The Next Move

Regulatory and policy developments in tech

December 2022

Five important trends in tech policy and regulation will accelerate in 2023. Protection is the unifying thread: for consumers, society, the economy and national security. Whether it's protecting consumers from financial scams and data privacy threats, or society from harmful social media content and biased artificial intelligence, or US economic and national interests from global threats, regulators are engaged and mobilizing. Learn more about these trends and how to respond strategically in this special edition of The Next Move.

In the December edition, we cover five developments:

Consumer protection vaults to the forefront of financial regulation

The trend

While financial regulation currently may not be the most pressing White House priority, there has been one notable exception: consumer protection. From launching an aggressive anti-discrimination campaign to scrutinizing fee structures to taking steps to increase competition, regulators have been hard at work on behalf of consumers — and these efforts will likely only increase in 2023.

What we're seeing

The administration's consumer protection efforts have spanned multiple agencies and approaches.

1. **Anti-discrimination in the spotlight**. Regulators have been focused on combatting discrimination in financial services, with Attorney General Merrick Garland announcing the Department of Justice's (DOJ's) "most aggressive and coordinated" anti-redlining initiative. The initiative, a partnership of the Consumer Financial Protection Bureau (CFPB) and the Office of the Comptroller of the Currency (OCC), will work to detect and enforce against lending discrimination in housing markets, including through new data analytics that will scrutinize service areas, branch locations and marketing practices for discriminatory behavior. Meanwhile, the CFPB launched its own anti-discrimination campaign to broaden its oversight scope to include nonbanks such as fintech firms. For the CFPB and other regulators, their focus remains on the use of algorithms that may inadvertently produce discriminatory outcomes.

2. **Focus on fees.** Attention to financial firm fee structures has intensified, with President Biden recently announcing efforts to address "unfair hidden fees … that are taking real money out of the pockets of American families." This initiative began late last year with the CFPB's scrutiny of overdraft fees, but recent guidance shows that the agency intends to expand its focus to all fees that it considers to be hidden or unfair, including late fees, application fees, convenience fees for payments, loan-origination fees, prepayment fees and bounced-check fees.

3. **Promoting competition.** President Biden made clear early in his administration, through an executive order, that promoting competition is a high priority. A recent CFPB proposal to boost financial services competition mandates that financial firms share customer data upon request. Director Rohit Chopra said this would increase competition by "empowering people to break up with banks that provide bad service," making it easier to move to a competitor without the painstaking set up of automatic payments and billing information at the new institution. Meanwhile, the Federal Deposit Insurance Corporation and the DOJ's Antitrust Division have announced reviews to their respective bank merger policies to address potential consumer harm and impact to underserved communities.

Why this matters for 2023

Many of the actions above include recently-launched initiatives and proposals that will likely become final over the next few months, so 2023 is gearing up to be a year of action with regard to consumer protection issues.

Your 2023 move

Financial firms should take the following steps to prepare.

- **Examine your practices for possible discrimination.** The anti-redlining initiative means that it's time to carefully examine whether your practices may inadvertently result in discriminatory outcomes.
    - **Use public data to assess compliance.** Leverage data reported under the Home Mortgage Disclosure Act to benchmark whether loans in racially/ethnically diverse neighborhoods stack up to peer banks. Take extra care to make sure that your data analysis is adequately sophisticated and that you are defining your "peer firms" accurately.
    - **Examine your outreach to racially/ethnically diverse communities.** For example, do you have intake channels with realty agents who cater to racially/ethnically diverse communities? Do you have advertising that is in a different language or targeted to those with limited English proficiency? Do you have non-English speaking loan officers?
    - **Address possible AI bias.** Catalog and map your internal automated decision systems and third-party/vendor software to understand the risks they might pose and how you intend to mitigate these risks. You may not be aware of AI mechanisms in your vendor software or how it's used, but if potential problems arise, your enterprise may be held accountable.

