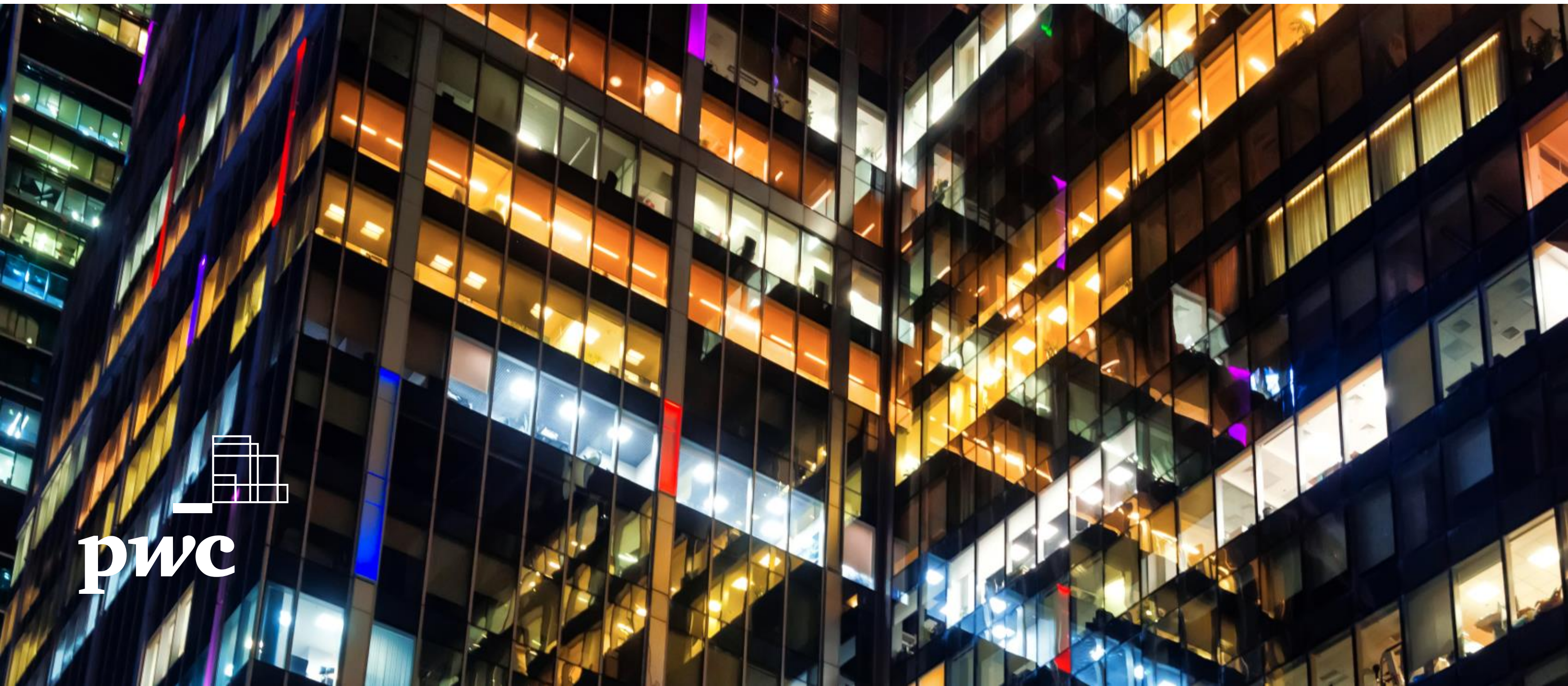
The Next Move

Regulatory and policy developments in tech — July 2024



Cyber harmonization push gains momentum but faces obstacles

By Shawn Lonergan, Matt Gorham and Jane Allen

The issue

Efforts to streamline the many overlapping and sometimes conflicting cybersecurity requirements, both domestic and global, are accelerating. Recent developments include a Government Accountability Office (GAO) study assessing progress on multiple cyber harmonization priorities, a summary of stakeholder comments received by the Office of the National Cyber Director (ONCD) in response to its request for information (RFI) on cyber harmonization, and proposed legislation to establish a harmonized framework.

