber audit rules

By Joe Nocera, Robert Donovan, Jocelyn Aqua, Matt Gorham

6

FCC pushes to restore net neutrality

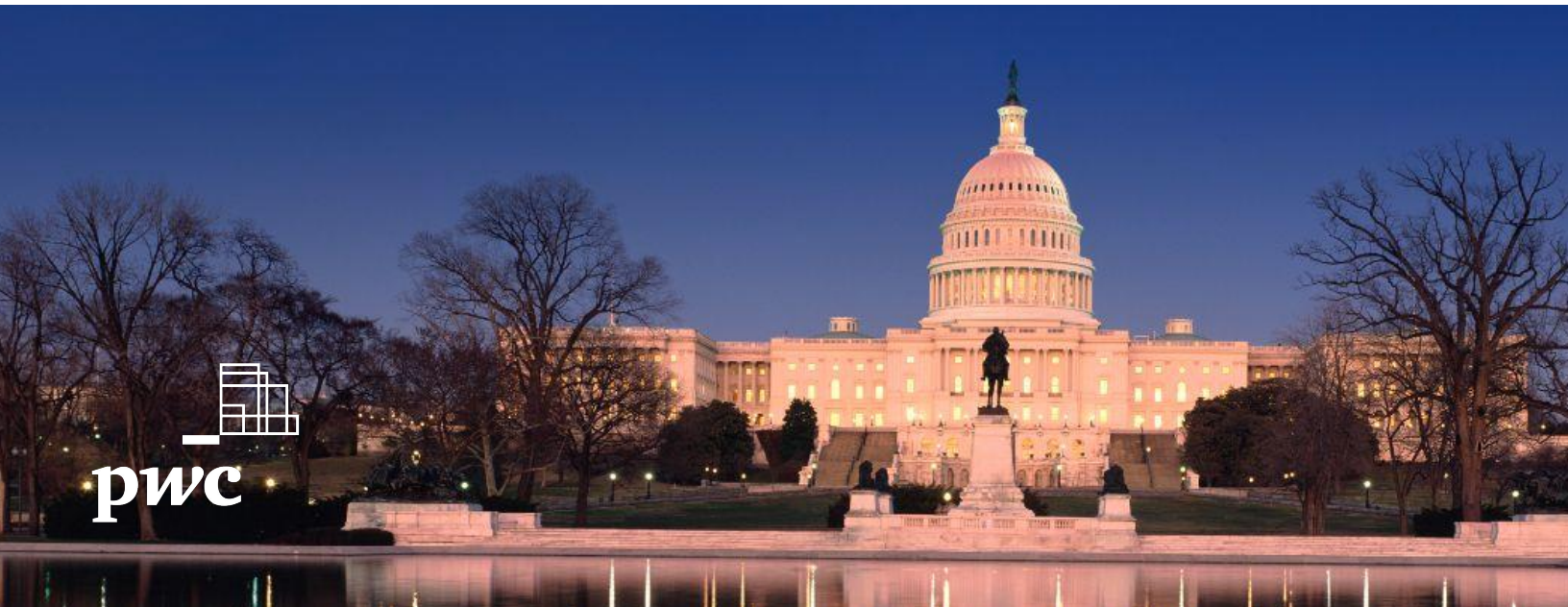
By Dan Hays, Chris Isaac, Jocelyn Aqua

10

On our radar:

EU policymakers agree on landmark AI framework

14



CFPB proposal targets digital wallet and payment apps

By Jim Russell, Jacob Sciandra, Vivek Parikh, David Durovy

The issue

The Consumer Financial Protection Bureau (CFPB) recently proposed a rule that would give the agency direct supervisory authority over large, nonbank participants in the digital payments market. The comment period is short, with the current deadline set at January 8, 2024.

Digital wallets and payment apps continue to grow in popularity, driven largely by Big Tech and other large technology firms that operate outside of CFPB supervision. These payment apps now rival traditional payment methods — credit cards and debit cards — in e-commerce volume. They've also gained a large share of in-person retail spending. At the same time, the CFPB notes, complaints about these apps and the companies that run them have grown in recent years.

The proposed rule would require these companies to play by the same rules as banks and credit unions, promoting a more competitive playing field. It would also allow the agency to monitor for new risks as companies increasingly offer funds transfer and wallet services through digital payment apps.

Affected companies should take this proposal seriously. It would impose a substantial compliance challenge that many companies outside of financial services have never experienced. Moreover, the proposal's reach may be broader than advertised, potentially extending beyond large tech companies to include retailers — an uncertainty that calls for immediate attention.

The regulator's take

Consumer use of digital payment apps and wallets is climbing steadily. Today, 76% of Americans have used at least one of four well-known P2P payment apps, and nonbank payment apps have become the most common way individual consumers send and receive money between friends and family.

Still, federal oversight of the companies behind these products is fragmented, and many are not subject to direct CFPB supervision. The proposal would change that by defining a market for "general-use digital consumer payment applications" over which the agency would have supervisory authority for larger participants. The proposed market definition includes providers of "digital wallets," "payment apps," "funds transfer apps," "person to person payment" apps and "P2P" apps to other persons for personal, family or household purposes.

