WWW.GLOBAL-COUNSEL.COM

Global Counsel

Online safety: the next wave of regulation

MARCH 2025

Introduction

Of all the issues that have driven the "techlash" over the past decade, online safety and content moderation have proven the most emotive and durable, but also contested. This is not surprising given that they raise fundamental questions for modern democracies – how news and opinion should be distributed, shared and consumed; how governments, political parties and candidates communicate with their electorates; what, if any, qualifications should be applied to freedom of expression online; and how to protect children and young adults when content, experiences and activities are easily accessible and seemingly limitless.

Over the past decade the Global Counsel team has worked on the landmark reforms of the EU's Digital Service's Act (DSA) and the UK's Online Safey Act (OSA) from their inception in the late 2010s to their implementation today. Our Washington DC team has tracked closely the legal challenges and policy debates around Section 230 and the growth of content moderation laws at the state level across the USA. We have had the privilege of working with the full spectrum of industries impacted by these changes from social media platforms and gaming companies to dating apps and app stores.

The objective of this report is to understand where we are likely to see future legislative reforms and the form they might take. Initially we were struck by the fact that before laws like the OSA were even in place, there was already an emerging debate about legislating to go even further. And before a single DSA enforcement case had concluded, Commission President Ursula von der Leyen was committing to further reforms in areas like addictive design.

The advent of the second Trump administration has transformed the online safety policy agenda and this report's focus. The strident views of the President and the Vice-President have elevated online safety and content moderation policy to the top of transatlantic relations. Online safety is no longer a domestic policy agenda - any decision in Europe for further legislation or enforcement will now be taken in the knowledge that it could prompt potential retaliation from the Trump administration.

This report aims to act as a guide to businesses, policymakers and the wider policy community as to how these tensions could play out and where we can anticipate further legislative reform and enforcement action in the coming years.

CONAN D'ARCY
Senior Practice Director, Technology, Media and Telecoms

Executive summary

Implications for businesses

COMPETING EXPECTATIONS ON COMPANIES

Companies will need to navigate opposing expectations from policymakers in the US and Europe, especially in areas like the moderation of misinformation. While the risk initially will be a reputational one, there is a growing prospect in this political cycle that it could evolve into competing legal obligations, for example, in areas like the accuracy of answers given by generative AI chatbots and other applications on contentious political questions.

NEW RULES FOR CHILDREN ONLINE AND AI CONTENT

Not all policy areas are equally exposed to transatlantic dynamics, and there remains a high likelihood that there will be new legislation on both sides of the Atlantic on the protection of children online and transparency measures for AI-generated content. In contrast, new legislation on misinformation and encryption is unlikely and these policy areas will primarily play out via enforcement actions.

MORE UNPREDICTABLE POLICYMAKING

In contrast to previous political cycles, which saw long policy formulation processes for the DSA and the OSA, the course of online safety policy will be less predictable. It will also be less self-contained - other sources of transatlantic tension, like tariffs, defence and Ukraine, will influence how Europe and the US pursue and prioritise online safety policy.

Protecting children

Legislative reform to protect children online is likely in the medium-term, driven by widespread public concern. There are three main areas where policy is likely to focus: age verification, restrictions on under 16s accessing online services, and measures to combat online addictiveness.

Renewed attempts to pass federal legislation while an increasing number of states pass legislation to protect children online.

A greater focus on child protection, including measures to tackle online addictiveness as part of the Digital Fairness Act (DFA).

A series of OSA enforcement cases and a notable chance of new legislation limiting online access for under 16s.

Misinformation

Transatlantic tensions will be most evident in misinformation policy, making the passage of new legislation unlikely in the near term. The focus of policy activity will therefore concentrate on enforcement of existing legislation, most notably the DSA.

While there is no prospect of misinformation laws, new proposals at state level on algorithmic management can be anticipated.

Ongoing controversy over the pace, scale and outcome of DSA enforcement cases.

A growing debate over “legal but harmful” content, including misinformation, with a slim chance of legislative reform.

AI generated content

There is a high likelihood of new rules coming into force in the next few years. The current policy consensus could, however, prove temporary should the strained debate on misinformation be transposed to AI chatbots and other generative AI tools.

A continued focus on AI labelling and disclosures at the state-level and potentially at the federal level too.

A focus on the practical methods of labelling AI content in order to implement the AI Act.

Legislation to ban sexual deepfakes with a potential focus on labelling later in this Parliament.

Encryption

There is no consensus in favour of reform, meaning that new legislation is unlikely in the coming years with the potential exception of the EU's Child Sexual Abuse Material (CSAM) regulation.

Renewed congressional attempts to pass CSAM reforms but will face significant headwinds.

There is an outside chance that the long-stalled CSAM regulation could pass, albeit in a modified form.

The prospect of enforcement activity under the UK's Investigatory Powers Act (IPA) remains contingent on the outcome of ongoing legal cases.

Research approach

Public

SURVEY

Quantitative survey in the UK, France and US to understand incidences of different views among the public and to enable robust comparison between and within countries. France was selected as an example of a major EU member state.

Online survey up to 15 minutes.

Nationally representative sample of n=1,000 in each of UK, France and US (with a total sample of n=3000). Quotas applied for gender, age, region and other demographic variables.

IN-DEPTH INTERVIEWS WITH MEMBERS OF THE PUBLIC

Interviews with members of the British public to understand their key concerns related to online safety, and awareness of existing online safety initiatives and regulation.

45-60 minute interviews conducted online.

10 members of the public were recruited to reflect a spread of ages, gender, ethnicity, socioeconomic group, parental status, area or residence (including urban, suburban, rural), internet usage, and awareness of online safety initiatives.

Policy community

QUALITATIVE INTERVIEWS

Qualitative interviews in London, Brussels and Washington DC to explore the views of policymakers and policy experts in relation to online safety, as well as potential regulatory initiatives.

In depth interviews, lasting 30-45 minutes, conducted either face-to-face or via video-conference.

In the interests of brevity, charts in this report occasionally feature abbreviated versions of the questions and answer options shown to respondents in the survey. Full data tables are available on request. Note that percentage figures based on public survey data may not always add to 100% due to rounding.

Context

THE ORIGINS OF ONLINE SAFETY REGULATION

Debates over user generated content have their origin in the early era of internet governance. The focus in the late 1990s was to support the growth of the nascent internet and ensure that websites and online services could facilitate the uploading and sharing of user content (or products) without incurring legal liability.

This resulted in two pieces of legislation which shaped the growth of social media, search and e-commerce. In the United States, Section 230 of the Communications Decency Act[1] provided liability exemptions for online platforms, clarifying that they should not "be treated as the publisher or speaker of any information provided by another information content provider." Section 230 also introduced a so-called "good Samaritan" clause by empowering online services to "restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" without fear of legal challenge.

In the EU, the e-Commerce Directive [2] similarly clarified that internet services were not liable for hosting, caching and transmitting user-generated content and made clear that there was no "general obligation" for platforms to monitor the content on their services. It did, however, empower EU member states to apply specific provisions on platforms to inform national authorities of illegal activity on their platforms.

THE BREAKDOWN OF THE 1990S CONSENSUS

This broadly held for the next fifteen years. However, particularly in the case of the EU's e-Commerce Directive - due to its absence of a comparable "good Samaritan" clause - the ambiguity over the roles and responsibilities of platforms was increasingly tested and the subject of political debate. As social media, video-sharing apps, gaming platforms and dating services matured and secured millions, and even billions, of users globally, a series of high profile safety incidents ignited the debate around online content moderation and how to balance this with free expression and the legal obligations (or absence of them) for platforms to proactively monitor and moderate their networks.

Perhaps the best known is the Cambridge Analytica scandal, ironically an incident that was less about online safety and more about data protection standards, but one which nevertheless prompted a renewed debate around online platforms and their influence over public discourse and, critically, electoral processes. In parallel, social media platforms increasingly faced criticism for facilitating the livestreaming of harmful content, some involving footage of serious crimes. Facebook responded by hiring thousands of content moderators, setting the template for other technology companies to follow.

In spite of these changes, online incidents have continued and have had a galvanising effect on political and media attitudes. The Christchurch shootings led to the Christchurch Call process[3], which was a

key stepping stone for France and other EU countries towards regulation in what ultimately became the DSA. Likewise, the suicide of Molly Russell transformed the UK's debate on online safety, ultimately contributing to the Online Safety Act[4] and the specific focus within the UK on "legal but harmful" issues like self-harm and suicide content.

EUROPE: THE FIRST PHASE OF LEGISLATIVE REFORM

In Europe, concerns over content moderation and online safety have formed part of a broader debate about the role of large American technology companies and their impact on Europe's economy and society. This has included concerns around data protection practices, antitrust and market dominance, and the ethics of artificial intelligence. Following the decline of European handset providers like Nokia in the late 2000s, the absence of major European competitors has reinforced policy concerns about a lack of control over technology companies, contributing to the so-called "techlash". This helps explain why Europe has moved earlier and harder in online safety regulation than most other parts of the world.

Online safety regulation in Europe has broadly occurred in two phases. The first was primarily focused on the removal of illegal content within set time periods, reflecting the e-Commerce Directive's focus on illegal activity rather than a broader "good Samaritan" clause. The most notable of these was Germany's Network Enforcement Act (NetzDG)[5] in 2018, which introduced obligations on platforms to remove illegal content within certain time periods. This was followed by the EU's Regulation to address the dissemination of terrorist content online[6] which obliged platforms to remove terrorist content at the latest within one hour of the receipt of a removal order from a relevant national authority. These powers were balanced by protections for free expression, including information and complaints rights for users, and the ability for platforms to seek judicial redress.

EUROPE: COMPREHENSIVE REFORM

The second phase of online safety regulation followed hot on the heels of the first and reflected an impatience with the limited nature of the first wave of legislation, both in its focus on content removal and on certain types of content. When publishing the initial version of the DSA[7], the European Commission argued that legislation was necessary because larger platforms were now "quasi-public spaces for information sharing" and that they were "systemic in nature"[8]. The Commission also argued that the legislation was not only necessary simply to deal with illegal content but of the risks online for "information flows and public participation", significantly broadening the scope for intervention beyond illegality.

The DSA and its legislative cousin, the UK's OSA, departed from previous rounds of reform by introducing a "systems and processes" approach. This was facilitated by the introduction in the DSA of a "good Samaritan" clause, thereby overcoming the legal ambiguity which had been cited as a barrier to proactive monitoring of illegal and harmful content on platforms in Europe. The purpose was less to specify what content should be taken down and how quickly (indeed, the DSA does not define illegal content), and more to put the onus on online platforms themselves to respond efficiently to enforcement notices and to put in place the internal processes to evaluate potential risks, the appropriate mitigation mechanisms, and avenues for redress for users where inappropriate decisions were taken.

Both laws make a distinction in obligations based on the size of companies and in the case of the DSA, "very-large-online-platforms" (VLOPs) face a range of obligations in areas such as disinformation, risks to democratic processes and "manipulation during pandemics". While the obligations in these areas differ from those for illegal content – risk assessments rather than responding to take down notices – these provisions marked a significant expansion in the scope of online safety law.

At the time of writing, both laws have yet to be tested in practice, though this has not prevented them from becoming significant points of tension with the new Trump administration. In the case of the OSA, it has yet to be fully implemented with core pillars of the legislation, such as on child safety, not coming into effect until July this year. The DSA is the more advanced of the two with its provisions having fully entered in force and with the Commission having undertaken initial enforcement activity. Whilst these have largely been restricted to requests for information, there are two live cases involving American companies, against X and Meta[9]. The former was found in breach of the DSA in the Commission's preliminary findings in July 2024, most notably on matters of transparency of information to users and researchers. With the case set to conclude soon, the Commission asked in January for yet more information from X looking at how its algorithm selects content, amidst allegations that it is unfairly promoting far-right accounts. With Meta, the investigation includes whether it has effective mechanisms for flagging illegal content. The length of time taken to investigate these cases has been the subject of increased criticism from Members of the European Parliament (MEPs)[10].

US: STATES DRIVING POLICYMAKING

In the US, the evolution of online safety debates has charted a different course, reflecting the fact that most large technology companies are American, as well as a political and media culture which has focused on upholding free expression online, grounded in the First Amendment to the US constitution. While this debate has also arisen in Europe, provisions to uphold free expression, such as the DSA's right for user appeals and the OSA's protection of political and journalistic content, were embedded within online safety legal frameworks rather than acting as a barrier to them being implemented in the first place.