These efforts make clear the extent of the compliance burden faced by US companies and the complexity of the harmonization task faced by policymakers.

But despite widespread agreement on the need for change, actual progress is lagging. Indeed, harmonization efforts seem to be outpaced by the push for new rules by the Cybersecurity and Infrastructure Security Agency (CISA), which differ from most existing US requirements and could exacerbate the problem. Layer in global obligations and the issue is even more complex.

Affected organizations should advocate that any new rules from CISA or other authorities be designed to help streamline existing cyber requirements, not compound the burden and potentially divert resources needed for risk mitigation. In short, new rules should be "harmonized by design" — before, not after, they're implemented.

The policymakers' take

Congress mandated cyber rule harmonization and reciprocity in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), a law designed to protect national security, economic security and public health and safety through a coordinated approach for understanding cyber incidents across critical infrastructure sectors. Under CIRCIA, a covered entity that's required to report substantially similar information on a covered cyber incident or ransom payment to another federal agency in a similar timeframe doesn't have to submit a CIRCIA-mandated report if CISA has an information-sharing agreement and mechanism in place with the other agency.

CISA proposed rule. CISA's proposed rule implementing CIRCIA, issued on March 29, 2024, considers this reciprocity mandate in §226.4. Under the proposal, CISA will enter into an information-sharing agreement with another federal agency when CISA has determined the agency requires cyber incident reporting on "substantially similar information in a substantially similar timeframe" and the agency has "committed to providing the covered entity's report to CISA within the relevant deadlines."

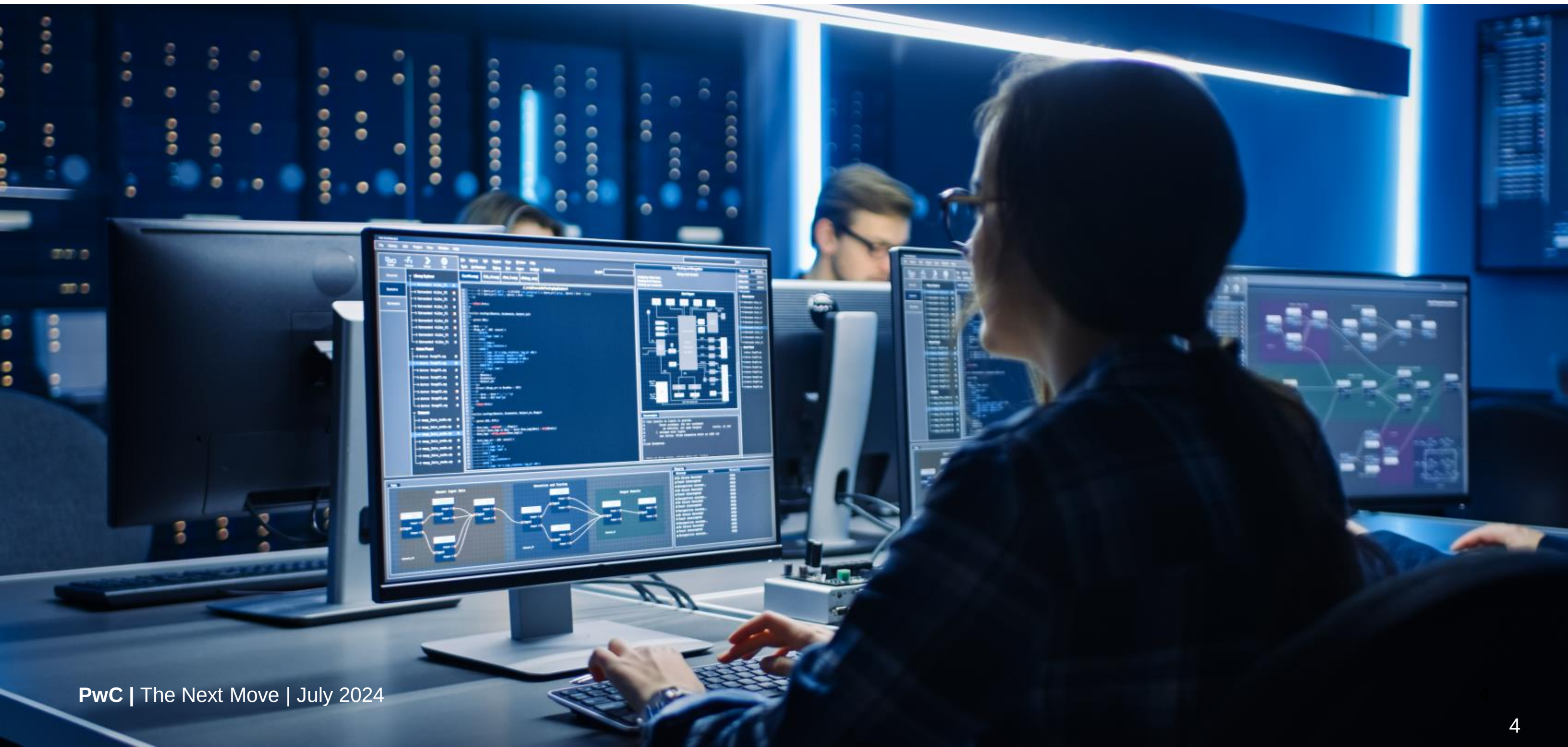
But whether this commitment will result in actual harmonization is unclear. CIRCIA reporting requirements are different from, and sometimes more stringent than, most existing requirements. Indeed, CISA noted, "While many of the regulations CISA reviewed have some similarities in how they define and interpret what is a reportable cyber incident, the specific language, structure, examples, and actual requirements varied greatly based on the specific agency mission and purpose of the regulation."