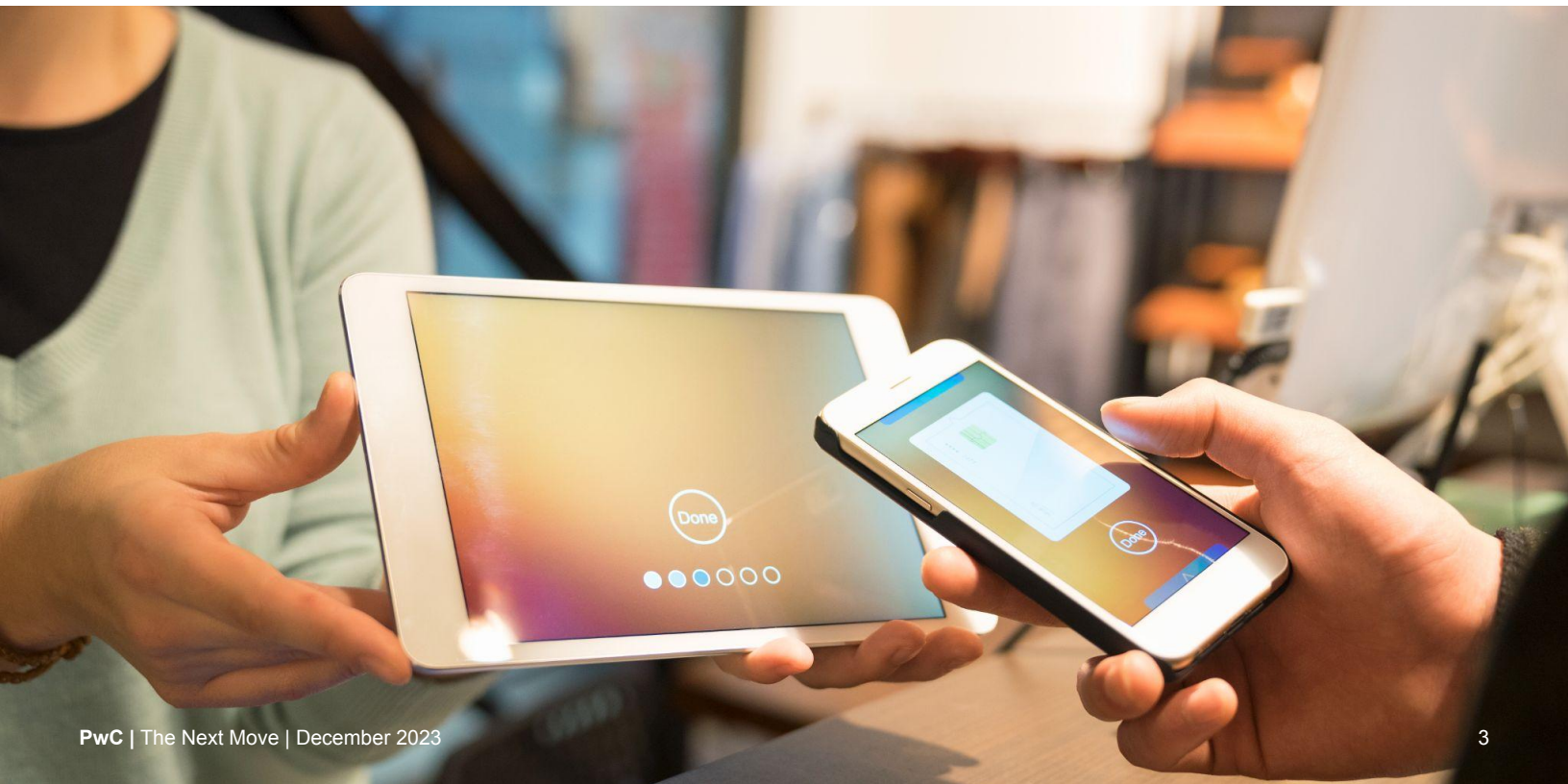
Digital assets would be covered. The proposal's definition of "funds" specifically includes crypto currencies and other digital assets. Similarly, the definition of "wallet functionality" can take the form of encrypted or tokenized data.