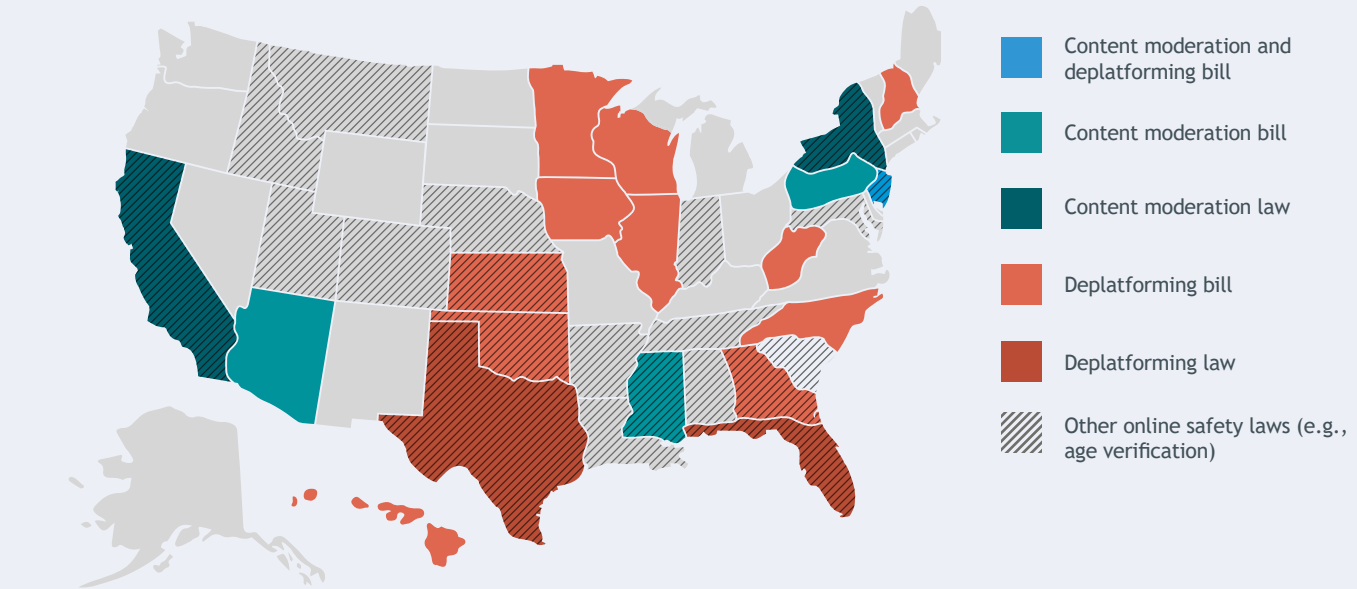
Like Europe, the US has witnessed a series of major controversies over online safety, including the leaking of internal Meta documents by Frances Haugen on the mental health of teenagers. However, this has yet to translate into federal online safety legislation. Indeed, where online safety has been invoked, it is often merged with online privacy discussions. This dates back to the Children's Online Privacy Protection Act (COPPA)[11], one of the first federal efforts to regulate children's digital privacy and which was updated in 2013[12]. COPPA provides a number of privacy related protections for children operating online, including the need for online services to have a privacy policy describing their practices related to collection of children's data and the need for parental consent before collecting children's data. COPPA was the basis on which the Federal Trade Commission (FTC) has launched cases against social media companies like TikTok and Facebook[13].

> *COPPA has been in place since the 1990s and, while it's enforced by the FTC, we've only seen a handful of enforcement actions over the years."*
>
> **CIVIL SOCIETY**

This picture was dramatically altered by the deplatforming of President Trump after the attack on the US Capitol in January 2021, most famously from Twitter (now X). This was perceived by Trump, conservative commentators and many Republicans as an overreach by technology companies and they argued for legal protections against deplatforming. While this reflected similar concerns in Europe about a perceived lack of process and transparency over tech companies' moderation policies, it took on a distinctly partisan texture in the US. Laws were quickly adopted by Republican-led states, such as Florida and Texas (SB7072[14] and HB20[15] respectively), which placed limitations on the ability of technology companies to remove political accounts.

Both laws faced legal challenges which saw

FIG 1: US state laws: an increasingly fragmented landscape



contradictory judgements on their validity at lower circuit courts, prompting the US Supreme Court to consider whether their provisions were consistent with the First Amendment. The Supreme Court – while not taking a definitive[16] decision – asked the lower courts to re-evaluate their decisions, though the implication of the judgement was that technology companies should retain their First Amendment rights to remove content and accounts which they do not wish to host.

As shown in Fig 1, state laws in the US are not limited to the issue of deplatforming with a majority of US states having passed or considering passing content moderation or online safety laws, ranging from age verification requirements to, as in the case of California's AB 2273[17] or Maryland's "kids code"[18], compliance requirements where services are likely to be accessed by children. Several of these laws are being legally challenged by industry associations and this remains their primary response to state-level regulation. The growing legal fragmentation has not yet reached the point where industry falls behind federal level legislation as a harmonised legal alternative.

TRANSATLANTIC TENSIONS

With the advent of the second Trump administration, there is a growing transatlantic gulf not only because of the divergent legislative starting points between Europe and the US, but also in ideological attitudes towards content moderation. While the policy thrust of the Trump administration has been unsurprising, as has its desire to more assertively contest EU technology regulation, the stark and abrupt rhetoric of JD Vance, Brendan Carr, Elon Musk and others has catapulted online safety policy to the top of transatlantic relations.

This will undoubtedly shape considerations in Brussels and London as further measures are considered. As noted above, it has already sparked a debate within Brussels on the pace of implementation of the DSA and major enforcement cases, though the European Commission has been at pains to deny any change of approach publicly. Likewise, in the UK, Peter Kyle, Secretary of State for Science, Innovation and Technology, has acknowledged that content moderation policy has become "politicised"[19], though he insisted it would not lead to watering down of the implementation of the OSA. The following chapters assess the extent to which this dynamic, and other factors, will shape the prospect for further reforms in the coming years.

ISSUE	OSA	DSA
Scope	User-to-user services and search engines accessible in the UK	Intermediary services, hosting services and online platforms
Regulatory Body	Ofcom	European Commission for VLOPs and very large online search engines (VLOEs); national Digital Services Coordinators for other companies
Platform categorisation	Category 1 companies: → Platforms with more than 7m users that use content recommender systems and allow users to reshare content → Larger platforms (34m+ UK users) with content recommender systems	VLOPs and VLOEs (45M+ users) must comply with additional transparency, risk assessment, and independent audit requirements
Fines for non-compliance	Up to £18 million or 10% of global revenue, whichever is higher	Up to 6% of global annual turnover for VLOPs and VLOEs
Transparency requirements	Annual transparency reports	All services must produce an annual report; VLOPs must record content moderation decisions in transparency database
Measures Against Illegal Content	Mandatory removal of illegal content (e.g., terrorism, CSAM)	Online platforms must remove illegal goods, services and content "expeditiously" once notified
Duty to Protect Children	Services must assess any risks to children from using their platforms and set appropriate age restrictions	Obligations on platforms to conduct impact assessments including on the fundamental rights of the child; a ban on targeted advertising to children
Artificial Intelligence (AI)	No specific AI related measures	Requires transparency in AI-driven moderation and recommendation systems
Misinformation & Disinformation	Direct provisions are limited beyond establishing a committee to advise Ofcom	Risk assessment and mitigation obligations for VLOPs and VLOSEs in areas such as disinformation, democratic processes and “manipulation during pandemics”
Age Verification	Requires age verification for pornographic platforms and those which host adult content	Age verification is a potential risk mitigation measure to protect children referenced in the DSA
Protections for Free Speech	Platforms must consider freedom of expression in their safety policies and protect content of "journalistic importance"	Rules protecting media content is covered in the European Media Freedom Act
Appeals	Platforms are required to implement clear and transparent complaints procedures	Internal complaint-handling system of platforms which can be referred to out of court dispute settlement bodies

Protecting children

Legislative reform and novel regulatory interventions to protect children online are likely in the medium-term, driven by widespread public concern over child protection. This applies across the EU, UK and US, though the exact form will differ, reflecting different legislative frameworks. There are three main areas where policy is likely to focus: age verification, restrictions on under 16s accessing online services, and measures to combat the addictiveness of apps and websites. The political salience of children's safety means that it is less likely to be impacted by the backlash from the Trump administration against content moderation than is the case for other policy areas, such as misinformation and "legal but harmful" content.

WHAT BUSINESSES SHOULD EXPECT

INCREASED SCRUTINY - Both reputational and regulatory - of corporate age verification policies and technologies.

US - Renewed attempts to pass federal legislation while an increasing number of states pass legislation to protect children online.

EU - A greater focus on child protection, including measures to tackle online addictiveness as part of the DFA.

UK - A series of OSA enforcement cases and a notable chance of new legislation limiting online access for under 16s.

What the public think

Public reaction when asked about children online was strong and emotional. Immediate associations were with risks and safety concerns (see Fig 2), a clear driver in putting children at the heart of political debates on online safety. Across all markets surveyed, over half of the public ranked online predators targeting children as a top three concern and other concerns associated with children, such as cyberbullying, ranked highly (see Fig 3). While there were some variations in attitudes between different demographic groups – for example, American women (58%) were more likely than men (49%) to have concerns about online predators – there was a broad consensus across different voter segments about the need to prioritise children.

> *When I think about what I am concerned about, children pop into my mind. Growing up with technology, children… can look up anything online without any regulation."*
>
> **UK PUBLIC**

When considering the appropriate policy response, a clear majority supports robust age verification measures even when these require the collection of sensitive details, such as photographic and other personally identifiable data. In the UK, for example, this received the support of 79% of the public (see Fig 4). However, it was notable that interventions like restricting access to phones in schools, while claiming majority support, gained less support than a range of other online safety initiatives (see Fig 6). This potentially reflects the nuanced debate on the issue and the fact that even child safety non-governmental organizations (NGOs) have mixed views on the initiative, citing the importance of phones for communications between children and their parents.

What the policy community thinks

The UK finds itself in a paradoxical situation, having the most advanced legislative framework with a duty of care to protect children enshrined in the OSA, but a contentious debate on introducing new measures before these provisions have been implemented and enforced. Relatively low levels of public awareness of the OSA may be a contributory factor in explaining this sense of impatience (see Fig 5), as well as a number of high profile tragedies involving British teens like Molly Russell and Brianna Ghey.

FIG 2: Safety is front of mind when thinking about children online

15 MOST FREQUENTLY ASSOCIATED WORDS AMONG ALL FRENCH RESPONDENTS

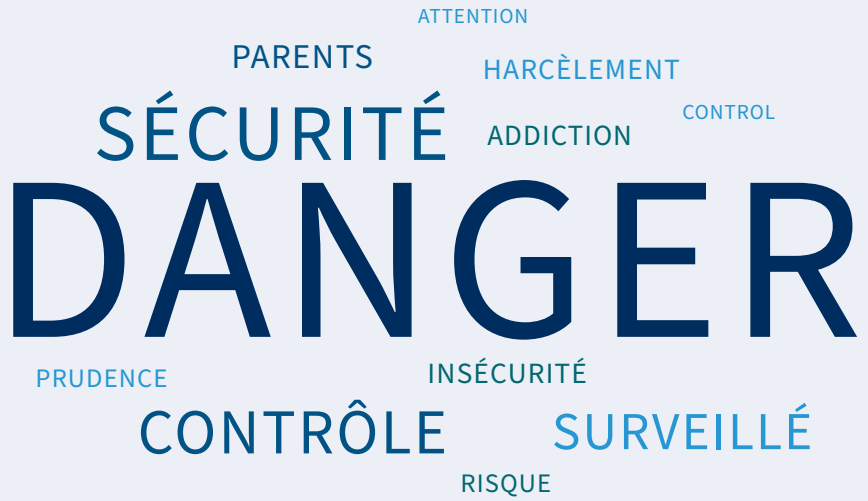
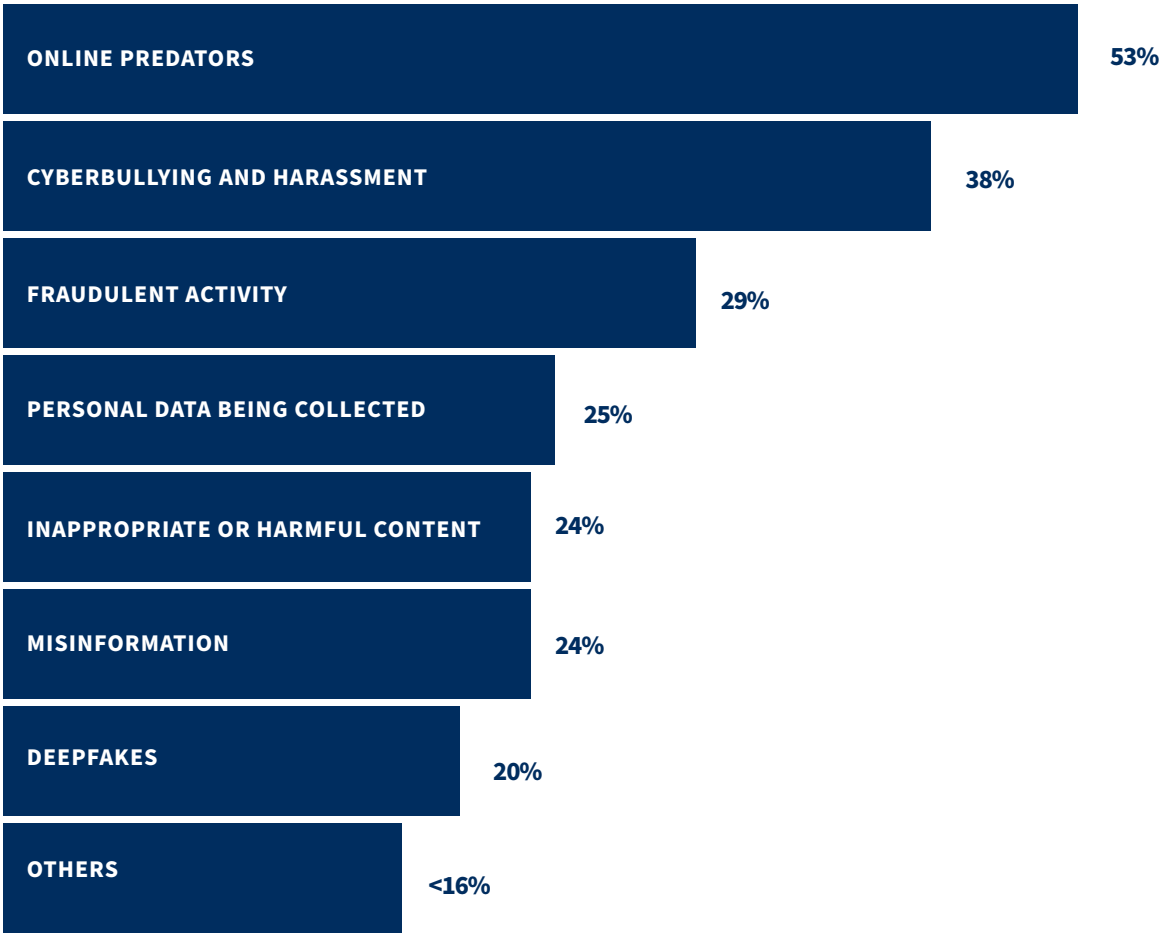


FIG 3: Protecting children is the key concern for US adults

% OF US RESPONDENTS SELECTING EACH AS A TOP THREE CONCERN



[In Australia] it was quite a last minute decision to carve out gaming, messaging and video sharing services. I'd be interested to see how that kind of rationale works out."