- **Confirm fairness and transparency of fee structures.** Following the CFPB's announcement that it will scrutinize overdraft fees, banks adapted quickly by either reducing fees or eliminating them entirely. With all fees now under the microscope, it's imperative to have a holistic catalog of fees and to examine customer-facing documents to make sure that fees are clearly disclosed and match how they are charged in practice. You should also review your pricing models with a focus on how they impact vulnerable customers and assess your operations to confirm that your systems are aligned with fee disclosures. Proactively engaging with regulators could be beneficial as it may provide regulators with welcomed transparency into your fee structures, while giving you insight into how they view your practices. We have seen several banks taking these steps, but those that have not will likely struggle with mounting regulatory scrutiny and competitive pressure.

- **Prepare for more M&A scrutiny.** With the DOJ and FDIC reviewing their guidelines around mergers, expect extended timelines and closer review before receiving regulatory approval. Considering the administration's focus on serving underserved communities, demonstrating that a potential merger will not impede consumer practices

can go a long way in making the regulators more comfortable with merger applications going forward. This includes not only having strong policies and procedures around consumer practices, but also reaching out to community groups to begin the discussion around community reinvestment plans the day the deal is announced — and having commitments in place for ongoing dialogue after the deal closes.

- **Assess how open banking may impact your business.** The CFPB's data-sharing proposal could create significant opportunities for new entrants by allowing bank customers to transfer account information, automatic payments features and billing history to other firms more efficiently. All firms should evaluate how open data access could disrupt their business and operating models and/or create new opportunities.

Data protection takes the global regulatory stage

The trend

China's stringent 2022 data privacy regulations have many multinational organizations scrambling to comply or reorganize, but 2023 is expected to be a banner year for data protection. A number of countries are proposing or considering initiatives, including India, Brazil, Russia, and possibly the US, where individual states are creating a patchwork of rules.

The impacts — as China's recent enforcement actions indicate — will likely extend beyond compliance to geopolitical ramifications and protection of intellectual property, among other concerns.

The regulations are emerging as companies, enabled in part by advances in artificial intelligence analytics, are finding more ways to use data they collect: to operate more efficiently, manage their risks, enhance customer services, create and support new business models, and more.

But unlocked data should be protected — something that many businesses still struggle with. Half of the business leaders we surveyed around the world said they don't feel confident in their organization's data governance and security.

What we're seeing

The EU's General Data Protection Regulation and the California Consumer Protection Act (CCPA) made waves when they appeared several years ago. (CCPA has been amended and expanded via the California Privacy Rights Act, taking effect January 1, 2023.)

But multinational organizations now face a flood of disparate data-protection and security laws from nations with competing interests. To navigate them successfully, you should begin planning now, taking into consideration a number of factors.

- **Proliferating regulations** so far include China's Data Security Law and the Cross-Border Data Transfer (CBDT) rule under its Personal Information Protection Law (PIPL). This rule already makes sending or accessing personal data across China's borders potentially fraught. It requires passing a cybersecurity assessment by March 1, with penalties for noncompliance. India, Brazil, and Russia are considering their own data-protection laws, as well.

- **Geopolitical agendas** bubbling under the surface can complicate the picture for multinationals. Enforcement decisions may at times appear arbitrary as data becomes more important to economic competitiveness and national security.

- **Intellectual property (IP)** is a growing concern, as companies worry that audits can expose sensitive information to competing eyes. Indeed, as fast-improving artificial intelligence analyzes the vast stores of data previously sitting in data lakes, this information becomes increasingly valuable to private enterprise and governments alike.

Why this matters for 2023

The regulatory focus on data, heightened in 2022, stands to rise to a fevered pitch this year. The Cyberspace Administration of China recently released privacy certification requirements. India's government recently published a draft of its data protection bill, which will likely come to a vote in 2023.

We expect to see more from both these countries, as well as possibly data laws from Russia, Ukraine, Brazil, Japan and others.

Your 2023 move

The right response to this trend goes beyond sharpening your compliance capabilities, as privacy has become about trust-building.

Multinational organizations should view data protection, privacy, and cybersecurity rules in the larger context of nations asserting policies, diplomacy and other tools that favor their economic competitiveness. To these nations, economic security is national security.

When confronted with a proposed data protection law, ask:

- Do we want to continue doing business in that market at our current level, or at all? Is it a risk worth taking?
- Do we want to reorganize our portfolio, shifting some of or all our focus to other markets?
- Are we concerned that our IP may be vulnerable? If so, how can we protect it?