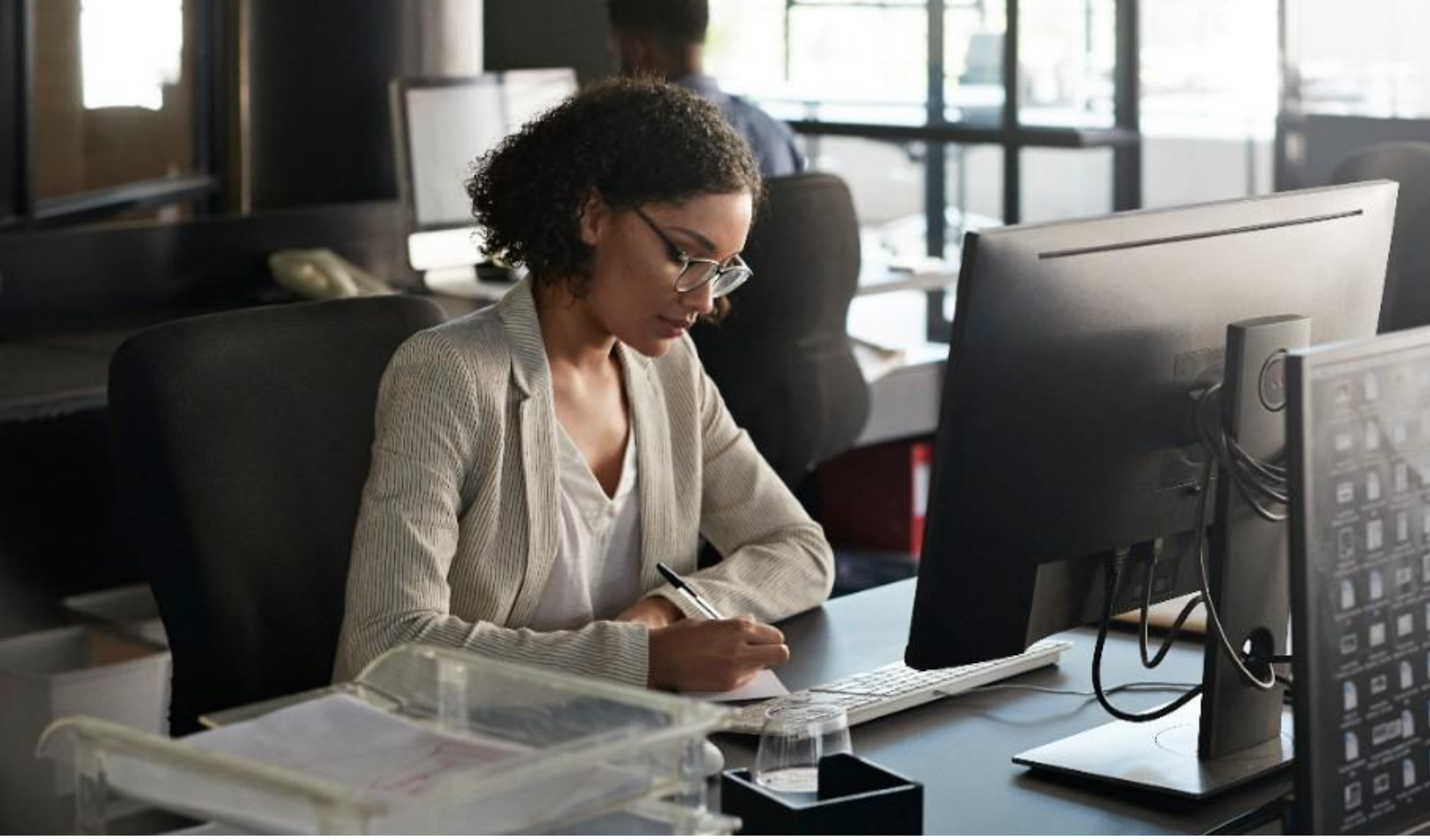
Expanded oversight powers. The proposed rule would give the CFPB additional oversight powers, including the ability to conduct examinations under the CFPA's prohibition against unfair, deceptive, and abusive acts and practices (UDAAP), the privacy provisions of the Gramm-Leach-Bliley Act and the Electronic Funds Transfer Act. The proposed rule would be the sixth in a series of CFPB rulemakings to define larger participants offering financial products and services that play a substantial role in the everyday lives of consumers.

The agency says that the proposed rule would affect 17 companies representing about 88% of known digital consumer payment transactions. If adopted, the proposed rule aims to confirm that these nonbank financial companies — specifically larger companies handling more than five million transactions per year — adhere to the same rules as large banks, credit unions and other financial institutions already supervised by the CFPB.

But perhaps the most significant impact on the digital payments industry is the insight that the CFPB would gain into the activities of larger market participants. Areas where the agency has signaled interest include the ways consumer financial data and behavior are used together and how payments are embedded in social media feeds.

This proposal comes directly after another proposed rule from the CFPB regulating "Personal Financial Data Rights," giving consumers the right to access and share their financial information between banks and other financial entities. Together, these rules could lay the foundation for the CFPB to play a larger role in regulating the intersection of digital payments and data.





Retailers could be affected, too. Big Tech may be at the center, but the rule has the potential to impact other companies, particularly in the retailer and merchant spaces.

For example, if the rule passes, nationwide grocery stores with embedded payment credentials in a proprietary app could become subject to CFPB oversight. But considering the thousands of end nodes and employees that stand to be affected by a UDAAP consideration, the compliance intricacies could snowball and become unmanageable. However, for some companies, the proposed rule could help level the playing field, specifically between nonbanks and depository institutions.

While any potential designation would be a long way away and would follow extensive communication with regulators, recent guidance on the nonbank designation process means that all large and interconnected firms should be vigilant of the potential to become subject to the same capital, liquidity and risk management requirements as systemically important banks.

Exclusions apply. The proposed rule does not apply to nonbanks (and affiliated companies) with an annual volume of fewer than five million payment transactions in a year. Also excluded are small businesses as defined by the Small Business Administration, international money transfers, exchanges of one type of funds for another (such as foreign exchange or exchanging crypto assets) and transfers to consumers outside the United States.

In addition, a credit card transaction would not be included if it does not rely on a “digital application.” If the credit card is used as part of a digital wallet, it would be included in the market definition.

Short timeline for comments and compliance. Comments must be received on or before January 8, 2024. Additionally, the proposed effective date of the final rule is 30 days after its publication in the Federal Register, giving companies the shortest amount of time allowable under the Administrative Procedure Act to demonstrate compliance.