REGULATOR

Interviews revealed an emerging split between politicians on the one hand and officials in regulators and government departments on the other. With the former, there is momentum behind new restrictions on under 16s and their access to online services. This could be via a ban on access to phones in certain settings, such as schools, or by limiting under 16s access to social media through either raising the digital age of consent or a more specific restriction specific to social media.

To date, this energy has been channelled into a private members bill from Josh McAlister MP[20]. While the bill has since been stripped back, due to a lack of support from the government and McAlister's own elevation to a government role, interviews suggested that raising the age of digital consent would have enjoyed support from a number of Labour MPs. The government has since launched the Whitty review[21] to assess whether to raise the digital age of consent. Meanwhile, the opposition Conservative Party has proposed a ban on smartphones in schools[22].

I am not aware of any evidence from countries like Ireland, which have a digital age of consent at 16, that have better protected children."

REGULATOR

In contrast, officials in regulators and government were at pains to emphasise that the OSA's provisions to protect children online should be introduced before considering further restrictions. Some of the objections raised were practical, with many seeing Australia's under 16s ban as a litmus test, particularly in how services such as YouTube and gaming platforms are out of scope. Others pointed to countries where the digital age of consent is 16 rather than 13, to argue that there was no noticeable improvement in the level of protection for children there. Other objections were more principled, including concerns about treating young children the same as teenagers, while some stakeholders were quick to argue that blanket prohibitions would mean losing many of the benefits of children interacting online. One area where all stakeholders agreed on the need to make progress was on age verification, both under the OSA but also other legislation like the General Data Protection Regulation (GDPR) and its Age appropriate design code[23].

There was disagreement, however, on whether the technology existed at this stage for this to be widely and successfully implemented across platforms.

In the US, the starting point for protecting children at the federal level is significantly more fragmented and limited than in Europe, despite bipartisan support for measures to enhance protection for children. "Protection" is also interpreted differently by policymakers, focusing as much on enhancing privacy standards as on managing the content children can access, see and experience online.

> *Policymakers find it easier to rally support for protecting kids because opposing it isn't a good look politically. But this focus can lead to rushed or overbroad legislation."*
>
> **CIVIL SOCIETY**

FIG 4: There is strong support for age verification

% OF UK ADULTS SAYING WHICH STATEMENT COMES CLOSEST TO THEIR VIEW

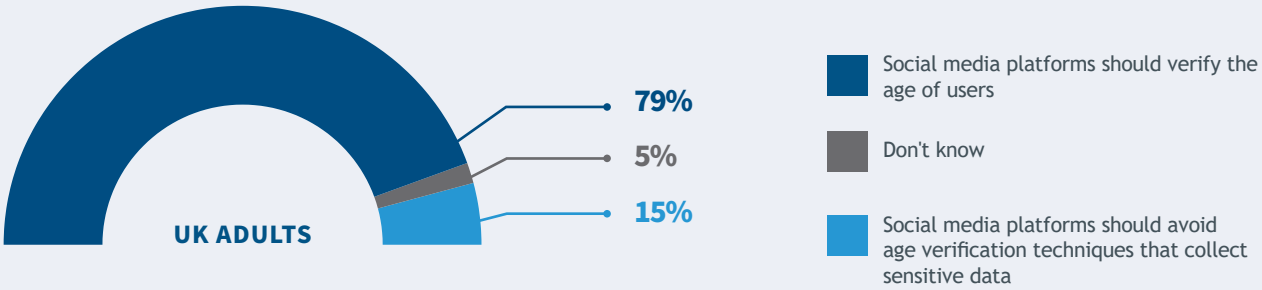


FIG 5: Only the GDPR is well known by the UK public

% OF UK RESPONDENTS THAT ARE FAMILIAR WITH EACH PIECE OF ONLINE REGULATION

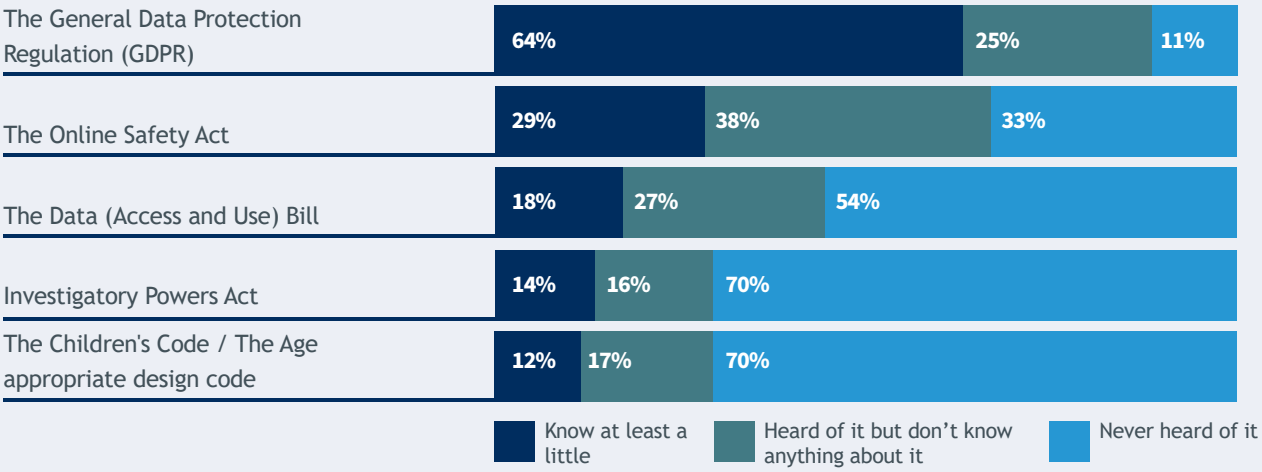
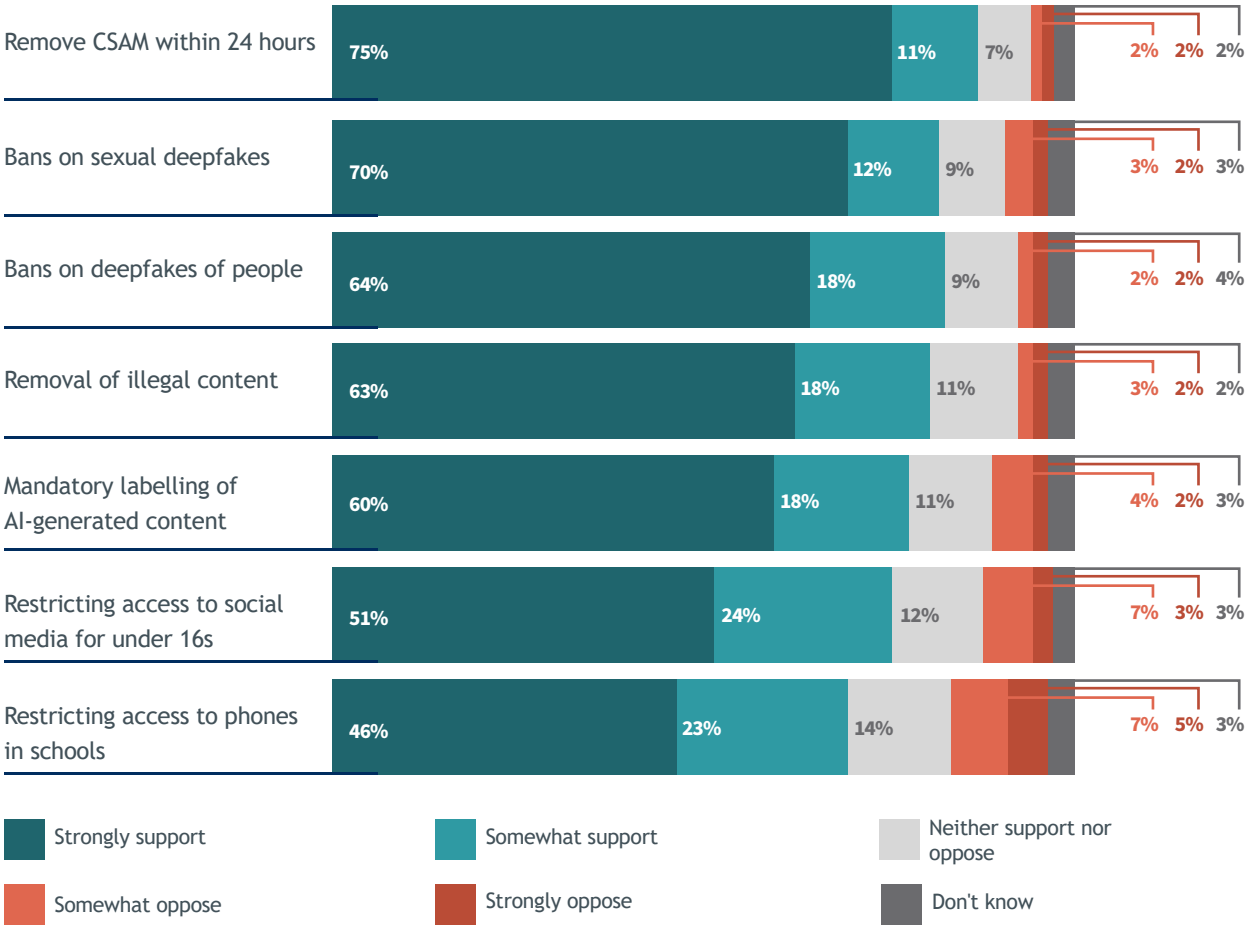


FIG 6: Under 16 bans are less popular than other measures

% OF US RESPONDENTS THAT SUPPORT OR OPPOSE EACH INITIATIVE



Interviewees made it clear that despite failed attempts in recent years to pass new legislation there remains sufficient political momentum behind reform. This finding is consistent with the high levels of public concern shown in our survey of the US public, though some argued that the debate is verging on "moral panic". Further attempts to pass bills at the federal level are likely but their success will depend on the proposed scope, with a desire to avoid the legal challenges seen by many states when passing children-focused legislation, most notably conflicts with First Amendment protections and Section 230. Given this context, future legislation may follow a narrower approach, similar to the REPORT Act[24], which successfully became law by focusing specifically on reporting requirements for CSAM online, rather than a much broader "duty of care" concept that was included in the Kids Online Safety Act (KOSA)[25].

There is a varied landscape at the state level with a number of laws which, while they do not contradict each other, are far from uniform and are contributing to an increasingly fragmented landscape. Stakeholders felt that this trend is likely to continue despite a number of legal challenges that state-level laws, such as California's Age-Appropriate Design Code and Maryland's Kids Code, are having to navigate. Interviewees speculated that might change in the event of a negative ruling for a state in a major test case.

> *Unfortunately, in some states, there's an attitude of "Let the courts sort it out," which wastes taxpayer money defending laws likely to be struck down."*
>
> **ACADEMIC**

While there is a bipartisan consensus on the need to enhance protection of children online, there are some emerging differences in the types of online safety legislation that are being pursued in states with Democratic versus Republican majorities. For example, an amended version of the Age-Appropriate Design Code (AADC) passed in Maryland in 2024, with similar proposals introduced in Democratic-majority states such as Hawaii, Minnesota, Illinois and Vermont. In contrast, Republican-led states are advancing age verification mandates for all users and parental consent requirements for younger users, as seen in Tennessee and Kentucky. Device filtering proposals, which require default content filters on smartphones and tablets, have typically been introduced by Republican lawmakers, with Alabama and Idaho being recent examples.