In short, CISA's proposed rule introduces a new layer of unique requirements that may not qualify for reciprocity with existing cyber rules.

Recent harmonization activity. Following CISA's proposal, the push for harmonization gained momentum with several new developments.

- GAO study. Issued on June 5, 2024, the GAO study reviewed multiple cyber harmonization initiatives and found that "significant work remains to be completed." For example, White House efforts to evaluate setting minimum cybersecurity requirements across infrastructure sectors, to increase agency use of frameworks and international standards to inform regulatory alignment, and to leverage reciprocity pilot programs are still in the works. In addition, a September 2023 report from the Department of Homeland Security (DHS) lacked specific starting and completion dates for implementation. As the GAO concluded, "Following through and executing specific plans and meeting established time frames, as supported by key organizations such as ONCD, DHS, and Congress, are essential to achieving harmonization."

- ONCD summary of stakeholder comments. Issued on June 4, 2024, the ONCD's report notes that the agency received 86 responses to its RFI on the challenges of regulatory overlaps, including input from organizations representing over 15,000 businesses spanning 11 of the 16 critical infrastructure sectors. Key findings include:
    - The lack of harmonization and reciprocity harms cybersecurity outcomes while increasing compliance costs through additional administrative burdens. Many respondents noted that compliance spending diverts resources away from cybersecurity programs.
    - Challenges extend to businesses of all sectors and sizes and cross jurisdictional boundaries. Respondents highlighted inconsistent or duplicative requirements across international and state regulatory regimes.
    - The US government is positioned to address these challenges. Respondents provided many suggestions for how the administration and Congress can increase harmonization. Examples include working with foreign allies to drive international reciprocity, holding vendors to the same standards as critical infrastructure operators and coordinating with state, local, tribal and territorial governments.
- ONCD pilot. Building on the RFI findings, the ONCD is exploring a pilot reciprocity framework to be used in a critical infrastructure subsector, as described in National Cybersecurity Strategy Implementation Plan Version 2 (initiative 1.1.5). The agency expects to complete the pilot in 2025.
- Proposed legislation. On July 8, 2024, Senator Gary Peters (D-MI) introduced a bill, the Streamlining Federal Cybersecurity Regulations Act (S 4630), which would require the ONCD to establish an interagency committee to harmonize cyber rules issued by federal agencies. At a previous Senate committee hearing on the draft bill, an ONCD official testified that such a mandate from Congress would help the agency to work with independent regulatory bodies to design a harmonization framework.