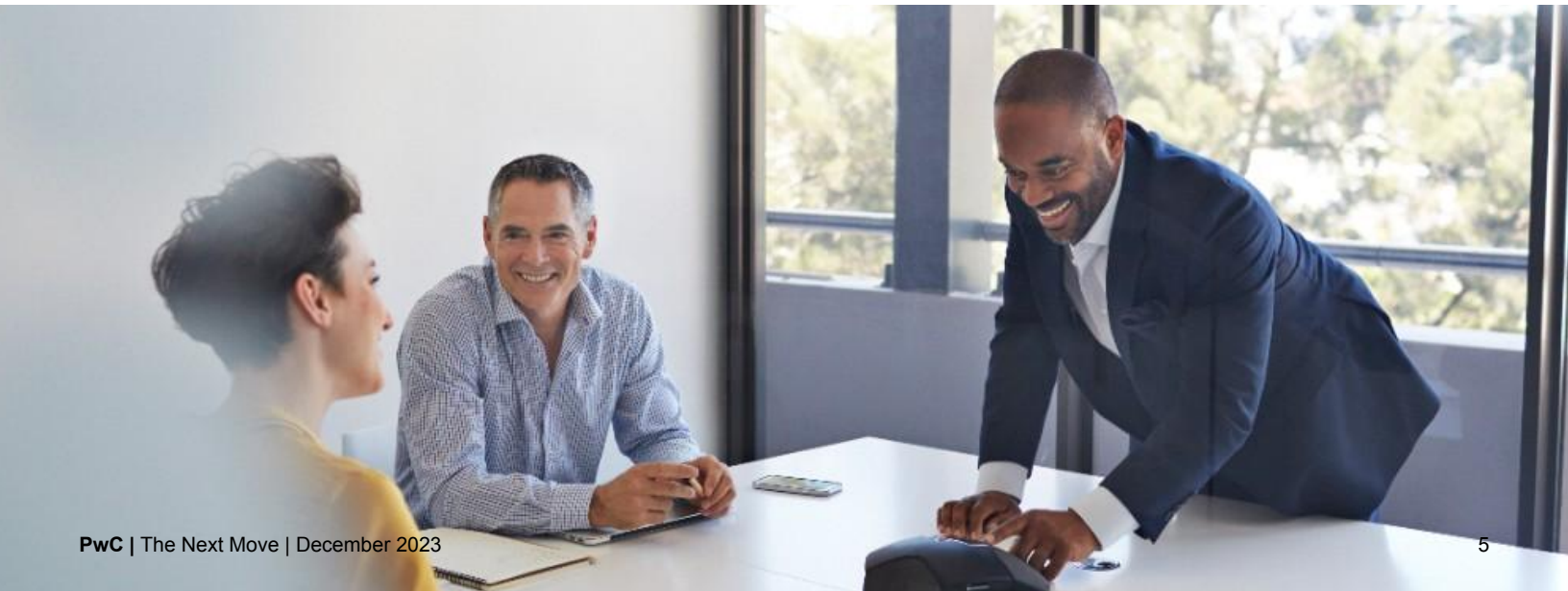
Your next move

This proposal is an aggressive move that poses a heavy compliance lift for tech companies and, possibly, retailers — many of whom lack the infrastructure, controls and capabilities required for examinations. While some have been under “indirect supervision” through their chartered financial services partners, direct supervision will introduce a new level of scrutiny that these companies aren’t accustomed to.

Prepare by taking the following steps.

- **Assess the proposal’s applicability**. Examine the proposal and its many exceptions to determine whether your company is in scope. Don’t assume this is strictly a Big Tech rule. Understand the proposal’s requirements, ambiguities and potential pitfalls.
- **Plan for regulatory exposure**. Assume the rule will be adopted in some form and make plans to develop the necessary infrastructure and capabilities. Train and hire personnel with requisite skills to prepare for potential examinations. Maintain a complete inventory of relevant regulations and understand how those regulations apply. Confirm that you have sufficient controls and other risk governance practices (e.g., risk assessments, testing and monitoring programs, training) in place. Pay close attention to the CFPB’s increasing expectations and scrutiny in areas including the use of consumer data, “gates and toll booths” for access to systems, fee structures, complaint management and terms in take-it-or-leave-it agreements.
- **Anticipate the cost**. The estimated cost of each exam is $25,000 under the CFPB’s cost-benefit analysis, but the actual cost could be far higher. What type of infrastructure, processes, staff and training will you need to maintain compliance?
- **Engage with regulators.** Work with your compliance and legal teams to develop a point of view on the proposal. Engage more broadly with the CFPB staff and industry groups to inform the rulemaking effort of your organization’s needs and concerns.

The implications of this rule cannot be downplayed. The CFPB recently expanded its enforcement and supervision staff, which is a good indication of what’s likely to come. Regardless of any changes to a final rule or legal obstacles to its implementation, scrutiny of nonbank payments firms is not going away. Preparing for a final rule now will go a long way toward meeting increased expectations in the future.



California advances prescriptive cyber audit rules

By Joe Nocera, Robert Donovan, Jocelyn Aqua, Matt Gorham

The issue

The California Privacy Protection Agency (CPPA) will move forward with its draft cybersecurity audit rules. At a December 8, 2023, meeting, the agency's board agreed to direct staff to prepare the audit rules for advancement to formal rulemaking, authorizing them to make further changes based on input from the meeting and elsewhere.