In Brussels, there has been less of a focus on child protection than in the UK or the US, with the DSA having a less overt focus in this area than the OSA. This has prompted criticism from some policymakers that child protection is not being sufficiently prioritised by the EU institutions. To some extent, this reflects a split between the EU-level on online safety – setting the broader frameworks for tackling illegal content – and national level where individual member states have, much like the UK, moved forward with their own legislative approaches. The most notable of these is France's 'digital majority' law[26] which obliges social media platforms to verify the age of users and to obtain parental consent for under 15s. Policy approaches on the use of smartphones in schools are being determined at a national and regional level rather than in Brussels, with restrictions introduced in Denmark, France, the Netherlands and Bavaria, but other jurisdictions like Estonia deciding against mandating such an approach.

> *We are obviously concerned about the addictive design of online platforms, in particular I worry that we do not yet properly understand the role of algorithms in pushing certain types of content."*
>
> **EU OFFICIAL**

There are, however, some signals that child protection is moving up the agenda within the European Commission, with President von der Leyen having committed to launch an EU-wide inquiry into the impacts of social media on young people. New measures will likely be funnelled through the DFA initiative which is intended to introduce measures to tackle the perceived addictiveness of some online platforms, as well as to introduce regulations around the role of online influencers. There remains a question of how such measures will interact with the ongoing tensions with the US on technology regulation, given large US technology companies will be at the coalface of these new regulatory initiatives. The timing of the DFA has been delayed till 2026, potentially a nod to this dynamic, and it is unclear the extent to which this might prompt further delays and changes in the scope of this new law.

Misinformation

Transatlantic tensions are most evident in misinformation policy, making the passage of new legislation unlikely in the near term, either specifically on misinformation or on wider "legal but harmful" content. This is reinforced by the divergence of views domestically within Europe with political persuasions shaping public opinion more than is the case for other online safety topics. The focus of policy activity will therefore concentrate on enforcement of existing legislation, most notably the DSA. The approach of European regulators will likely be one of caution in the near term, though this could shift depending on the evolution of relations with the US.

WHAT BUSINESSES SHOULD EXPECT

Competing expectations of, and potentially legal obligations on companies from American and European policymakers.

US - While there is no prospect of misinformation laws, new proposals at state level on algorithmic management can be anticipated.

EU - Ongoing controversy over the pace, scale and outcome of DSA enforcement cases.

UK - A growing debate over "legal but harmful" content, including misinformation, with a slim chance of legislative reform.

What the public think

The spread of misinformation online is a notable, though not top tier, issue for the public with between a fifth and quarter having ranked it in their top three issues. The highest proportion citing this as an issue is in the UK (27%), the lowest in France (21%). However, it is notable that even in the US, concerns about misinformation were ranked significantly higher than the concern for the erosion of free expression online (24% and 7% respectively): a striking result given the arguments from the Trump administration and leading Republicans that free expression is being imperilled by online content moderation rules. This could perhaps be explained by different views amongst the public about what constitutes misinformation.

I'd like to see government doing something about misinformation, but I don't know how likely they are to do anything about it. I think it is down to individual platforms to remove content that isn't real or accurate."

UK PUBLIC

When it comes to the appropriate policy response, the headline view of the public is that social media companies should intervene to prevent and remove misinformation, even if it means restricting some forms of content (see Fig 8). Beneath this headline conclusion there are a number of distinctions between geography and between political leanings. The UK saw higher levels of support, particularly compared to the US (75% vs 66% respectively). There were also unsurprisingly differences between supporters of political parties with right-leaning voters - Reform in the UK, Trump in the US and Rassemblement National in France - all showing higher levels of support for free expression than more centrist and left-leaning voters, with one in four Reform voters prioritising free expression above misinformation.

These differences in geography and political leanings were also evident when exploring which institutions and actors should be trusted to remove online misinformation. The UK and to a lesser extent France saw high levels of trust in the independent regulator and in law enforcement, while the US saw comparatively higher levels of trust in technology companies. Interestingly, in light of recent debates on community notes systems, such as those on X and planned by Meta, the US public were notably more comfortable with users playing a role in policing misinformation than their British peers (see Fig 7).

FIG 7: US adults are more trusting of other users

% OF RESPONDENTS SELECTING COMFORT OF INDIVIDUAL PLATFORM USERS BEING RESPONSIBLE FOR REMOVING ONLINE MISINFORMATION

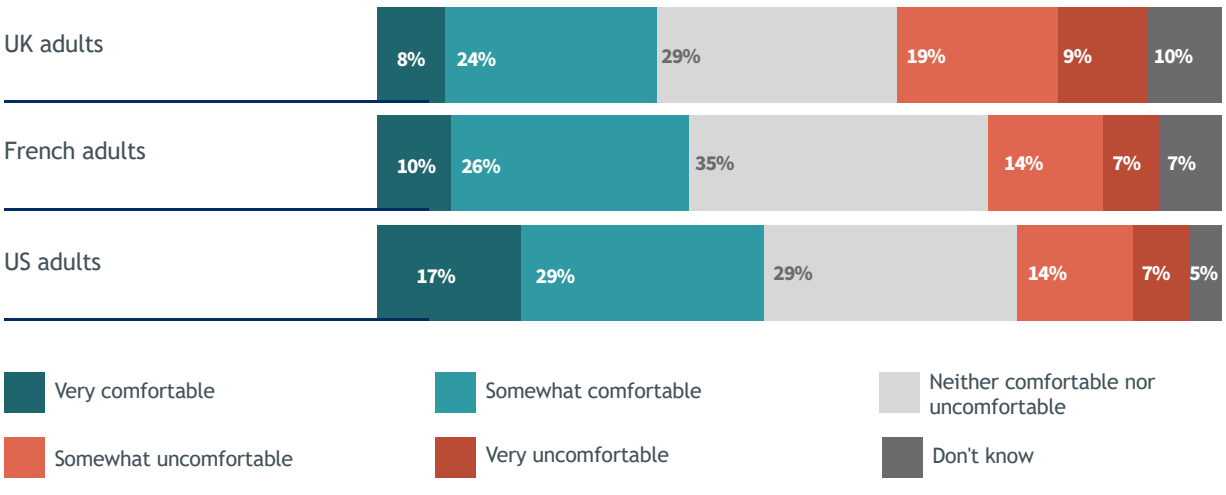
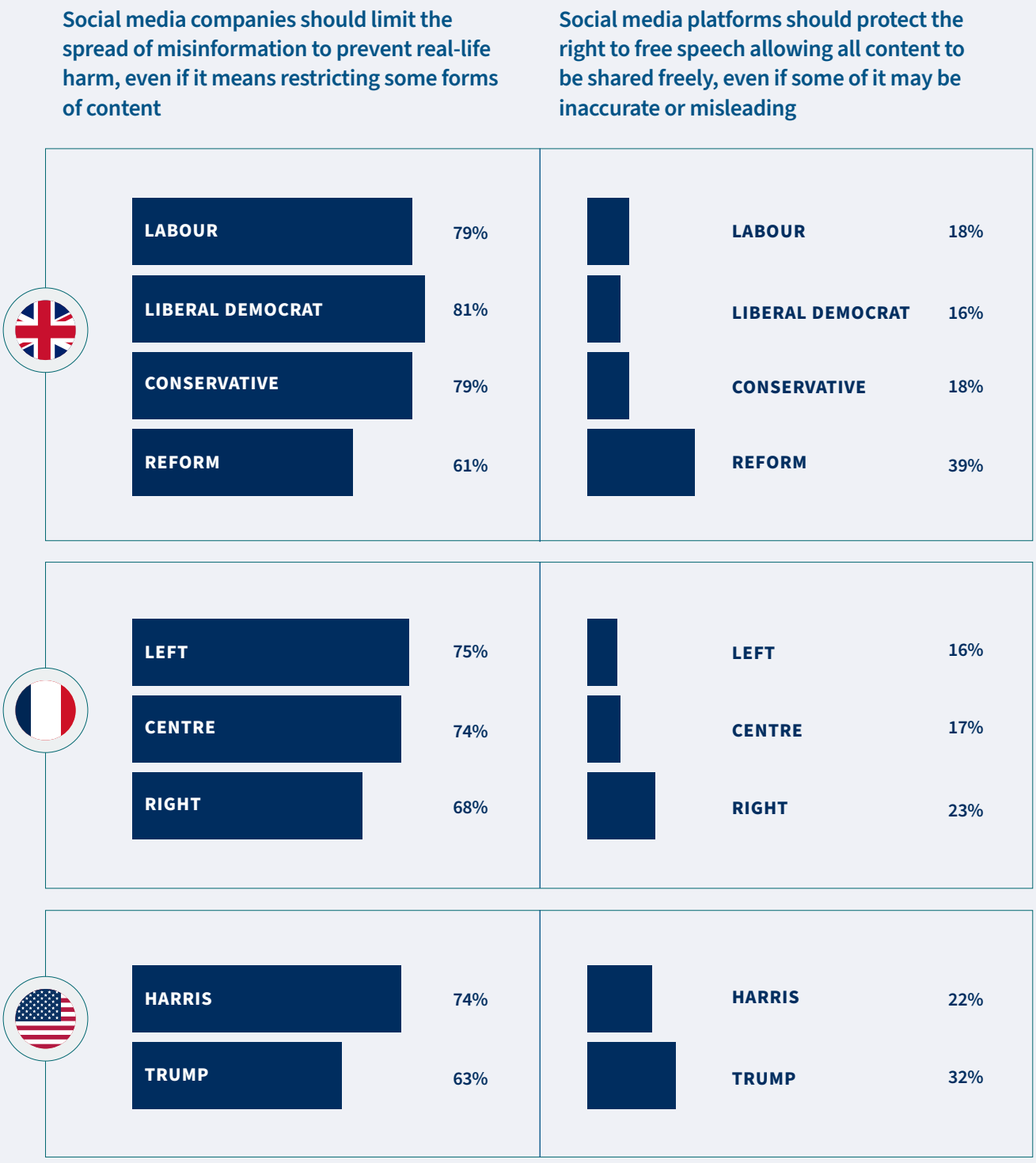


FIG 8: Right-leaning voters prioritise free expression more than other groups

% OF EACH VOTER GROUP SAYING THEY ARE MORE LIKELY TO AGREE WITH EACH STATEMENT



What the policy community thinks

Despite public support to act, there is a sense across the US, EU and UK that political momentum to address online misinformation is fading. Indeed, the question in the next political cycle appears to be less whether we will see new laws on misinformation and instead whether we are likely to see a reversal in policy or, perhaps more likely, a more cautious use of enforcement powers. As hinted at in the public surveys, this reflects the fact that views on misinformation are informed by political outlook and allegiance in a way which is less evident in other aspects of online safety policy.

Nowhere is this more apparent than in the US. Interviewees were quick to point out that there has never been a serious prospect of laws on misinformation at either the federal or state levels due to the protections for free expression under the First Amendment, and the willingness of industry associations to launch legal challenges on this basis. This dynamic has been reinforced by the second Trump administration and the alignment between the US government and a number of technology companies, seen most notably in the role of Elon Musk and the content moderation changes announced by Meta in January.

Due to the absence of misinformation laws in the US, conservative pushback against this form of content moderation has focused on corporate content moderation policies and the accusation of "coercion" by the federal government on technology companies, particularly during the pandemic. Towards the latter, this took the form of legal challenges by the attorney generals of Louisiana and Missouri, both Republican-led states, who argued that there should be limits on the interactions between the Biden administration and technology companies to avoid coercion to limit free expression. While their case was ultimately rejected by the Supreme Court, President Trump has since issued an executive order (EO) stating that "the previous administration trampled free speech rights by censoring Americans' speech on online platforms…under the guise of combatting "misinformation."[27] The EO directs federal employees to avoid unconstitutionally "abridge[ing] the free speech of any American citizen" and for the Attorney General to investigate the practices of the previous administration.

> *The Trump Presidency will increase divergence between the EU and US on online safety… we should always remember that the most important market for US corporations is the US."*
>
> **POLICY OFFICIAL**

At state level, there has been a shift in focus of legislative activity, in part to navigate the constraints imposed by the First Amendment. This has included looking at product design and algorithmic management rather than a specific focus on the content moderation of misinformation. One example – albeit with a children's protection focus – is New York's SAFE For Kids Act[28] which places limits on the curation of social media content to avoid content being directed to children without parental consent. While some interviewees argued that focusing on design rather than content moderation was a sensible approach, others raised concerns that even this is being challenged by industry groups and could, depending on the outcome of legal test cases, have a chilling effect on legislation.

> *If we reach a point where even product design cannot be regulated… we're entering a scenario where it becomes nearly impossible to implement any form of regulation."*
>
> **CIVIL SOCIETY**

While the impact of the Trump administration on the domestic debate regarding misinformation has been notable, its true significance has been in the ambition to export this approach to other jurisdictions, especially in Europe. This has been seen in recent speeches from Vice President JD Vance in Paris[29] and remarks from Brendan Carr, Chair of the Federal Communications Commission, at Mobile World Congress criticising the Digital Services Act[30]. In Brussels, this pressure has added to the already pessimistic view of policymakers about misinformation. While most identified this as a priority area of concern,

especially when considering disinformation or foreign information manipulations and interference (FIMI), there was a sense of impotence in the EU's ability to tackle this challenge. Many stakeholders expressed scepticism over the upcoming Democracy Shield and argued it was unlikely to add considerably to existing measures like the EU Electoral Coordination Committee and Rapid Alert System.