Take action now to determine which markets are most important to your organization, learn as much as you can about pending or proposed data privacy laws in those markets, and develop a plan for how to prepare and respond.

If your company might need to localize its handling of data, consider revising your business systems architecture to add process controls and segment your systems.

Your plan should be an integrated one, designed not just for cyber, tech and privacy functions but for the enterprise as a whole. Data governance, ownership and privacy in today's climate are not just CISO, CIO or CCO issues but matters that can carry significant business implications. Protecting customer and business data, as well as company IP, requires a concerted effort and often a large investment that needs executive management and board-level deliberation and buy-in.

Long dormant US industrial policy reasserts itself

The trend

American industrial policy is back, after a decades-long hiatus. Protecting US competitiveness is a significant driving force in the Biden administration's agenda, both domestically and abroad.

On the domestic front, industrial policy informs myriad actions to create jobs, spur economic growth, rebuild infrastructure, restore supply chain resilience and fight climate change.

Globally, protecting US competitiveness — particularly in advanced technologies such as artificial intelligence, semiconductors, biotech and clean energy, which the administration considers "force multipliers" throughout the tech ecosystem — has become a matter of national security.

The White House views technology leadership as a vital bulwark against global threats to the economic, democratic and security interests of America and its allies.

What we're seeing

The new industrial policy spans multiple federal actions, including investments, protective measures and partnerships.

Investing in technology and infrastructure

CHIPS and Science Act	Inflation Reduction Act	Infrastructure Investment and Jobs Act	Biotech and bio manufacturing order	Climate crisis order
$52.7 billion to support semiconductor manufacturing, R&D and workforce development over the next five years	Nearly $370 billion in tax credits, incentives and funding to help companies tackle climate change and support renewable energy innovation and manufacturing	$1.2 trillion for investments in high-speed internet access, power grid upgrades, electric vehicle charging stations, public transportation and environmental remediation, and more	Investments in R&D, production capacity and workforce development to encourage medical innovations, improve food and energy security and sustainability, secure supply chains	Requires federal agencies to support clean energy priorities in making procurement decisions and in managing federal lands and assets

Protecting our tech advantage

A recent executive order instructs the Committee on Foreign Investment in the United States (CFIUS) to apply heightened scrutiny of deals that may give foreign adversaries access to critical technologies or that may endanger US supply chains, cybersecurity and personal data. A corollary effort is underway to screen outbound investments in sensitive technologies, particularly those not captured by export controls, that could threaten US competitiveness.

Similarly, the CHIPS Act contains guardrails that prevent funding recipients from expanding semiconductor manufacturing in nations deemed to be “countries of concern.”

As for export controls, sanctions against Russia severely restricted that country’s access to computer chips and other technology that could facilitate attacks on Ukraine, America and its allies. Regarding imports, the Federal Communications Commission banned the import of Chinese telecommunications and surveillance equipment deemed a threat to national security.

Further, the US Patent and Trademark Office is experimenting with fast-tracking patent awards for innovations in emissions-reduction, allowing rapid deployment without risking a company’s intellectual property.

Deepening global alliances

The Trade and Technology Council, formed in 2021, is charged with promoting US and EU competitiveness and prosperity as well as the spread of democratic, market-oriented values by increasing transatlantic trade and investment in emerging technologies. In June 2022, the White House announced various G7 initiatives promoting cooperation on supply-chain resilience, cyber and quantum technology, and democratic, market-oriented approaches to trade.

The Indo-Pacific Economic Framework for Prosperity, announced in May 2022, looks to increase cooperation on technology and trade between the United States and 12 Indo-Pacific region nations. Quad leader summits have championed cooperation between the United States, India, Japan and Australia on climate resilience, emerging technology, telecommunications infrastructure and exchange programs for STEM scholars. The administration’s proposed Chip 4 Alliance with Japan, Taiwan and South Korea would strengthen coordination in the semiconductor supply chain, while excluding China in the process.

Why this matters for 2023

We believe this industrial policy trend will likely continue and grow, despite the 2022 midterm election results. A divided Congress will likely lessen the prospects for passing new legislation, but major legislation has already been enacted. The impact of recent spending bills is only starting to take hold and accelerate into 2023 and beyond. Moreover, the goal of countering China’s global influence, which animates much of the new industrial policy, enjoys bipartisan support.