In contrast to other state regulators such as the New York State Department of Financial Services (NYSDFS) — which rely on certification to the regulator — the CPPA is placing the emphasis on accountability through audit reporting to the company.

Acting under the agency's statutory mandate, the CPPA draft rules would require businesses whose processing of consumers' personal information "presents a significant risk to consumers' privacy or security" to perform a thorough, independent cybersecurity audit on an annual basis. They would define broadly the businesses subject to the audit requirement; set strict standards for audit thoroughness, independence and certification; and enumerate a long list of safeguards and program components in scope.

While still only a draft, the text under consideration received the CPPA board's general approval and is a strong indicator of the agency's leanings as it heads into formal rulemaking. Affected companies should understand and prepare for the potentially challenging audit requirements to come.

The regulator's take

Mirroring the authorizing statute, the CPPA audit requirement would apply to every business whose processing of personal information presents significant risk to consumer security. The draft rules define this group to include any business that derives 50 percent or more of its annual revenues from selling or sharing consumer personal information. Also included are businesses with annual gross revenues exceeding $25 million that process certain amounts of personal information, sensitive information or information about children under age 16.

These definitions and thresholds could potentially apply to a substantial number of data brokers, credit reporting agencies, marketing companies and big tech companies.

Independence and certification. Audits would have to be completed “using a qualified, objective, independent professional” auditor that’s either internal or external to the company. The auditor must “exercise objective and impartial judgment on all issues” without influence by the business and without participating in activities that may compromise or appear to compromise the auditor's independence. The auditor can’t, for example, participate in business activities that the auditor may assess in the current or future cyber audits, including developing procedures, preparing business documents, making recommendations regarding the cyber program, or implementing or maintaining the cyber program.

If a company uses an internal auditor, the auditor would have to report directly to the board or other governing body, not to management that has direct responsibility for the program.

The audit would have to include a signed, dated statement by a board member or, if no board or equivalent body exists, the highest-ranking executive responsible for the cybersecurity program. The statement must certify that the company has not attempted to influence the auditor and that the signatory has reviewed and understands the audit findings.

Scope of audit. The audit must assess and document how the cyber program protects personal information from unauthorized access, destruction, use, modification or disclosure, and how it protects against unauthorized activity that could result in the loss of availability of personal information. It must also assess and document with specificity the company's establishment, implementation and maintenance of its program, including the related written documentation.

The draft rules include a long list of program components that the audit would have to cover. For any that are not applicable, the company would have to address or "document and explain why the component is not necessary." Examples include:

- Multifactor authentication
- Encryption of personal information, at rest and in transit
- Zero trust architecture
- Account management and access controls
- Vulnerability scans, penetration testing, and vulnerability disclosure and reporting
- Audit log management
- Segmentation of an information system
- Cybersecurity awareness, education and training
- Oversight of service providers, contractors and third parties
- Retention schedules and proper disposal of personal information no longer required to be retained
- Incident response management
- Business continuity and disaster recovery plans, including data recovery capabilities and backups

For each component, the audit would have to assess and document its effectiveness, describe any gaps or weaknesses and document the company's plan to address those gaps or weaknesses. Contrast this with the New York rules, which require audits but based on the company's risk assessment.

If the company has already completed an audit that satisfies these requirements, it would not have to undertake a duplicative audit. It would, however, have to explain how the audit meets the CPPA requirements or, in the case of partial compliance, the company must supplement the audit with additional information required to fill any gaps.

Notice of compliance. Similar to the NYSDFS rules, each company required to complete an audit would have to submit to the CPPA every calendar year either:

1. A certification that it complied with the CPPA requirements, or
2. An acknowledgement of noncompliance that identifies all sections not complied with and the extent of noncompliance and includes a remediation timeline or confirmation that remediation has been completed.

The certification or acknowledgment would have to be signed and dated by a board member, or if no board or equivalent body exists, the highest-ranking executive responsible for oversight of cyber-audit compliance. It also would have to include a statement certifying that the signatory has reviewed and understands the audit findings.

Your next move

While formal rulemaking has yet to get underway, the CPPA's draft rules suggest companies could face a substantial compliance responsibility. As the process unfolds, consider what's already required under California Civil Code Section 1798.81.5 as a guiding principle. That provision requires companies to "implement and maintain *reasonable security procedures and practices* ... to protect the personal information from unauthorized access, destruction, use, modification, or disclosure" (emphasis added).

With that context in mind, take the following steps.

1. **Assess your exposure.** Determine whether the draft audit rules apply to your organization. If so, identify any misalignment between your current program and the CPPA draft requirements. Assess your compliance risk
2. **Stay informed and engaged.** Closely monitor the rulemaking process as it progresses. Consider submitting comments to the CPPA to address your concerns and resolve potential ambiguities.
3. **Align your program to industry standard.** Perform a risk assessment of your current program. Develop a plan to align your program to an industry cybersecurity standard such as the NIST Cybersecurity Framework for instance, and then tailor your capabilities accordingly. If your company operates in multiple jurisdictions, determine which ones set the highest bar for each program component and decide what's necessary for compliance.

FCC pushes to restore net neutrality

By Dan Hays, Chris Isaac, Jocelyn Aqua

The issue

The Federal Communications Commission released a proposed rule on October 20, 2023, titled *Safeguarding and Securing the Open Internet*. The proposal seeks to reestablish the framework the FCC adopted in 2015 — but abandoned in 2018 — to classify broadband internet access service (BIAS) as a telecommunications service and empower the agency to safeguard the open internet, otherwise known as net neutrality. Net neutrality refers to the principle that all internet traffic should be treated equally, without discrimination or preferential treatment.