The US elections are a turning point - disinformation is no longer just about foreign digital interference but also about organic content."

POLICY OFFICIAL

Interviewees stressed their concerns about the Commission's enforcement of the DSA, echoing the public concerns of MEPs in recent months, arguing that it has proved less effective than anticipated at stemming misinformation. Central to this complaint is the slow pace of investigations launched by the Commission and the paucity of investigations, though it should be noted that similar complaints were made about the GDPR after its entry into force. Other concerns flagged by stakeholders include the capacity and resources of the Commission for effective enforcement, and limited funding and political support for trusted flaggers. In line with wider calls to simplify the EU's complex tech rulebook, interviewees stressed the numerous overlapping requirements of the DSA, European Media Freedom Act[31], AI Act[32] and Code of Practice for Disinformation[33]. This complexity was framed as a central obstacle to effective compliance, enforcement and European competitiveness.

The UK has also been subject to criticism from the US administration on its approach to misinformation including when JD Vance raised "infringements on free speech" with Prime Minister Keir Stamer during his visit to the White House in February[34]. The criticism from the US is on the one hand counter-intuitive since the OSA includes few explicit provisions on misinformation aside from the obligation on Ofcom, to establish an advisory committee on misinformation.

However, as some interviewees highlighted, there are a number of other obligations introduced by the OSA which could be applied to limit the spread of misinformation. These include the creation of a new offence of knowingly spreading false information which is intended to cause "non-trivial psychological or physical harm to a likely audience"[35], a charge which was used by law enforcement in response to riots in August 2024. However, the application and potential limits of this offence are yet to be fully tested in courts, especially how to determine whether a person knows that the information they are sharing is false and, even if they do, establishing the level of intent to cause harm. A further potential flashpoint between the UK and US on misinformation will be the introduction of rules for categorised companies to apply their terms and conditions consistently, with Ofcom likely to consult on the issue at the start of 2026. Depending on the outcome of this consultation, these powers could in principle be used to enforce against technology platforms where they fail to take action against misinformation on their platforms.

The false communications offence was introduced recently, but it hasn't yet been really tested in the courts whether it will be able to deal with somebody domestically posting harmful misinformation."

REGULATOR

US pressure does reinforce the likelihood that the UK will not move forward with a major revision of the OSA in this political cycle. In opposition, the Labour Party had suggested an openness to revising the OSA and strengthen the provisions on "legal but harmful" content (of which misinformation would be one variety). While many interviewees highlighted this aspect as a notable gap, there was widespread scepticism about the prevalence and impact of misinformation during the 2024 general election. One legislator expressed concerns about whether Ofcom or another body would have the authority to be an arbiter on misinformation, not least under pressure from the US administration and technology companies.

AI generated content

Despite a sense that the risks from AI generated content have so far failed to materialise, this is an area with a surprising degree of policy consensus and a high likelihood of new rules coming into force in the next few years. This reflects public support for intervention and the fact that policy measures are primarily focused on transparency of content rather than moderation and removal. This consensus could, however, prove temporary should the strained transatlantic debate on misinformation be transposed to AI chatbots and other generative AI tools.

WHAT BUSINESSES SHOULD EXPECT

Increasing expectations on model developers to justify the answers given by chatbots and, in Europe, their independence from the perspectives of the US administration.

US - A continued focus on AI labelling and disclosures at the state-level, and potentially at the federal level as well.

EU - A focus on the practical methods of labelling AI content in order to implement the AI Act.

UK - Legislation to ban sexual deepfakes with a potential focus on labelling later in this Parliament.

What the public think

Deepfakes and AI-generated content online are a notable but not leading concern for the public, with between 18% (in France) and 23% (in the UK) having placed it as a top three concern (see Fig 16). The public's expectation is that existing regulation of AI is limited, reflecting the nascency of the technology.

For example, around a third of adults in all markets believe there is no current regulation relevant to AI generated content, which is both accurate in the sense that few jurisdictions have AI-specific rules, but misses that a range of pre-existing legislation and regulation applies to AI technologies. Likewise, in France over half of the public had either never heard of the EU's AI Act or claimed they had heard of it but did not know any of its details. This is perhaps unsurprising, given that the AI Act is yet to be fully implemented.

> *More recently, there is this whole deep fake thing that has come up with AI and that is definitely worrying, especially as a woman"*
>
> **UK PUBLIC**

On policy interventions, there is strong support from the public for targeted interventions to address the dissemination of AI-generated content online. One approach is the mandatory labelling of AI content, which saw a majority in support across all three markets, though with notable variation in levels support between the UK (71% strong support), US (60%) and France (52%) (see Fig 10). When this was tested in more depth, the public categorically supported a broad labelling requirement rather than limiting this to instances where reality was clearly distorted (see Fig 9). On more forceful interventions, such as bans on deepfakes and sexual deepfakes specifically, as the UK government is planning, the public was likewise supportive with over two thirds in all markets strongly supporting bans on sexual deepfakes and over half supporting bans of deepfakes as a whole.

What the policy community thinks

Following anticipation that 2024 – "the year of elections" – would be impacted and potentially shaped by generative AI and deepfakes, there was a broad consensus amongst the policy community that this did not materialise. Indeed, the role of social media and technology platforms and potential misuse of them for disinformation and misinformation was – aside from individual examples like Romania – not seen as a major factor in influencing the results, unlike or at least not more so than previous electoral cycles, most notably in 2016.

> *I don't think we saw much evidence from the elections that generative AI has shifted political debates."*
>
> **LEGISLATOR**

This is, however, not to say that policymakers are unconcerned, and some pointed to the experience of other jurisdictions like South Korea where policymakers have faced a much higher prevalence of deepfakes. The impact of AI-generated content on electoral processes and broader public discourse is seen as a major policy challenge that will need to be addressed in the coming years. Some interviewees highlighted the limited evidence base available to judge the prevalence of deepfakes and AI-generated content, highlighting how data from technology platforms for content removals was largely unavailable and that user surveys likewise had their limitations given the deceptive nature of deepfakes mean that they are often not identified as such by online users. Despite this, many argued that prevalence was increasing even if not to the extent predicted last year.

> *Generative AI is a powerful tool that has the power to disrupt democratic processes."*
>
> **POLICY OFFICIAL**

There was a 3,000% increase in convincing deepfakes across the financial services industry at the end of 2023. So it's a vast industry that's growing. And that sophistication is only becoming better over time."

FORMER GOVERNMENT OFFICIAL

Interviewees were concerned about how quick and easy it is to create content with generative AI and what this means for the changing profile of who is behind deepfakes. The original assumption has been that it would be mostly malign actors from hostile states. However, the lowering of the bar to entry has widened accessibility to create deepfakes, including for children. EU stakeholders were quick to point out how this also has implications for disinformation campaigns in that it more easily allows malign actors to overcome one of the central obstacles – the language barrier. Prior to generative AI tools, hostile actors found it difficult to obtain widespread reach for their disinformation campaigns, with linguistic mistakes often proving a sign of inauthentic content.

You're now in a situation where you're looking at super cheap influence operations."

FORMER GOVERNMENT ADVISOR

The policy response has fallen into three categories where approaches are broadly consistent between the EU, US and UK: evaluations of whether AI generated content is captured by existing legislation, proposals for labelling of AI content and bans of specific types of deepfakes.

On the question of scope, the debate in each jurisdiction has varied according to the unique features of each's legislative framework. In the UK, the OSA is targeted at "user-to-user services", which prompted a series of questions around AI-generated content both during the legislative process and into its implementation. Interviewees noted that Ofcom had been forced to confirm the circumstances under which AI-generated content is included, most notably when it is shared by users on user-to-user services. In the EU, there remains ambiguity around a number of use cases with MEPs and industry looking to gain clarification from the Commission, such as whether AI-bots should be considered in risk assessments by VLOPs. However, stakeholders noted that the challenge was less one around the scope as such – the responsibilities for VLOPs under the DSA are not constrained by the user-to-user concept of the OSA – and more, as noted in the previous section, about how the DSA aligned with the AI Act and the consistency in obligations faced by companies. In the US, interviewees speculated whether Section 230 protections applied or not for AI chatbots, with most arguing that this will likely need to be resolved in court.

FIG 9: The public support default AI labelling

% OF FRENCH ADULTS SAYING WHICH STATEMENT COMES CLOSEST TO THEIR VIEW

If a chatbot generates harmful or misleading information, responsibility likely falls on the company operating the system. Whether Section 230 shields them in these cases is still an open legal question."

CIVIL SOCIETY

On labelling, the US has moved fastest in introducing rules around disclosures of AI-generated content. The Biden administration's AI executive order charged the National Institute of Standards and Technology (NIST) with bringing forward content authentication standards and guidance for federal agencies, though it is unclear if this will remain a focus under the Trump's administration's AI Action Plan. At state-level, over 20 states have passed or considered legislation, with notable examples including Washington's SB 5152, Michigan's HB 5141 and Hawaii's SB 2687. The rush of laws was prompted by the 2024 elections and a desire to ensure transparency requirements on candidates ahead of November. This in turn means that those laws are mostly focused on electoral content rather than wider applications of AI labelling. Notably these laws were proposed across both Democrat-led, Republican-led and split legislatures, indicating a greater bipartisanship compared to topics like misinformation.

In Europe, Article 50 of the AI Act introduces obligations on all companies to inform users when they are interacting with an AI system and stresses that synthetic content (like deepfakes) must be disclosed to users. Whilst there is agreement on the need for transparency around AI-generated content, there remains fierce debate over the technical tools that should be employed to meet this obligation, risking fragmentation across the market and "labelling fatigue". Moreover, interviewees expressed concern about the effectiveness of content labelling as a tool to improve online safety, arguing that large technology companies need to invest in labelling and that there is not currently the impetus to do so. Labelling is one area where the UK debate lags behind other jurisdictions, despite a number of policymakers expressing support for some form of labelling regime, though at the time of writing the government is consulting on labelling as part of a wider initiative on AI and copyright rules.

Labelling would be a better route than outright banning deepfakes."

LEGISLATOR

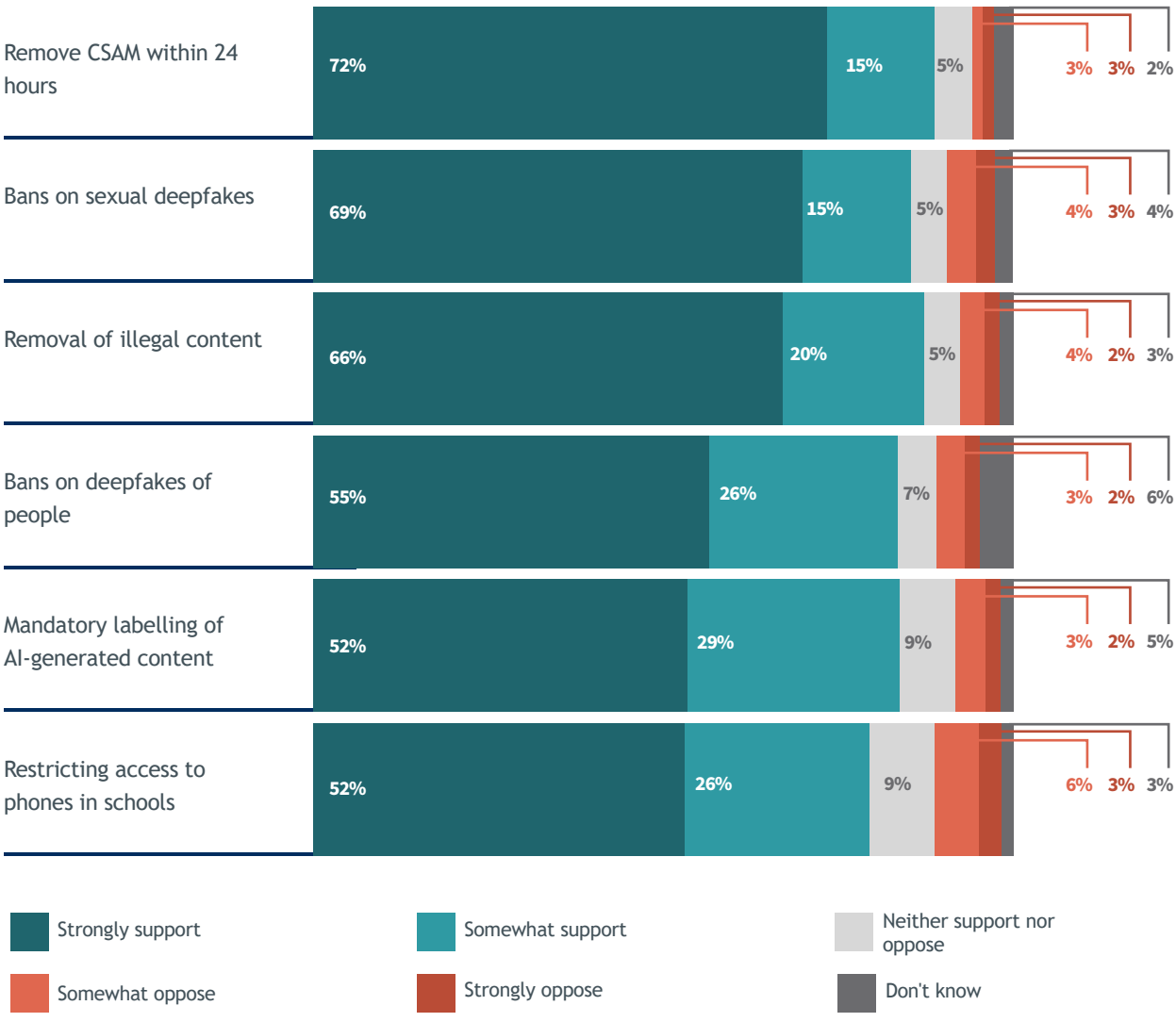
On proposals to ban deepfakes or specific types of deepfakes, the UK is bringing forward criminal offences for both creating and sharing sexually explicit deepfakes in the Crime and Policing Bill[36], which will in turn place responsibilities on technology platforms to prevent its dissemination via their illegal content obligations under the OSA. At the federal level in the US, the Take It Down Act[37], a bill aimed at combating the spread of non-consensual intimate imagery, including AI-generated deepfakes by criminalising the distribution of such content, passed the Senate in February 2025 and has momentum to pass the House. In the EU, the non-consensual manipulation of images and fabrication of deepfakes by means of artificial intelligence, is covered by the Directive on Combating Violence Against Women[38], which complements the EU AI Act and defines such practice as a criminal offence, albeit it must be proven that such conduct is likely to cause serious harm.

