JENNER & BLOCK

Online Safety Act: The 2027 Risk Map for Regulated Companies

Three years on from Royal Assent: what has changed, why it matters commercially, and what boards and general counsel should be preparing for in 2027.

Client Alerts

November 25, 2026
By: Joanna Ludlam

Three years after Royal Assent, the Online Safety Act 2023 (the Act) is no longer a regime of consultations and codes. It is a live enforcement system with a growing record of fines, a first set of investigations into the largest platforms, and a first win for Ofcom in the High Court.

But the record is uneven. Almost every fine so far has fallen on pornography providers and small, often offshore, services; the investigations into Meta, X, and TikTok remain open; and Ofcom has conceded publicly that against an overseas forum it has reached the limit of what the Act allows. Supporters of the regime say Ofcom has been too slow and too cautious. Platforms and civil liberties groups say it reaches too far. Both critiques will shape 2027.

The Act is a test of trust in two directions. The public is asked to trust that platforms will keep children safe; regulated businesses are asked to trust that the regulator will use far-reaching powers predictably, proportionately, and subject to effective challenge. How Ofcom has used those powers so far, and how the courts have responded, says a great deal about both.

At a Glance

- Enforcement is live but uneven, with no fine yet on a major platform.
- The courts have backed Ofcom twice. The right to challenge is real but narrow.
- Information notices, risk assessments, and age assurance are where companies are exposed now.
- For 2027, the risk moves up the market.

The Regime So Far

The architecture of the Act is now substantially in force. The core duties arrived in three waves during 2025: age-check duties on pornography providers from January; illegal content risk assessments and safety duties from March; and the children's safety duties, including highly effective age assurance, from July.

The second phase, the additional duties for the largest services, moved forward in July 2026 when Ofcom published its register of categorised services. Ofcom has asked Category 1 and 2A providers to publish summaries of their risk assessments by November 2026. The fees regime has also gone live: in October 2026 Ofcom published the list of providers required to pay online safety fees.

Ofcom has kept layering obligations onto the codes. Three developments of the last three months stand out.

- **Crisis response.** Since 2 November 2026, large and high-risk user-to-user services must have written crisis protocols, cross-functional response teams, and a dedicated law enforcement communication channel. Ofcom mandates the protocols, but platforms decide when to activate them.

- **Intimate image abuse.** On 9 September 2026, Ofcom launched an enforcement programme on illegal intimate images and deepfakes, alongside updated Illegal Content Codes in force from 30 September. Its first two investigations under that programme opened on 26 October.

- **Child sexual abuse material (CSAM).** On 16 November 2026, Ofcom announced strengthened CSAM measures: banning users who generate, upload, or share such material; introducing wider hash matching; and requiring automated tools to detect previously unknown material on certain platforms.

Against all this, the first outcome data is sobering. Ofcom's first statutory report on content harmful to children, published on 22 October 2026, found no significant change in children's reported exposure to several categories of harmful content in the nine months after the children's duties took effect. It found that 14% of 11- to 17-year-olds reported seeing suicide or self-harm content in the previous four weeks, and that 23% reported seeing eating disorder content. Critics add that the same measures have restricted adults' access to lawful content and required them to hand over personal data to verify their age. Both perspectives will frame the political debate in 2027.

The Enforcement Record

Ofcom's financial penalties to date are set out below, in date order. Every one has fallen on a pornography provider, a nudification service, or an online forum; none has yet been imposed on a major social media platform.

Date	Provider	Breach	Penalty

Date	Provider	Breach	Penalty
13 Oct 2025	4chan	Failure to answer two information requests	£20,000 + £100/day
20 Nov 2025	Itai Tech (nudification site)	No age checks; information failure	£50,000 + £5,000
4 Dec 2025	AVS Group	Ineffective age assurance; information failure	£1 million + £50,000
12 Feb 2026	Kick Online Entertainment	No age checks; information failure	£800,000 + £30,000
23 Feb 2026	8579 LLC	No age checks; information failure	£1.35 million + £50,000
19 Mar 2026	4chan	No age checks; other safety duties	£450,000 + £70,000
13 May 2026	Online suicide forum	Illegal content duties	£950,000
19 Jun 2026	First Time Videos	No age checks	£80,000
3 Sep 2026	Xgroovy	No age checks; information failure	£700,000 + £30,000

Four features of Ofcom's approach emerge from this record.

First, it has prioritised by reach and by ease of proof. Shortly after the age-check duty took effect, Ofcom opened investigations into 34 pornography sites, chosen by user numbers. Age assurance is a binary, observable obligation, which makes it the natural place for a new regulator to build a body of decisions.

Second, it treats the information duty as non-negotiable. Almost every decision pairs a substantive fine with a separate penalty for failing to answer a statutory information request. Ofcom's very first fine, against 4chan, was for that alone. The message to every regulated service is that non-engagement is itself a breach.

Third, penalties track size and remediation. Ofcom says it sets fines with regard to the size and turnover of the service, and it has taken account of providers withdrawing from the United Kingdom. The highest single penalty remains £1.35 million, far below the statutory ceiling of the greater of £18 million or 10% of qualifying worldwide revenue.

Fourth, with the major platforms, it is supervising first and enforcing second. In 2026 Ofcom moved its focus to household names: a formal investigation into X from January; binding information

requests to Facebook, Instagram, Roblox, Snapchat, TikTok, and YouTube in March; a section 12 investigation into TikTok's age assurance from July; an investigation into Pornhub's provider from 23 September; and a first investigation into Meta, over the risk assessment for Instagram's Instants feature, from October.