Your next move

While these developments are encouraging, they may be too late in coming to address CIRCIA rulemaking that's already underway. We're now at an inflection point. Delaying implementation until after another layer of rules takes effect could set the harmonization effort back significantly.

Affected organizations should take immediate action.

1. **Map your cyber compliance program to regulatory expectations.** Understand the common elements of your program and map them to the many applicable cyber rules, including the proposed CIRCIA reporting rule. The sooner you identify the one-to-many and document your story, and your plan if applicable, the better. That can help identify current gaps in compliance. Going forward, continue to track new requirements and adjust your mapping to help prevent new gaps from forming.

2. **Develop a harmonization point of view.** Work with your compliance, legal and other stakeholder teams to craft your organization's stance on cyber regulatory harmonization and the impact of a delay in its implementation. Specifically, craft your position on the urgency of harmonizing the CIRCIA reporting rule with existing rules before it becomes final. Consider potential approaches to facilitating reciprocity between CISA and other regulators, as well as ways to reduce duplication of new and existing requirements overall.

3. **Engage with policymakers to effect change**. Collaborate with industry groups, the White House, Congress and your sector risk management agency to advocate for your organization's concerns. Communicate the importance of timely implementation — including harmonization of any new rules before they're adopted — to avoid compounding the complexity of this critical, shared policy goal.

4. **Explore the *Chevron* implications for your strategy.** Consider how the Supreme Court's recent ruling overturning *Chevron* deference may alter the future of cyber regulation. The decision may, for example, encourage more court challenges to agency rules, resulting in greater regulatory uncertainty.

5. **Prepare for a new regulatory model.** Start planning for the target harmonized model (one set of rules in lieu of many) by identifying the most likely elements that emerge as the process unfolds. This includes considering global regulations from a practical perspective of execution and compliance. Work closely with your general counsel to align on strategy and bolster the compliance infrastructure now — using automation and managed services to streamline your compliance function — to support both current obligations and the anticipated end-state. Whatever the outcome, having the program in place to assess compliance risks and gaps, and to test and measure the strength of your controls, can help you quickly adapt to a harmonized model and demonstrate a defensible posture along the way.

For more information on the CIRCIA proposed rule, see Cyber reporting for critical infrastructure: CISA proposal raises many questions, invites comments.

Crypto policy shift signals need for strategic action

By Matthew Blumenfeld, Andrew Hillyer and Roberto Rodriguez

The issue

The lack of comprehensive federal legislation establishing guardrails for digital assets has prompted many firms in the financial sector to move operations abroad, and other companies continue to struggle with the uncertainty. Finally, however, a surge of bipartisan legislation suggests that the regulatory environment may be starting to change.

In May 2024, Congress initiated several important measures to regulate digital assets, including passing a resolution that allows firms holding crypto for customers to remove the assets from their balance sheet (H.J. Res. 109), advancing a digital asset market structure bill (FIT21), and blocking the Federal Reserve from issuing a central bank digital currency (CBDC Anti-Surveillance State Act). Also noteworthy was the introduction of the Lummis-Gillibrand Payment Stablecoin Act in April 2024 and President Biden's veto of H.J. Res. 109.

Although still early, with far to go in terms of implementing substantial reforms, this activity represents a clear shift toward broader, bipartisan support for digital assets. For affected organizations in financial services and other sectors, it's time to get ahead of this trend. These businesses should plan accordingly to help maintain a competitive edge as the changing regulatory dynamic opens the door for traditional market participants to innovate with this technology.

The legislators' take

A closer look at each of these measures reveals how they address specific challenges and contribute to a larger regulatory framework.