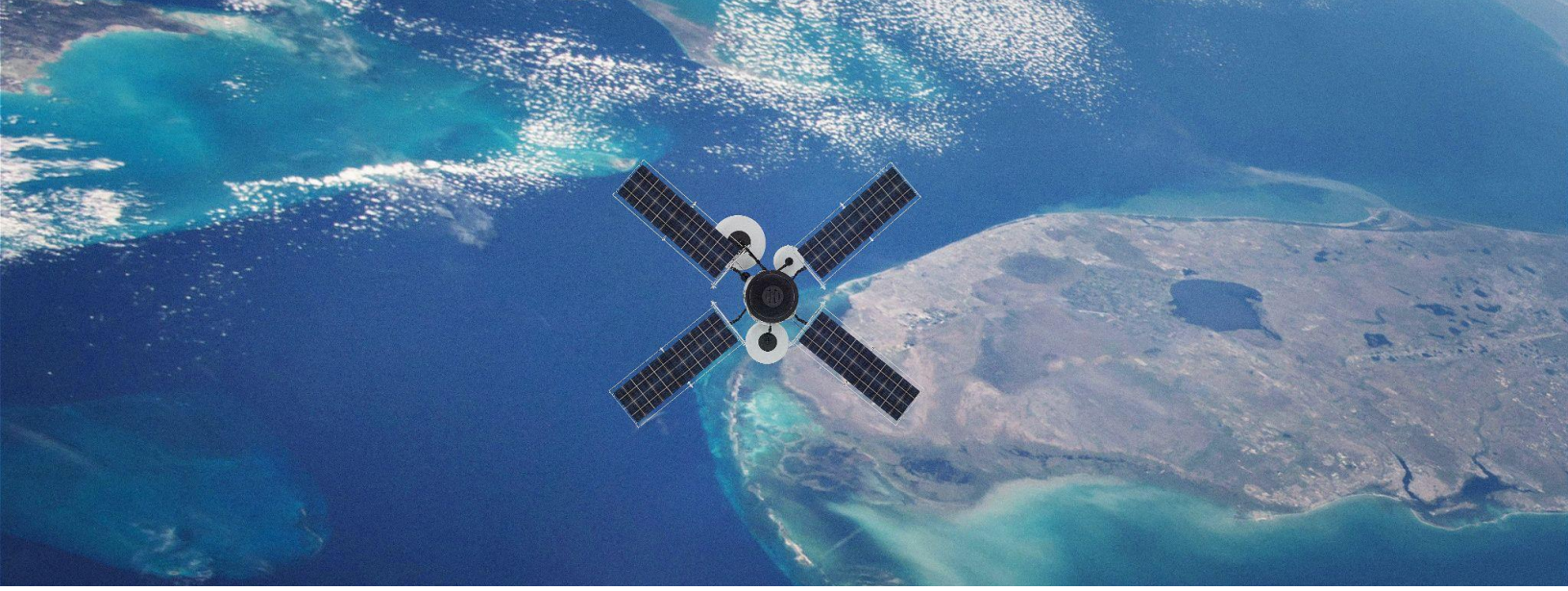
The proposal has sparked intense debates among telecommunication carriers and internet service providers (ISPs). Although it seeks to create a fair and open internet, the initiative carries the potential for major operational, budgetary and infrastructure consequences, and it raises the prospect of pricing regulation. Moreover, many in the industry argue that net neutrality solves a problem that doesn't exist, with no significant examples of net neutrality violations to speak of.

Affected companies should pay close attention and consider, among other things, how this might affect their capital spending plans.

The regulator's take

As explained in the FCC's press release, "There is currently no expert agency ensuring that the internet is fast, open, and fair." This proposal represents the first steps toward reaffirming rules that would treat broadband internet service as an essential service for everyday life.

As work, healthcare, education and commerce have moved increasingly online, the FCC reasoned, "no US household or business should need to function without reliable internet service." The proposal, the agency believes, would reaffirm that broadband service is on par with other essential services like water, electricity and phone service.



Policy objectives. The proposal would implement conduct rules for ISPs to establish a uniform, national approach for safeguarding internet openness. It also aims to bolster national security by deterring ISPs from contracting with foreign companies that pose a national security threat or are owned, controlled or subject to the jurisdiction of foreign adversaries. Public safety is another goal to be achieved, for example, by empowering the FCC to support first responders and other public safety officials in their use of broadband for emergency communications, accessing databases and information gathering.