There is one area of potential divergence in transatlantic policymaking. An alleged "liberal bias" in AI models has been a common conservative criticism in the US of generative AI chatbots and this was alluded to in the Trump administration's executive order on AI which stated, "to maintain this leadership, we must develop AI systems that are free from ideological bias or engineered social agendas."

There remains a notable likelihood that this will be developed further in the AI Action Plan expected later this year and this is already prompting alarm from EU policymakers. Several interviewees noted the US ownership of large AI models and their potential vulnerability to political pressure, and the impact this could have on the online safety and misinformation landscape.

FIG 10: There is strong support for bans of deepfakes

% OF FRENCH RESPONDENTS THAT SUPPORT OR OPPOSE EACH INITIATIVE



Encryption

The debate on encryption has ebbed and flowed over the past decade, often flaring up in response to specific safety incidents or public spats between governments and individual technology companies. There is not a consensus in favour of reform, meaning that new legislation is unlikely in the coming years with the potential exception of the EU's CSAM regulation. As seen recently in the case of the UK's Home Office, enforcement activity in this space has the potential to be caught in wider transatlantic tensions over technology policy.

WHAT BUSINESSES SHOULD EXPECT

US - Renewed congressional attempts to pass CSAM reforms but will face significant headwinds.

EU - There is an outside chance that the long stalled CSAM regulation could pass, albeit in a modified form.

UK - The prospect of enforcement activity under the UK's Investigatory Powers Act (IPA) remains contingent on the outcome of ongoing legal cases.

What the public think

The public have conflicting and sometimes contradictory views on encryption, without a clear consensus on the issue, reflecting the stop-start nature and nuance of this policy debate. This appears to be relatively consistent across all three markets.

I don't think there should be a blanket approach of monitoring everyone's messages. But I also think that if information was needed by an agency or government, and they can't access that because of encryption, then that is an issue."

UK PUBLIC

Linking back to the earlier section on protecting children, the public are instinctively concerned about the types of issues that are commonly linked to encrypted messaging services. Concern about online predators is universal and strongly felt, and a similar trend is seen when testing attitudes towards views on regulation of CSAM, with large majorities of over 8 in 10 respondents in favour of requirements to remove CSAM content within 24 hours of it being identified. A similar trend, albeit with marginally lower levels of support, is seen on removing other types of illegal content.

This does not necessarily translate to public support for reducing privacy protections via encryption and much depends on the way in which questions are asked. Some responses suggest the public are bullish in favour of online safety. When asked about the arrest of Telegram CEO, Pavel Durov, by French law enforcement in August 2024, 56% of the French public claimed to have heard about the case and 63% of that cohort supported the arrest (see Fig 11). Likewise, when given the choice between upholding privacy via encryption in the case of serious crimes, a majority of the public in the UK and France, and a plurality in the US supported access to encrypted services for law enforcement (see Fig 12).

In contrast, when the association with serious crime is removed, the majority of the US and British public support encryption over law enforcement access, as well as a narrow plurality in France (see Fig 13). Likewise, when the public were asked about the most important factors for choosing online messaging platforms, strong encryption practices were found to be the second most important factor for the public in France and the US after the ease of use and design of the app .

FIG 11: The French public support the arrest of Telegram's CEO

% OF FRENCH ADULTS WHO HAVE HEARD ABOUT THE CASE THAT SUPPORT OR OPPOSE ARREST OF TELEGRAM CEO

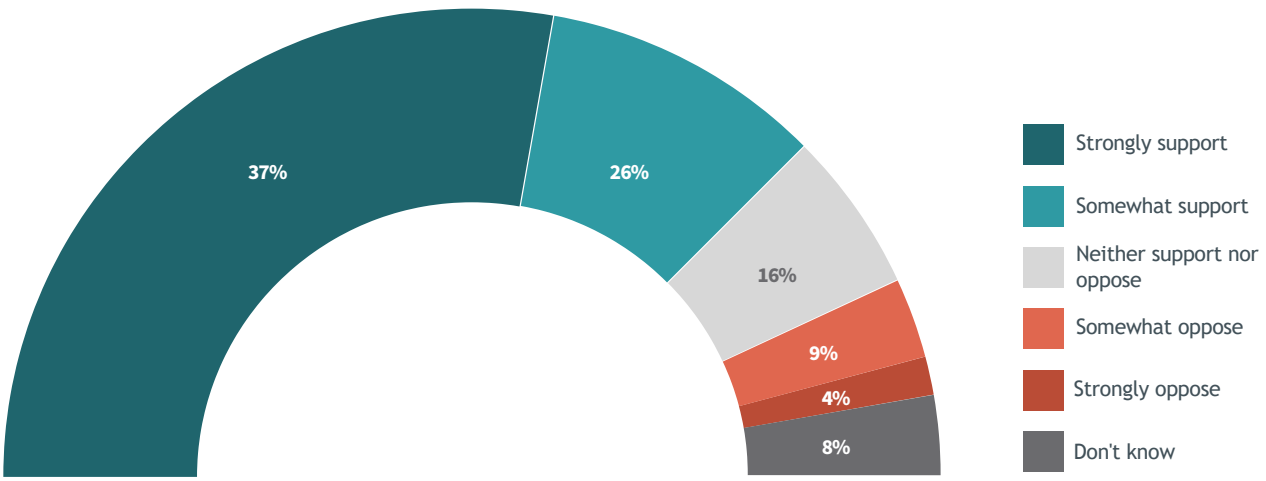
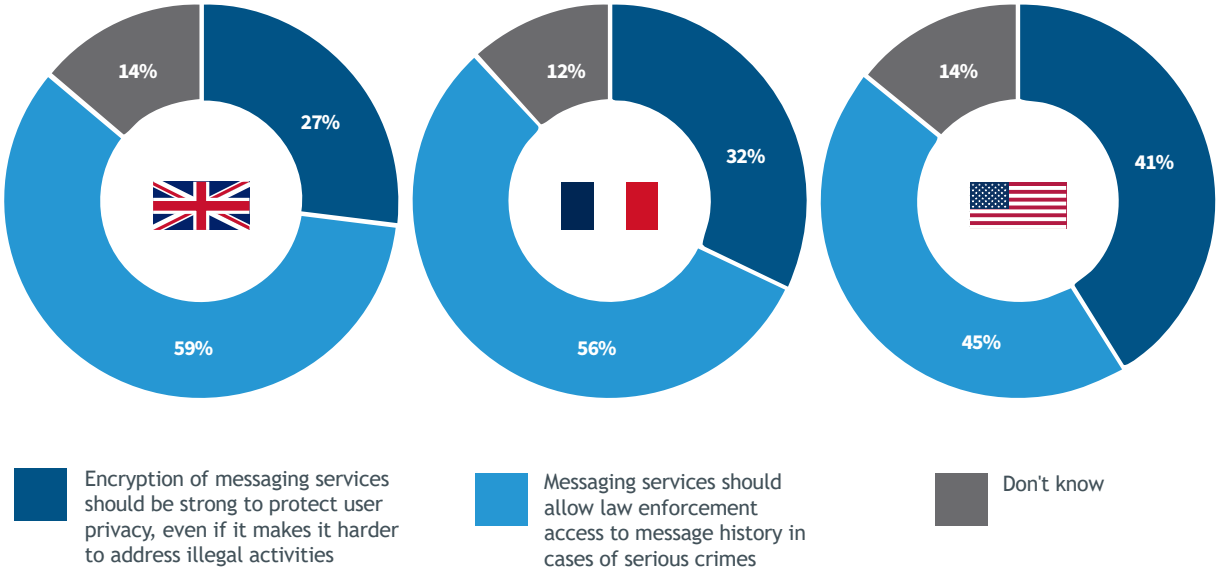


FIG 12: The public are more supportive of breaking encryption in cases of serious crime

% OF ALL RESPONDENTS SELECTING EACH STATEMENT AS CLOSEST TO THEIR VIEW



What the policy community thinks

There is equally a lack of consensus amongst the policy community with regards to striking the balance between encryption and online safety. This is unsurprising given the emotive debate on the topic, pitting security and child safety arguments on the one side and cybersecurity and privacy on the other. Some interviewees argued that the lack of "best in class" legislation globally made it a challenging area for policy formulation, with Australia's policy framework no longer seen as the potential model that it once was.

In the US, while encryption remains a contentious issue, it is not currently dominating the policy agenda in the same way as online safety, AI regulation or content moderation. Law enforcement continues to push for lawful access to encrypted communications, arguing it helps fight crime and terrorism. Meanwhile, privacy advocates and technology companies warn that weakening encryption creates security risks, putting national security, consumer privacy, and business trust at risk. This has its roots in the Snowden leaks, which provided a major spur for technology companies to provide their users with end-to-end encryption, as well as the earlier backlash to the Clipper Chip which was advocated for by the Clinton administration. Interviewees noted that interest in the debate tends to spike in response to particular incidents. While the San Bernardino case is the touchstone for the US debate, interviewees noted the growing interplay with developments in other jurisdictions, including the arrest of Pavel Durov and seen recently by the sharp reaction of the Trump administration to the UK government's requests of Apple.

> *Section 230 is crucial as a legal backstop for privacy. People have the right to private communication without outside monitoring. Encryption ensures that right, and Section 230 reinforces it.*
>
> **ACADEMIC**

There have been attempts in Congress to pass legislation that critics argue could lead to requiring online services to introduce "backdoors". The most notable example is the EARN IT Act[39], which proposed establishing a commission to provide best practice for technology platforms in combatting child sexual exploitation. The bill also proposed weakening Section 230 protections, allowing lawsuits against technology companies where it is demonstrated that they have not tackled

CSAM. Supporters argue that this would hold platforms accountable for the spread of CSAM, but opponents warn that removing liability protections would potentially force online platforms to abandon end-to-end encryption, as they could face lawsuits for failing to monitor encrypted content. Interviewees were quick to emphasise the importance of Section 230 provisions for privacy rights and raised concerns about attempts to modify those, highlighting why such efforts to legislate at a federal level have stalled.

In Brussels, there is a similar air of stalemate between the opposing camps against the backdrop of the stalled CSAM Regulation[40]. This proposal, first published in May 2022, includes a range of obligations on online services, including controversial detection orders which would, under certain circumstances, compel technology services to operate detection technology for CSAM.

Encrypted services are a challenge because they make it much harder to to collect data. It makes it much harder to assess impact because you have no idea how many people that content has reached."

FORMER GOVERNMENT ADVISOR

Interviewees were quick to point out the policy challenges of encrypted services, not just for protecting children but also in monitoring the spread of mis- and disinformation. They stressed the need to explore technical solutions which would provide certain insights and data points to authorities without breaking encryption itself and leading to a general monitoring provision of messaging services. One element that could potentially prompt movement in Brussels on the regulation is the change of government in Germany, one of the leading member states in the pro-encryption camp alongside Austria and Poland. The exit of the liberal FDP and the Greens from government could – in principle – allow for a modest shift in German positioning, though this is far from guaranteed and, in the event that it materialises, would likely see support for voluntary rather than mandatory monitoring, as per the proposals of the Polish Presidency of the Council.

Privacy cannot trump every concern... political sentiment is strong on this issue, and will eventually win out against an outright refusal to act from end-to-end encryption platforms."