Resolution to nullify SAB 121. Passed with clear majorities in the House and Senate, H.J. Res. 109 would rescind the SEC's Staff Accounting Bulletin 121, which requires digital asset trading platforms and financial institutions to list crypto assets held for customers as a liability on the firm's balance sheet. Rescinding SAB 121 would eliminate this disincentive to holding crypto assets for customers. As Congress explained:

> By placing custodial assets onto the balance sheet, it puts customer assets at greater risk of loss if the custodian becomes insolvent or enters receivership. Likewise, SAB 121 will increase capital, liquidity, and other burdens on digital asset custodians under the existing prudential regulatory framework by requiring on-balance sheet treatment of digital assets. As a result, it will be far more expensive for a firm to custody digital assets compared to traditional assets. This in turn is likely to discourage banking organizations from providing custodial services for digital assets.

Despite its bipartisan support, however, President Biden vetoed the measure on May 31, 2024. The House tried but failed to override the veto on July 11, 2024. The issue remains a hot topic among legislators driven in part by continued lobbying efforts from market participants.

The Financial Innovation and Technology for the 21st Century Act (FIT21) passed in the House on May 22, 2024, by a vote of 279 to 136. It aims to delineate oversight responsibilities between the SEC and the Commodity Futures Trading Commission (CFTC), resolving longstanding regulatory uncertainty in the digital asset market.

The bill would create three categories of digital assets: "restricted digital asset" (subject to SEC jurisdiction), "digital commodity" (subject to CFTC jurisdiction) and "permitted payment stablecoin" (subject to either agency, depending on the transaction's intermediary). Digital asset intermediaries would have to register with the SEC or CFTC based on the type of asset. Both agencies would have to issue rules, for example, exempting duly registered intermediaries from duplicative, conflicting or unduly burdensome requirements. The bill would also repeal SAB121 for banks and trust companies, but not other public companies.

Despite passing overwhelmingly in the House — the first time a chamber of Congress has passed major digital asset legislation — FIT21 faces considerable hurdles. The Biden administration, for example, expressed concerns that the measure lacks sufficient investor protections. The bill now awaits consideration in the Senate, where its fate remains uncertain.

While many in the industry view this development as a positive move, critics within crypto point to aspects that would vastly expand the regulatory reach of the SEC and CFTC compared to their traditional remits and how they treat similarly situated assets today.

The CBDC Anti-Surveillance State Act, passed by the House on May 21, 2024, would prohibit the Federal Reserve from developing or issuing a digital dollar. It would also prohibit the central bank from using any CBDC to implement monetary policy. Approved largely along party lines (216 to 192), the measure reflects concerns over governmental surveillance and control over personal spending habits, as well as the potential competitive impact on financial institutions. Opponents argue that the bill could hinder the global competitiveness of the US financial system, restricting the central bank's ability to innovate with CBDCs while other nations are actively developing their digital currencies. As with the FIT21 bill, this measure faces substantial hurdles in the Senate.

The Lummis-Gillibrand Payment Stablecoin Act, introduced in the Senate on April 17, 2024, would create a regulatory framework for stablecoins. Designed to protect consumers, foster innovation and promote US dollar dominance while preserving the dual banking system, the bill would require that issuers maintain adequate reserves (typically a 1:1 ratio with a stable asset) to back digital assets and improve financial stability. It would also include mechanisms to prevent illicit stablecoin use and require issuer transparency and accountability.

While the Stablecoin Act has been welcomed by many as a necessary step towards a more mature cryptocurrency market, it also faces obstacles. Critics argue that while the act provides needed regulatory clarity, it could impose strict requirements that could stifle innovation and limit flexibility. Furthermore, there are concerns about how these regulations align with broader federal and state laws governing monetary and financial services.

Looking ahead. The convergence of ongoing legislative action, industry engagement and the November elections will likely determine the trajectory and pace of cryptocurrency regulation in the United States. As the dynamic between Congress and regulatory agencies like the SEC becomes more pronounced and industry lobbyists continue to push awareness of the technology's nuances and the risks of innovation moving offshore, this year could mark an important turning point in regulatory policy.