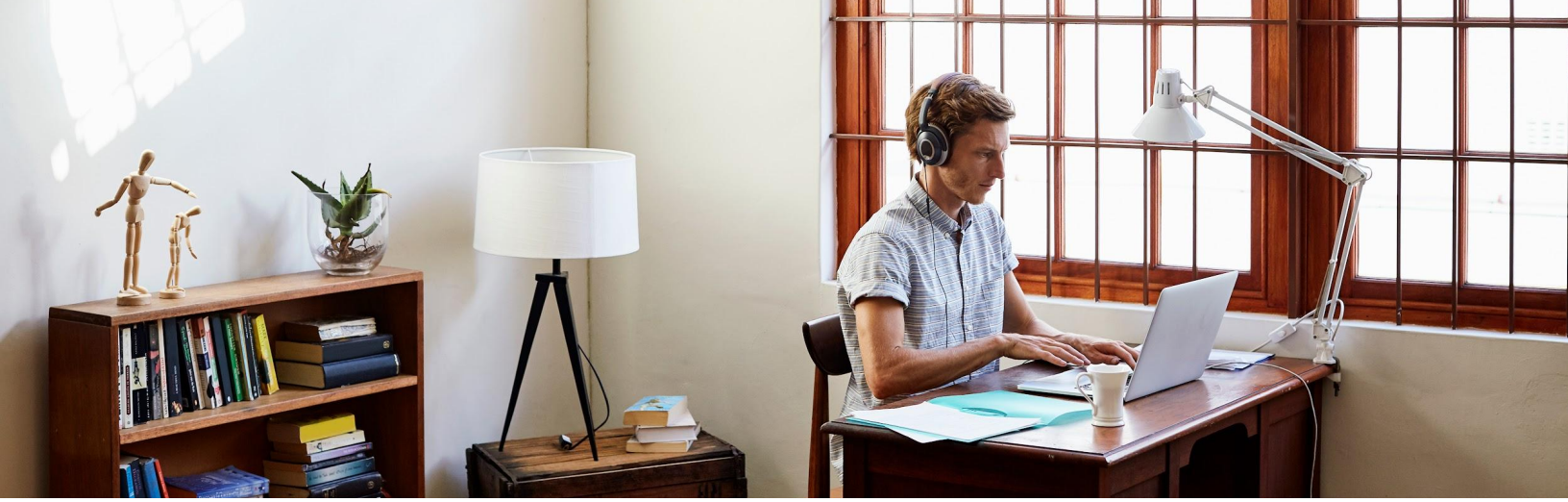
Who's affected? By reclassifying BIAS as a telecommunications service under Title II of the Communications Act and reclassifying mobile BIAS as a commercial mobile service, the proposal would cover both fixed and mobile broadband providers. Specific stakeholders affected include:

- ISPs: Operators of terrestrial fiber, coaxial cable, twisted pair copper and fixed wireless operators, as well as cellular mobile network and satellite operators, would face conduct-based standards that prohibit practices such as blocking, throttling and engaging in paid or affiliated prioritization arrangements. These rules aim to establish a level playing field and prevent practices that harm consumers, competition and public safety. The FCC is seeking comments on steps it can take to reduce the economic impact on small entities and may implement alternative rules that could lessen regulatory burdens for small businesses.
- Consumers and edge providers: General conduct standards (adopted in the 2015 Open Internet Order) would protect consumer access to the open internet and prevent practices that could limit their ability to access online content and services. This standard prohibits practices that cause unreasonable interference or unreasonable disadvantage to consumers or edge providers (companies or services that deliver content or services via the internet such as search engines and bloggers). The proposal provides a framework for preventing harmful practices and behaviors and would be enforced on a case-by-case basis. The FCC has also launched the Privacy and Data Protection Task Force to address consumer privacy concerns in the context of broadband.
- Platforms and hyperscalers: Large online platforms and hyperscalers may be the most affected and, in some cases, may benefit the most from this effort. If implemented, the proposal would prevent ISPs from charging online platforms and hyperscalers extra fees to prioritize (or not deprioritize) their traffic. It also raises the specter that startup applications and services in the BIAS market will be able to compete on par with larger ISPs, further driving down costs for platforms and hyperscalers.

Price regulation concerns. Reclassifying broadband as a telecommunication service would subject broadband services to all the rules and regulations of the 1934 Communications Act and potential associated FCC action. Though the act requires pricing to be “just and reasonable,” the FCC has assured the industry that this will not lead to price regulation. Even so, questions remain about the potential for price regulation. For example, does Title II reclassification empower the FCC to take enforcement action where pricing regulation is a condition of government broadband funding like BEAD?

Privacy and data protection focus. Reclassification of BIAS as a telecommunications service would also support the FCC's efforts to protect consumer privacy and data security. The agency believes that "consumers may not fully comprehend — and therefore may not be able to meaningfully consent to — ISPs' collection, processing, and disclosure of customer information, including potentially through the use of artificial intelligence models." It also worries that ISPs may not have sufficient technical, physical and procedural safeguards to protect their customers' data. Further, the FCC seeks comment on whether reclassification can strengthen its authority to support consumer privacy by combating illegal robocalls and robotexts.

On these issues, the agency recently adopted changes to its data breach notification rules — the first update in 16 years — to ensure that providers of telecommunications, interconnected Voice over Internet Protocol (VoIP) and telecommunications relay services (TRS) adequately safeguard sensitive customer information. It also issued a notice of inquiry to understand the implications of AI technologies to protect consumers from robotexts and calls. And it launched the first-ever enforcement partnerships with state attorneys general from Connecticut, Illinois, New York and Pennsylvania to share expertise, resources and coordinated efforts in conducting privacy, data protection and cybersecurity-related investigations.



Your next move

Affected companies, particularly ISPs, should take steps to prepare for potential changes in the regulatory landscape.

1. **Assess your exposure.** Conduct a thorough risk assessment of how the proposed rule might affect your business model and revenue streams. Identify potential risks and opportunities and the impacts on your investment and operational costs.