Executive and regulatory activity will likely continue unimpeded by the new Congress. Government procurement will continue. Global alliances will continue and, in fact, may even

flourish, if America's partners are reassured by the resilience of its electoral system demonstrated during the midterms.

All of this policy activity will persist because the underlying challenges — global warming, supply chain bottlenecks, talent shortages, geopolitical conflict and the new technology race — remain as pressing as ever.

Your 2023 move

Looking ahead, companies should consider taking advantage of the many grants and investment tax credits available through the various spending bills. These incentives, designed to entice companies to expand their capabilities or operations in the United States, are unprecedented. They do come with strings attached, however. You should understand clearly the restrictions and compliance burdens that go along with accepting federal dollars.

Businesses also should o stay on top of the many restrictions that govern foreign investments. These include CFIUS investment screening, potential outbound investment review and various import/export controls that can result in severe penalties.

Content moderation: The end of government deference?

The trend

Content moderation is at a crossroads. Regulators are taking action as social media companies work to control the proliferation of disinformation, harassment and scams. The White House has expressed concern over the effectiveness of self-regulation by social media companies. Meanwhile, Congress, the Federal Trade Commission, the Supreme Court and state legislatures have started weighing in. Internationally, several regulators are much further along in pushing for protections against harmful content. The recent relaxation in content moderation practices by some platforms, along with mass layoffs across technology companies, have only reinforced concerns among stakeholder groups.

Regulatory skepticism of online platforms' ability to self-govern extends beyond content moderation to include emerging technologies such as artificial intelligence, augmented reality, conduct in virtual reality and the metaverse, and accountability for abuses on web3's distributed systems.

What we're seeing

Globally, efforts to regulate online content include the following.

EU's Digital Services Act	Canada's Online Streaming Act	UK's Online Safety Bill	Australia's Online Safety Act 2021	India's Information Technology Rules 2021
Designed to better protect consumers and their rights online, this act will require companies to put in place systems for flagging illegal goods and content for faster removal	If passed into law, the C-11 bill will allow the country's radio and telecommunications commission to regulate audiovisual content on the internet	Proposes to make it mandatory for platforms to disclose content rules, due process protections, transparency reports, risk assessments and mitigation measures for harmful content	Allows an eSafety commissioner to compel digital platforms to remove "cyber-abuse material" within 24 hours	Requires tech and media companies to disclose the source of content within 72 hours of a request from certain agencies, and to remove "unlawful content" within 36 hours

The governments of Turkey, Germany and Brazil are also considering imposing new obligations on social media companies.

Disclosure-influenced self-regulation. Domestically, key states have also begun to act. California's AB 587, for instance, takes a new approach to content moderation. The law requires large social media companies to begin posting semiannual reports about their content-moderation practices, including details on flagged content and actions taken, no later than January 1, 2024. Rather than dictating how these companies moderate content, the law uses public disclosure as a tool to encourage better self-regulation.

Public-private collaborative governance. The California approach reflects an emerging perspective that advocates for "collaborative governance" as an alternative to the current moderation paradigm of self-regulation with little or no government oversight. This implies the creation of an administrative structure in which organizations will be accountable through audits, impact assessments, transparency reports, ongoing monitoring and other governance tools. In such a system, private and public entities can work together to achieve shared goals.

Why this matters for 2023

Section 230 of the US Communications Decency Act protects social media companies from most forms of liability related to the content they host. However, the Supreme Court is considering whether to hold companies accountable for content allowed on their sites.

Further, increased governmental scrutiny and differing requirements are likely to have major economic and operational implications, including significant costs for audit, technology and R&D, and recruitment and training.

Your 2023 move

To uphold trust, technology companies should start cultivating effective capabilities to monitor their platforms' compliance with potential new regulations. They also should build capabilities to identify and mitigate new forms of abuse on their platforms. This means developing the governance structures and operating models that can bridge the gap between policy formulation and enforcement. These capabilities should be supported by a holistic trust strategy that can confirm consistency in values across all the markets while accounting for local laws and cultural norms.