LEGISLATOR

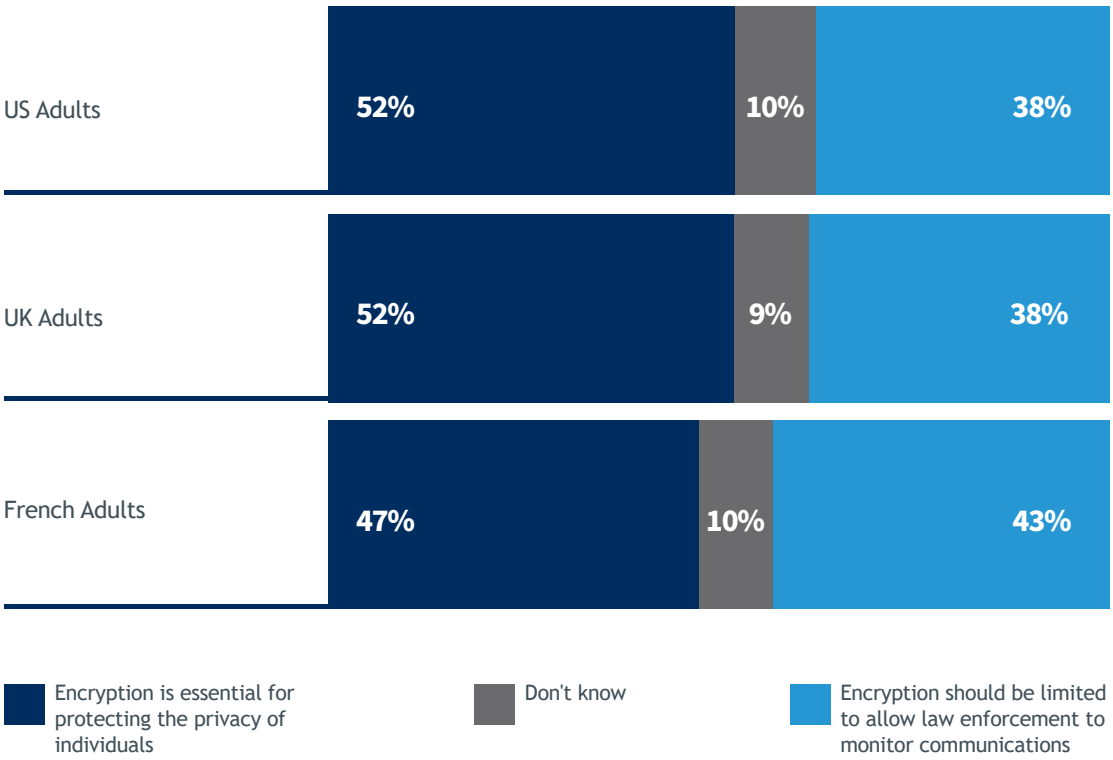
In the UK, the long simmering debate around encryption has been reignited in recent months amidst media reports that the Home Office has issued Apple with a technical capability notice (TCN)[41]. In response, Apple announced that it will withdraw its Advanced Data Protection (ADP)[42] option for UK users and the incident has drawn criticism from President Trump and his administration . This has prompted a renewed debate within the UK's technology sector and law enforcement communities, as well as from media commentators. Interviewees argued that the outcome of this case would be the key determining factor for the future of TCNs under the IPA, speculating that other technology companies were watching closely to see whether the government would successfully uphold its case upon appeal.

If the Home Office loses the case then it probably nullifies the value of the whole technical capability notice system."

FORMER POLICY OFFICIAL

FIG 13: The public are less supportive of breaking encryption for law enforcement monitoring

% OF ADULTS IN EACH MARKET SAYING WHICH STATEMENT COMES CLOSEST TO THEIR VIEW



Attitudes on encryption amongst interviewees varied according to the role of the individual and the institution they represented, with government and political stakeholders more bullish on the need for targeted access to encrypted services and regulators, industry and civil society being significantly more cautious and extolling the benefits of encryption. Several stakeholders drew a distinction based on whether the data was 'at rest' or 'in transit', as well as the type of access and monitoring required, with former government officials contrasting what they felt was essential access for law enforcement via TCNs with some scepticism about the "mass surveillance" required to implement Ofcom's powers under the OSA. These empower Ofcom to require any user to user platform to use 'accredited technology' when deemed 'necessary and proportionate' to scan for and remove terrorism and CSAM content. Amidst pushback from industry, Ofcom and the government have stressed that they do not intend to use these powers, leading to what one interviewee has described as a "fudge".

> *Encryption is an important technology to ensure security… any technical interventions must be proportionate to the risk of harm that they could pose if they were introduced."*
>
> **REGULATOR**

Conclusion

As this report demonstrates, online safety policy has fundamentally shifted since the beginning of the second Trump Presidency. Our analysis depicts a transatlantic relationship of growing tension and mistrust. Companies face the prospect of being caught between the different worldviews of European and American policymakers with major reputational and, potentially in the future, regulatory and legal implications.

As we look ahead, it is worth questioning whether the current dynamics are likely to endure and to test whether the EU and the US could "do a deal" to smooth differences in online safety and other areas of technology policy like taxation, AI, data protection and antitrust. Ideas that have been floated include a transatlantic digital single market, a Stargate for Europe, a turbocharged digital economy agreement or some form of revived EU-US Trade and Technology Council (TTC).

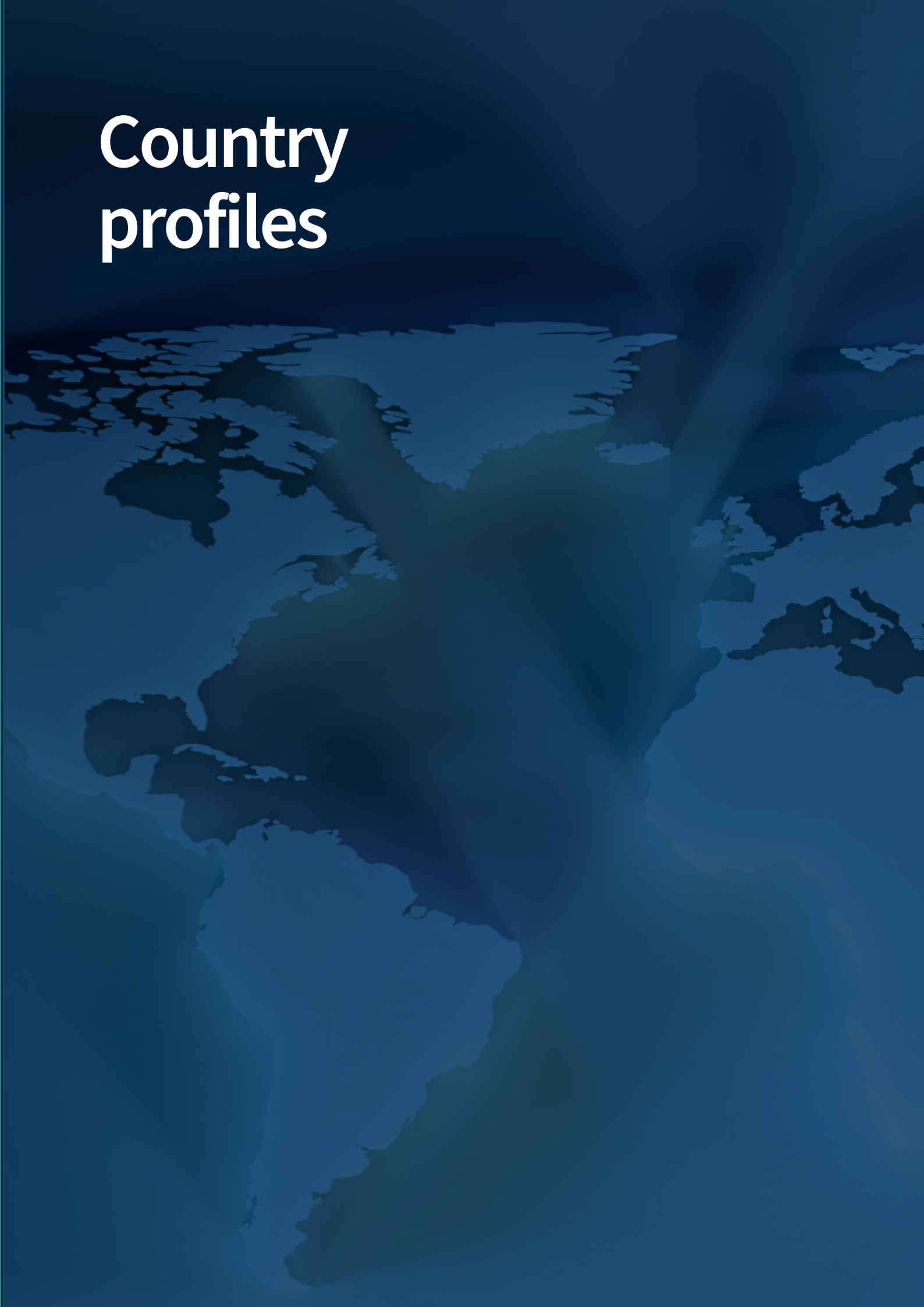
While nothing can be ruled out when Europe's security guarantee is at risk, the prospects of such a "deal" appear remote. The posture of senior members of the Trump administration implies that the ideas listed above would not be sufficient unless they included meaningful policy or enforcement changes in the DSA or other totemic legislation like the GDPR. Accepting such demands would be a humiliating volte-face for the European Commission after a decade of positioning itself as the world's digital regulator, and would face sustained opposition from politicians, media and civil society in Brussels and in individual member states. Indeed, EU policymakers are rapidly coming to the opposite conclusion and, after years of equivocating on "open strategic autonomy", are increasingly embracing technological sovereignty.

In contrast, a "deal" is more likely between London and Washington DC. The UK has neither the scale nor the ambition to pursue technological sovereignty and is looking to negotiate a digital agreement with the US. The prospects of a "deal" will also rest on enforcement of the UK's digital legislation by Ofcom, the Competition and Markets Authority (CMA) and even government departments like the Home Office. The example of the GDPR may be instructive here – the UK shares essentially the same legal framework as the rest of Europe, but unlike the EU it has yet to face criticism from large technology companies or the Trump administration. This can be explained quite simply by the fact that the largest fine levied by the UK's Information Commissioner's Office (ICO) against an American company is £18 million, compared to €1.2 billion in the EU (Ireland). It remains to be seen if Ofcom and other UK regulators will follow the ICO's enforcement template.

Perhaps more consequential than the question of a "deal" is the impact of online safety incidents and tragedies. As noted throughout this report, online safety policy campaigns have been repeatedly galvanised by the response to a succession of tragedies. There is nothing to suggest this will change in the coming years and the policy pendulum could plausibly start swinging back in the other direction.

At Global Counsel, we will track and analyse the evolution of these debates with this report acting as the first in a series of insights analysing the future of transatlantic technology policy.

Country profiles



US

THE AMERICAN PUBLIC'S VIEWS ON ONLINE SAFETY

Attitudes of the American public on online safety are – at face value - surprising in that they broadly align with those of their European counterparts. This is at odds with the policies of the Trump administration which has forcefully criticised what it terms as "censorship" of European regulations such as the DSA and OSA. Likewise, public support for regulation contrasts with the absence of federal level technology rules on online safety and in adjacent areas such as privacy.

That said, there are a number of important nuances in the views of the US public. They are more likely than their European counterparts to think that there is already regulation in place across a range of online safety topics despite, as noted above, there being an absence of recent federal technology legislation. This likely reflects the idiosyncratic US discourse on the role of government and federal agencies. This was also seen in a number of different responses which suggested the US public are more concerned about online surveillance and less convinced about giving law enforcement access to encrypted messaging platforms.

While they were in favour of all safety initiatives put before them, the US public expressed this with less enthusiasm than the UK public, though their attitudes are broadly similar to the French. They are also more likely than Europeans to trust tech companies and individual users to address risks of misinformation and less trusting of law enforcement and regulators in this regard.

THE AMERICAN PUBLIC AND THE POLICY AGENDA

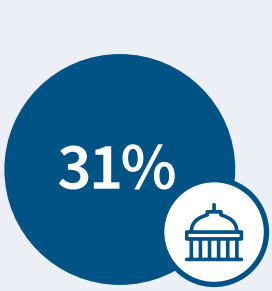
The key dynamic in US technology policymaking is the interplay between the federal and state levels. Congress has repeatedly failed to pass technology legislation despite bipartisan support in areas like privacy, children's privacy and children's protection. Where Congress made progress on tech legislation under the Biden administration was in passing bills which were either designed to improve the US' competitiveness vis-à-vis China, such as the CHIPS Act[43], or were targeted at Chinese companies, including the law on TikTok's ownership[44].

As discussed in the context chapter, states have moved to fill the void, creating an increasingly complex situation where technology companies face a myriad of different rules across the 50 states. While state laws have yet to outright contradict each other, there is scope in the future for competing and contradictory requirements being applied to companies, potentially making the case for a federal-level bill.

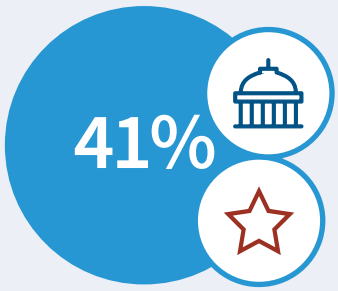
When asked about the appropriate level to regulate online safety, there was a plurality in favour of a federal rules that set a consistent baseline across the country, though there were mixed views about whether individual states should be allowed to go further and enact stronger protections (see Fig 14). Those preferring only state-level rules were in the minority at 17% of the US public.