2. **Revisit capital spending plans.** For telecommunications carriers specifically, look at the impact on your return on capital — and the flow of capital — into the fiber market. Also consider the implications of universal service and how "carrier of last resort" obligations might impact profitability — and your customer base. This includes BEAD funding and the conditions that could be attached to it, such as complying with net neutrality rules and providing access to underserved areas.

   Net neutrality regulations may hinder the deployment of 5G and the offering of differentiated, low latency services. The impact of the proposed rules will depend on how exceptions for reasonable traffic management and specialized services are interpreted. A broad interpretation could accommodate new business models needed for 5G, while a narrow interpretation could restrict innovation and investment.

3. **Prioritize transparency.** Evaluate your network management practices. Consider implementing measures that provide consumers with clear information about how their internet traffic is treated and any potential limitations or restrictions.

4. **Upgrade your privacy and data security practices.** Renewed FCC scrutiny in this area may warrant strengthening your program capabilities and resilience. Understand your current-state practices for data management, cybersecurity and privacy compliance, the potential gaps and risks, and develop a remediation plan.

5. **Stay informed and engaged.** Closely monitor the rulemaking process and stay current on any developments, including congressional or legal challenges, so you can adjust investment and pricing strategies, as well as overall operations, accordingly.

On our radar

Noteworthy policy and regulatory developments that we're monitoring

By Rohan Sen, Jennifer Kosar, Jocelyn Aqua

EU policymakers agree on landmark AI framework

On December 8, 2023, the EU Council, European Parliament and European Commission reached a political agreement on the EU AI Act, a sweeping legal framework for the development and use of AI. This followed significant debate and eleventh-hour negotiations over concerns raised by the German, French and Italian governments about fostering innovation and protecting law enforcement needs. Although the final text is not published and is still undergoing revisions pending its formal adoption, the regulation's contours are now set.

The result is an ambitious, prescriptive standard that will have a global impact and could become a template for other AI regulators. It applies to both public and private developers, importers, distributors and deployers or users of in-scope "AI systems," a term defined to align with the recently updated OECD approach. The AI Act is the latest step in a broader EU strategy — including the Data Act, Digital Markets Act, Digital Services Act and GDPR — that focuses on responsible data use and algorithmic accountability.

Risk-based, tiered approach. The agreement preserves the risk-based approach reflected in the EC's original proposal. It applies different requirements depending on the risk tier that an AI system falls under:

- Minimal risk: AI systems that pose little or no risk to individuals' safety or rights will be exempt from most provisions.
- High-risk: AI systems used in machinery, medical devices, vehicles, critical infrastructure, education and employment-related decisions will face substantial obligations, including requirements related to risk mitigation, transparency, human oversight, data training set quality, and strict standards for accuracy, robustness and cybersecurity.
- Unacceptable risk: AI systems used to manipulate human behavior or for "social scoring" purposes, and some biometric uses, will be prohibited in most cases.

The negotiations resulted in a two-tiered approach for general purpose AI based on low and high systemic risks. Provisions include transparency obligations to alert users that they're interacting with a chatbot or that content is the product of generative AI. Model providers need to respect EU copyright law when training their models. The size of compute thresholds is a factor in determining high risk, which will trigger stringent model evaluation and reporting requirements. Deployers of certain high-risk systems will need to conduct a "fundamental rights impact assessment" of the risks to individuals before releasing the AI system on the EU market, as well as technical model evaluations, adversarial testing and incident reporting.

Governance and enforcement. A new AI Office within the EC will oversee the most advanced general purpose AI models, contribute to fostering standards and testing practices, and enforce the common rules in all member states. A new AI Board composed of member state representatives will serve as a coordination platform and an advisory body to the EC on the regulation's implementation, including the design of codes of practice for foundation models.

Member states will enforce the regulation directly. Maximum fines will range from €7.5m or 1.5% of global turnover to €35m or 7% of global turnover, depending on the organization's size and the specific infringement.

Once it's formally adopted, the regulation will enter into force incrementally over two years. Prohibitions become enforceable at the six-month point; transparency and governance requirements, at 12 months; and all other requirements, at the two-year mark.

Your next move. Although the final text is not expected until early 2024, companies with EU operations can begin taking steps to prepare. Start by assessing your potential exposure and the impact on your strategy, product design, operations and compliance program. Perform a risk assessment of your AI models to get a preliminary view on the mitigation lift. Inventory and monitor your AI-based activities now to avoid rushing into this task during the compliance readiness period. Follow principles of responsible AI, including governance, testing, training and risk management. Document your processes and controls and bolster their fitness for external reporting.

About | Contact us | Contributors

Why do we publish The Next Move?

Regulators and policymakers — keen to build new guardrails for a digital society — stand on largely unfamiliar ground. They often take different, sometimes contradictory, approaches because they have different missions and visions. At the global level, regulatory divergences reflect profoundly different value systems. Building trust in technology is complex work.

Through PwC's Next Move series, we can provide context to policy and regulatory developments in technology and tell you how you can get ahead of what might come next.

For additional information on our Next Move series, please contact:

Matt Gorham

Cyber & Privacy
Innovation Institute Leader

202 951 0439

matt.gorham@pwc.com

Chris Pullano

Financial Services
Advisory Partner

917 520 4447

christopher.pullano@pwc.com

Contributing editors and authors: Ted Trautmann, Jane Gari