Your next move

Recent legislative activities signal a policy reset in favor of a structured framework for digital assets. Affected organizations in financial services and other sectors should consider how broader acceptance of this technology may affect their business.

- **Develop or refine your viewpoint.** If your organization stands to be affected by this policy trend, think through and assess the implications for your business model. Ask how to take advantage of the technology and the emerging regulatory clarity — from product offerings to service delivery and customer engagement. Ultimately, this early thinking will inform your approach and messaging as the regulatory environment becomes increasingly amenable to digital assets.
- **Create a plan.** With a viewpoint in place, develop a strategic plan that incorporates the anticipated regulatory frameworks. This plan should outline how to leverage the benefits of digital assets while managing the risks associated with regulatory change. It's crucial to consider integrating emerging technologies, such as blockchain and stablecoins, into existing business models.
- **Establish a digital asset group.** Creating an internal group dedicated to digital assets is an effective way to focus efforts on assimilating these technologies into your business operations. This group should be tasked with staying current on regulatory developments, exploring new opportunities for using digital assets and confirming compliance with regulations as they evolve.
- **Monitor policy developments.** Track and follow legislative progress in this space. Engage with policymakers and industry groups to help shape the contours of the emerging framework.

UK adopts bespoke, flexible approach to Big Tech oversight

By Manuj Lal, Jake Meek and Sara Putnam

The issue

On May 24, 2024, the United Kingdom adopted the Digital Markets, Competition and Consumers Act (DMCCA), the most significant reform to UK competition and consumer law since the Competition and Markets Authority (CMA) was created in 2014 and the first major post-Brexit reform. Despite similarities to its EU counterpart, the Digital Markets Act (DMA), the UK law offers a more flexible, tailored approach to regulating Big Tech.

This flexibility is apparent in how the DMCCA defines who’s covered and what conduct requirements they’ll face. Covered entities — those tech giants found by the CMA to have “strategic market status” — are companies that satisfy a mix of quantitative and qualitative criteria, in contrast to the EU approach of automatic “gatekeeper” designation based on user number and financial thresholds. Conduct requirements — equal treatment, interoperability, user choice, etc. — will be tailored to each SMS firm's situation and position.

Although welcome for companies also subject to the EU DMA, the DMCCA’s flexible approach could result in a complex array of parallel and potentially conflicting obligations. It also means greater uncertainty about what conduct rules will apply. Affected organizations should prepare to adapt their risk and compliance programs to accommodate these potentially divergent requirements.

The regulator’s take

The DMCCA creates a new framework to improve competition in UK digital markets by conferring powers and duties on the CMA to regulate competition in these markets, including new powers to investigate and enforce competition and consumer protection law. The law protects consumers against unfair commercial practices, subscription traps and prepayments to savings schemes.

Covered entities. A company may be designated as having strategic market status (SMS) if it:

- Engages in “digital activity”, meaning it provides services via the internet or digital content.
- Has UK-linked activity, either by user or business presence, or because it's likely to have an immediate, substantial and foreseeable effect on UK trade.
- Has substantial and entrenched market power forecast over at least five years.
- Has strategic significance, as determined by its relative size or scale, a significant number of business users, the ability to leverage its digital activity in favor of other activities and the ability to determine or substantially influence the conduct of other undertakings.
- Has turnover that exceeds £1 billion in the United Kingdom or £25 billion globally.

The CMA has issued draft guidance on how it intends to apply these criteria in an SMS investigation. Unlike the EU DMA approach of automatically designating certain online platforms as gatekeepers based on their size (subject to challenge), CMA’s Digital Markets Unit (DMU) will have discretion to determine whether a company has SMS in relation to a given digital activity. The DMU is expected to seek early engagement with potential designees at the front-end of the process.

Conduct requirements. The DMCCA provides that the DMU will develop an individual, bespoke code of conduct for each SMS firm designed to address the particular harms associated with a company’s digital activities. Drafting these tailored requirements will require a collaborative process involving dialogue between the regulator and firm to account for the firm's individual circumstances, including its business model, products and third parties.