FIG 14: Most US voters prefer federal involvement in lawmaking

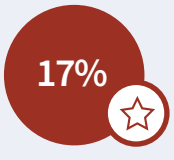
% OF US RESPONDENTS SELECTING EACH STATEMENT AS CLOSEST TO THEIR VIEW



Online safety laws should be made at the **federal** level, to create a single national standard for online safety across all states

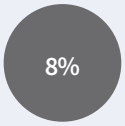


Online safety laws should be made at a **mix of both federal and state** levels, with federal laws setting a baseline and states having the option to enact stronger protections



Online safety laws should be made at the **state** level, to allow individual states to address their specific needs and concerns

NONE OF THE ABOVE



DON'T KNOW

EU

THE FRENCH PUBLIC'S VIEWS ON ONLINE SAFETY

The French public occupy the middle ground between the pro-regulatory attitudes of the British and the less enthusiastic sentiment of the US. In some areas their views edge closer to those seen in the US - for example, in being less enthusiastic about introducing new regulations. In other areas they are closer to the British in being less trusting of tech companies and users for moderating misinformation and more trusting of regulators and law enforcement.

A couple of areas stand out in the attitudes of the French public. First, linked to the point about trust in law enforcement, is greater support in France for prioritising law enforcement access to encrypted communications. The French public were, as noted in the encryption section, highly supportive of the arrest of Telegram's CEO.

Second, the French public recorded higher levels of concern about cybersecurity and harassment - with 43% placing this in their top three concerns, compared to 38% in the US and only 27% in the UK. This may reflect a number of high-profile cases in France, including the suicides of Marion Fraisse and Nicholas, as well as the high-profile "L'affaire Mila" which ultimately led to the Justice Minister defending the right to blasphemy.

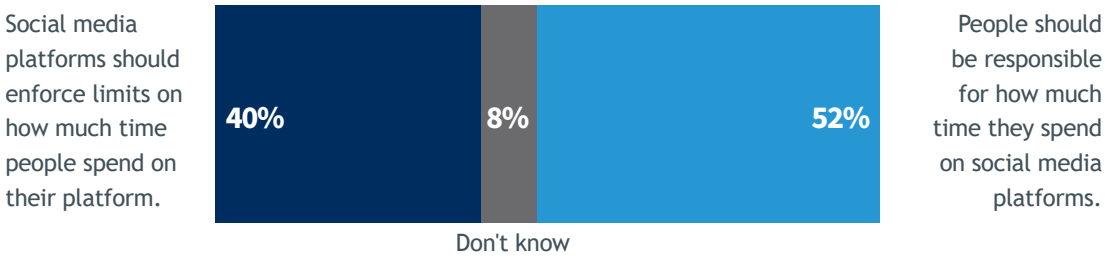
FIG 15: The French public appear unpersuaded on key DFA initiatives

% OF FRENCH RESPONDENTS SELECTING EASE/DIFFICULTY OF EACH OPTION

EU

FIG 16: The French public prioritise individual user responsibility for screen time

% OF FRENCH ADULTS SAYING WHICH STATEMENT COMES CLOSEST TO THEIR VIEW



THE FRENCH PUBLIC AND THE EU POLICY AGENDA

The European Commission has committed to proposing the DFA in the coming years with a legislative proposal expected in 2026. While ostensibly about consumer protection, the DFA will be relevant to a number of online safety issues, particularly in its proposed focus on issues of addictiveness online and how these fuel potential harms for both children and adults.

The sentiment of the French public does not, however, indicate overwhelming support for the types of interventions which are currently being discussed in Brussels. For example, the impact of online addiction on mental health was only ranked as a top three concern by 11% of the French public and the result was even lower at 7% for targeted advertising. Likewise, when looking at a series of issues seen as potentially problematic under the DFA, the French public was split on current corporate practices. For example, on the ease of being able to understand terms and conditions for apps (see Fig 15).

More encouragingly for proponents of the DFA, a majority in France were in favour of changing how social media sites are designed and, in response to the concern about influencers not being transparent about their advertising practice, in favour of greater transparency on paid-for adverts. However, these were amongst the least popular of the measures that were tested, again suggesting that the case for the DFA has yet to be made, at least to the French public.

UK

THE BRITISH PUBLIC'S VIEWS ON ONLINE SAFETY

Compared to the French and American public, British people stand out as the most supportive of further interventions on online safety. They believe that the regulatory starting point is lower and that there is less existing legislation in place to govern online activities, despite the passing of the OSA and previous legislative frameworks such as the Video-Sharing Platforms regime. UK adults tend to be more supportive than their US and French counterparts of regulatory interventions. They are also the least trusting of technology companies to self-regulate on issues like misinformation, preferring law enforcement or Ofcom to perform that role.

These results are consistent with previous studies that GC has conducted into public attitudes. For example, our 2022 research report on attitudes to the metaverse revealed a more sceptical attitude towards online technologies than the American or French publics. A similar tendency was found in our 2023 survey on generative AI. This exposes the misconception that because deregulation has been long espoused by UK governments, it is also widely supported by the British public.

FIG 17: The UK public are more concerned about online fraud than other countries

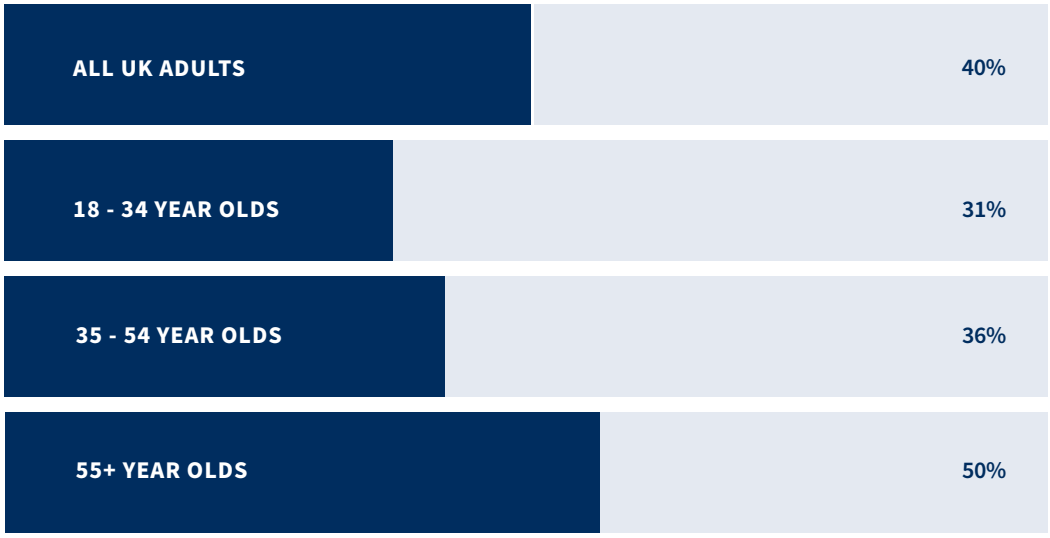
% OF RESPONDENTS SELECTING EACH AS A TOP THREE CONCERN

			
Online predators targeting children	55%	52%	53%
Fraudulent activity (e.g., unauthorised online transactions) and scams	40%	29%	29%
Exposure to inappropriate or harmful content online	31%	19%	24%
Cyberbullying and harassment	27%	43%	38%
Spreading of false or misleading information	27%	21%	24%
Personal data being collected without consent	25%	22%	25%
Deepfakes and AI-generated content	23%	18%	20%
The impact of online addiction on mental health	15%	11%	15%
Inadequate age verification on social media platforms	13%	16%	14%
Tracking and surveillance of online activities	12%	11%	16%
Erosion of freedom of expression online	7%	6%	7%
Adverts targeting users based on browsing history	4%	7%	7%
None of the above cause me concern	2%	3%	3%
Prefer not to say	1%	1%	1%

UK

FIG 18: Older voters are more concerned than younger adults about online fraud

% OF UK RESPONDENTS IN EACH AGE GROUP SELECTING FRAUDULENT ACTIVITY AND SCAMS AS A TOP THREE CONCERN



THE BRITISH PUBLIC AND THE POLICY AGENDA

Compared to their French and American counterparts, the UK public show differences in their priority concerns on online safety in two areas. The first is on online fraud and scams, where 40% of UK adults identified this amongst their top three concerns, compared to only 29% in the US and France (see Fig 17). This is driven by higher levels of concern amongst older members of the public with 50% of over 55 year olds selecting fraud compared to 31% of 18 to 34 year olds (see Fig 18).

This aligns with the active media and political debate on fraud in the British media and in Parliament, which saw campaigns for "economic harms" to be included within the scope of the OSA. The UK government committed in its election manifesto[45] to bring forward a new fraud strategy and the Home Office is understood to be already working on this. One of the major debates is the extent to which technology companies should be made liable for fraud compensation payments in the same way that financial services have been.

The second area is on tackling "legal but harmful" content. The UK has seen an intense debate in the context of the OSA and has seen a number of parliamentary committees scrutinise issues such as body image online. Concerns expressed in this wider debate appear to align with views of the British public, with around a third placing harmful content in their top three concerns compared to less than a quarter in France and the US.

Endnotes

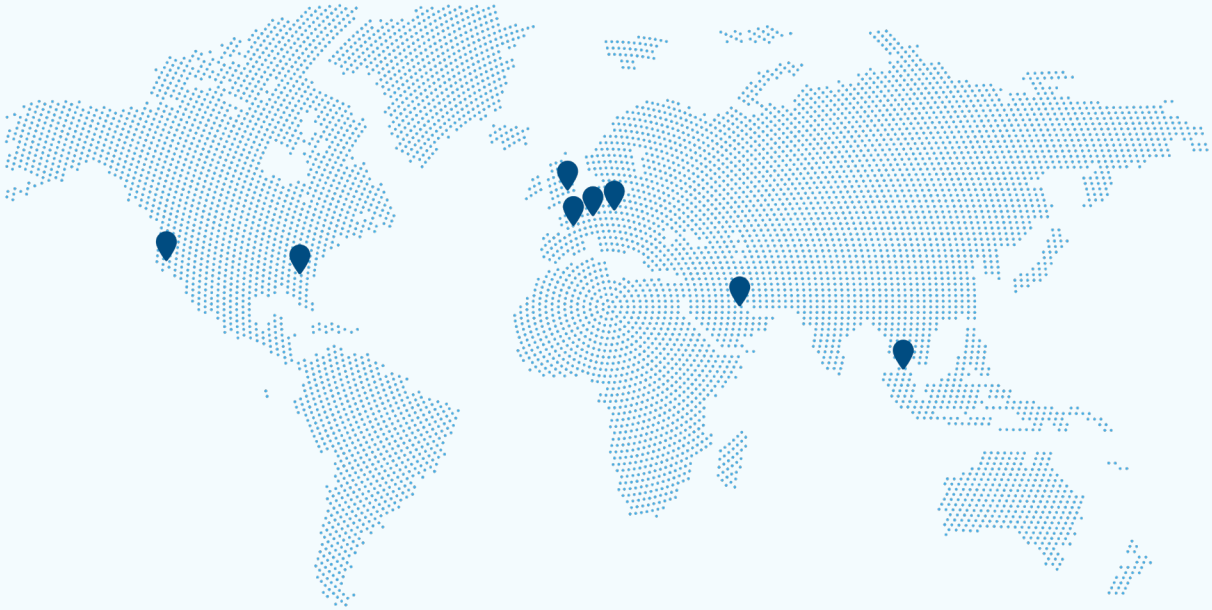
1. See United States Government Publishing Office (GPO)
2. See EUR-Lex
3. See The Christchurch Call
4. See legislation.gov.uk
5. See Bundesministerium der Justiz
6. See EUR-Lex
7. See EUR-Lex
8. See European Commission
9. See European Commission
10. See European Parliament
11. See US House of Representatives
12. See FTC
13. See FTC
14. See Florida Senate
15. See Texas Legislature
16. See US Supreme Court
17. See California legislative information
18. See Maryland General Assembly
19. See Politico Pro
20. See UK Parliament
21. See the Times
22. See BBC
23. See ICO
24. See Congress
25. See Congress
26. See Legifrance
27. See New York Senate
28. See White House
29. See The American Presidency Project
30. See Reuters
31. See EUR-Lex
32. See EUR-Lex
33. See European Commission
34. See Sky News
35. See legislation.gov.uk
36. See UK Parliament
37. See Congress
38. See EUR-Lex
39. See Congress
40. See EUR-Lex
41. See legislation.gov.uk
42. See Apple
43. See Congress
44. See US Supreme Court
45. See Labour Party

About Global Counsel

Global Counsel is a strategic advisory business.

We help companies and investors across a wide range of sectors to anticipate the ways in which politics, regulation and public policymaking create both risk and opportunity - and to develop and implement strategies to meet these challenges. Our team has experience in politics and policymaking in national governments and international institutions backed with deep regional and local knowledge.

Our global team operates across Berlin, Brussels, Doha, London, Paris, San Francisco, Singapore and Washington DC, and are supported by a network of policymakers, businesses and advisers. Our partnership with The Messina Group and wider international network further strengthens our global reach.



Global Counsel Ltd

E: info@global-counsel.om
www.global-counsel.com

LEAD AUTHOR

Conan D'Arcy,
Senior Practice Director
c.darcy@global-counsel.com

CONTRIBUTORS

Jeffrey Afianmagbon
Josh Bates
Adriana Capparelli
Natasha Dixon
Chris Levy
Matilda Milne
Emma Morris
Ugonma Nwankwo
Megan Stagman

Global Counsel