Developing these capabilities with a relentless focus on stakeholder trust is seen as the most effective way to avoid government over-regulation and the concomitant economic and reputational consequences. The time to act is now.

See The quest for truth: Content moderation in action for a more detailed look.

Largely unregulated, artificial intelligence faces a reckoning

The trend

While many technologies face increased regulation in the coming years, perhaps none commands such a sense of urgency as artificial intelligence, or AI. The terrain is largely unregulated, brimming with potential, but also fraught with unintended risk to people and

societies. AI development often embodies a “fail fast” mindset that spurs a rapid pace of innovation, which can lead to mistakes and bias.

Recognizing the dangers, governments — with the European Union leading the way — are preparing the ground for regulatory fences around AI’s use. Concerns over AI are wide-ranging, but the most prevalent include:

- Bias and discrimination/fairness
- Transparency and explainability
- Data protection, privacy and surveillance
- Governance
- Accountability
- Third-party management

We expect to see many regulatory efforts come to fruition in 2023.

What we’re seeing

More than 800 AI policy initiatives are pending in 69 countries, according to the Organisation for Economic Co-operation and Development (OECD). Key regions include:

- **Europe.** The EU’s AI Act establishes a “future-proof” definition of AI, presents a taxonomy with prescribed governance actions for high-risk AI forms, and bans from use those that pose “unacceptable risk.” It aims to encourage companies to design AI systems to reduce harm.

  The AI Act is in its final stages of development and approval and it’s expected to pass in mid-2023. Like the General Data Protection Regulation (GDPR), it’s likely to have a far-reaching effect extending to AI-using organizations in all countries that interact with EU residents.

  The EU AI Liability Directive will make it easier for individuals to sue companies using AI for harms they have suffered because of the technology. It aims to provide recourse to those who have been harmed by AI. Only proposed in September 2022, it’s not known when it might pass.

- **United States.** The White House’s recently released Blueprint for an AI Bill of Rights aims to mitigate the risks of consumer-facing AI. Simultaneously, the administration announced a host of actions that federal agencies will take to advance the blueprint.

Although not a mandate per se, the blueprint states that its principles "should guide" AI design and use, and the Federal Trade Commission could use those principles as justification in enforcement actions.

- **New York:** The City of New York Local Law 1894-A, effective January 1, 2023, requires employers within the city to audit AI employment decision systems for bias before using them. It mandates notification of candidates and employees living in the city that the tools are being used and how.

The year 2022 saw a raft of AI policies, guidelines, stimulus bills and related measures worldwide. Of the current policy initiatives regarding AI use, 299 take the form of guidance or regulation, according to the OECD. We can expect to see many of these adopted in the coming year.

Why this matters for 2023

Although governing bodies have heightened their scrutiny of business AI use in recent years, the rapid advance of "generative AI," which creates new content from existing data, and the emergence of such technologies as "plausible reality," AI-created scenarios that mimic reality without replicating it, has them stepping up the regulatory pace.

As a result, we can expect to see AI laws and mandates appearing at a rapid rate in 2023. Advances in the field have far outpaced regulation. Fearing harm to their constituents, governments want to correct that imbalance before it's too late.

Your 2023 move

Enterprises of all stripes may have to scramble to comply with emerging AI mandates in 2023. Will yours be among them? We recommend starting the process of compliance with an AI framework such as the in-progress National Institute for Science and Technology (NIST)'s AI Risk Management Framework. See PwC's Responsible AI: AI you can trust for a more detailed look.

Contact us

For additional information on our Next Move series or PwC's Technology, Media & Telecommunications Regulatory Practice 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

Michael Corey
Technology, Media and Telecommunications Partner
415.505.2482
michael.j.corey@pwc.com

For deeper discussion, please contact:

AI regulation
Anand Rao
Jocelyn Aqua
Ilana Blumenfeld

Consumer protection in finance
Amanda Cox
Nicole Anderson

Data protection
Nalneesh Gaur

Incentives for tech investments
Mike Pegler

Content moderation
Dan Hayes

Contributing editors and authors:

Ted Trautmann, Cristina Ampil, Tanya Pazhitnykh, Michael Horn, Jennifer Day