In contrast, the EU DMA lists do’s and don’ts for all gatekeepers, though the commission may in certain circumstances “further specify” the steps an individual gatekeeper must take to establish effective compliance.

The DMCCA conduct requirements must serve one or more of these objectives.

- Fair dealing, meaning that users and potential users are treated fairly and can interact with the SMS firm’s service or digital content on reasonable terms. Examples include requirements that the firm trade on fair and reasonable terms, have effective processes for handling user complaints and refrain from using data unfairly.
- Open choices, meaning that users can choose freely and easily between the SMS firm’s services or those of its competitors. Examples include requirements forbidding the firm from using its position or access to data to treat its own products more favorably than those of competitors, or from restricting interoperability between the relevant service or digital content and competing products.
- Trust and transparency, meaning that users have the information they need to understand the SMS firm’s services and terms, and to make informed decisions about whether and how they interact with the firm regarding the relevant digital activity. Examples include requirements that the firm provide clear, accurate and accessible information about the relevant digital activity, give notice before making material changes and present default settings in a way that allows users to make informed decisions about those settings.

Exemptions. SMS firms may be exempt from complying with applicable codes of conduct or remedies if they can show that the conduct in question produces net consumer benefits that outweigh any actual or likely detrimental impact on competition and where the conduct is indispensable and proportionate to realize those benefits. This allows even more flexibility in tailoring conduct requirements to the firm's situation and the broader consumer impact. In contrast, the EU DMA has no such exemption.

Pro-competition interventions. The CMA may impose pro-competition interventions (PCIs) on designated undertakings if it finds that factors relevant to a digital activity are preventing, restricting or distorting competition, and that imposing a PCI would likely help to mitigate or prevent the anticompetitive impact. PCIs can include a range of behavioral or structural remedies, including measures enabling consumers to easily transfer their data from one provider to another, requiring different products and services to be interoperable or mandating divestiture within SMS undertakings.

Sanctions. The DMCCA, like its EU counterpart, allows fines for infringement of up to 10% of a company's worldwide annual turnover. Unlike the DMA, the UK law also provides for sanctions against responsible individuals, including director disqualifications for serious regulatory breaches and civil penalties on named senior managers who fail to comply with requests for information.

Implementation timeline. It's unclear when the DMCCA will take effect, the timing of which will depend largely on the new government's priorities. Companies should prepare for the possibility that the law may enter into force later this year.

The CMA's SMS designation investigations are expected to begin in the fall of 2024 and take up to nine months.

Your next move

Tech companies with significant UK operations will need to prepare for potential SMS designation. If they're already subject to the EU DMA, they'll need to adapt their risk and compliance programs to a new set of potential obligations. Here are some strategic, "no regrets" moves toward DMCCA compliance that you can start implementing now.

1. **Make data portability easy.** Take steps to allow your end users and third parties authorized by them to easily access and transfer their data in real-time. You may already be doing something similar under the General Data Protection Regulation (GDPR) and/or DMA. Data portability requires that you provide end users and third parties with free, effective tools to facilitate any portability requests. A preliminary step might be to understand how your end users and third parties would access and transfer their data, if allowed.
2. **Support and foster interoperability.** Identify any current policies and business practices that the DMU might deem self-preferencing or anti-competitive due to a lack of interoperability. Consider how to modify them in a way that advances interoperability. This means allowing consumers and business users to choose freely and easily among your company's and its rivals' services or content.
3. **Define fairness.** Define what fairness means in the context of pricing, business terms, internal processes and user outcomes. Develop internal metrics that would help to assess fairness in each area and collate data to assess fairness according to these metrics.
4. **Increase data transparency.** Consider what types of data would be useful to provide to publishers and advertisers to empower them to make better decisions and address the DMU's competition concerns. Explore what format and channels are the most appropriate in providing this data to advertisers and publishers.

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

LinkedIn

Chris Pullano

Financial Services
Advisory Partner

917 520 4447

christopher.pullano@pwc.com

LinkedIn

Contributing editors and authors: Ted Trautmann, Rachael Joyce, Sida Yin