The X case reveals Ofcom's methods. In May 2026, while its investigation continued, Ofcom accepted public commitments from X on illegal terror and hate content: an average 24-hour review time, 85% of reports handled within 48 hours, and quarterly performance data for a year. In October it narrowed the investigation to X's illegal content and complaints duties. Negotiated commitments backed by an open investigation look set to become a standard tool for the largest platforms.

Lines of Conflict

Three lines of conflict now define the regime, and they pull Ofcom in opposite directions. Each is at root an argument about trust: whether the public can trust the regime to protect children and whether companies can trust Ofcom to use its powers proportionately.

Campaigners against Ofcom: too slow, too cautious. Child safety and suicide prevention groups argue the Act is not delivering. After Ofcom's July 2026 statement on the suicide forum, campaigners said publicly that the Act in Ofcom's hands was not working. Commentators sympathetic to the regime have levelled the charge of a 'paper tiger', and accusations of a minimalist implementation have been widely reported. Ofcom's own October report on children's exposure to harmful content gives this camp its strongest evidence.

Platforms and free speech advocates against Ofcom: too far, too intrusive. The largest platforms have taken Ofcom to court over the scope of its information powers (see below). TikTok has publicly disputed Ofcom's characterisation of its child safety measures. Civil liberties critics argue the regime pushes platforms towards over-removal and intrusive age checks, and that Ofcom's response to underperformance is simply more regulation.

Extraterritoriality: the limits of UK reach. The Act applies to services with links to the United Kingdom wherever they are based, and Ofcom has been explicit that being offshore does not take a service out of scope. The practical reach is another matter.

- 4chan has refused to pay its penalties and has sued Ofcom in the United States; Ofcom moved to dismiss that suit in December 2025.
- The US-based suicide forum did not pay its £950,000 fine by the deadline, and Ofcom says it has begun work to pursue the debt, as it has with every company that has missed a payment deadline.
- In July 2026 Ofcom announced that the forum's blocking of most UK users was the fullest extent of what the Act could achieve, and that no further legal route, including a court-ordered block, was available.

The result is an asymmetry. Ofcom's tools work well against companies that want to stay in the UK market and badly against those that do not. That asymmetry is now a policy question for government as much as an enforcement question for Ofcom. For compliant businesses, it is also a fairness question: the burden of regulation falls on those who stay and engage, while those who refuse to engage are hardest to reach.

The Legal Challenges to Ofcom

The courts have so far backed the regime twice, while signalling where future challenges could succeed.

The routes. Certain Ofcom decisions can be appealed to the Upper Tribunal; codes of practice, secondary legislation, and other measures can be challenged by judicial review in the High Court. Both apply ordinary judicial review principles, and claims must be brought promptly and in any event within three months. Challenges will therefore turn on legality, rationality, procedure, and proportionality, not on whether Ofcom reached the right answer.

Wikimedia (August 2025). In *Wikimedia Foundation v Secretary of State for Science, Innovation and Technology* [2025] EWHC 2086 (Admin), the Administrative Court dismissed a challenge to the Categorisation Regulations. It held that the Secretary of State had not acted irrationally and had followed the procedure the Act requires. The judge stressed that the ruling was not a green light for a regime that would significantly impede Wikimedia's operations, leaving the door open to a challenge to any categorisation decision itself.

Meta, X, and TikTok (October 2026). On 30 October 2026, in *R (Meta, X and TikTok) v Ofcom* [2026] EWHC 2779 (Admin), the Divisional Court rejected the platforms' challenge to section 100 information notices seeking content moderation data. Permission was refused on most grounds, and the proportionality and human rights grounds failed on their merits. This was the first judicial test of Ofcom's information-gathering powers, and Ofcom won it.

Two questions were left open: whether the cumulative burden of repeated requests is a basis for challenge, and how the sanctions behind a notice bear on proportionality. Those are where the next challenge to an information notice is likely to be pitched.

What is still in play. Meta has brought a second judicial review challenge against the regulations defining qualifying worldwide revenue, the base for both fees and penalties. Any confirmation decision against a major platform in the open investigations is also likely to be appealed.

The pattern is clear. The courts give Ofcom and the Secretary of State a wide margin on the design of the regime, but they have flagged that how the powers are applied to a particular service, especially where rights are engaged, remains open to review. For regulated companies, the practical lesson is that the right to challenge Ofcom is real but narrow. Claims must be brought quickly, and the courts will not substitute their own view for the regulator's. A challenge is only as strong as the

representations, evidence, and proportionality arguments a company has put in during the investigation. Recourse has to be prepared for from the first information notice, not after the decision.

The Practical Priorities for Regulated Companies

The moments that test a company's relationship with its regulator tend to arrive without warning: an information notice, a product launch, a provisional decision. The enforcement record and the case law point to seven practical priorities. Most come down to one thing: giving Ofcom reasons to trust your process before it has cause to doubt it.

1. **Treat every information notice as a legal deadline, not a request.** The information duty is the most enforced provision in the Act. After the October 2026 judgment, a refusal on grounds of burden or proportionality is unlikely to succeed unless the notice is genuinely excessive, and the attempt will be costly.

2. **Engage early.** Ofcom's confirmation decisions repeatedly cite non-engagement. Its 4chan decision records offers of introductory meetings in March and April 2025 that went unanswered before any investigation opened.

3. **Make risk assessments live documents.** The Meta investigation turns on whether a new feature was risk-assessed before launch. Section 9(4) of the Act requires a fresh risk assessment before any significant change to a service's design or operation. Companies should build that step into their product release process, so that no significant new feature or change goes live until a documented risk assessment has been completed and signed off.

4. **Test age assurance against Ofcom's standard, not your own.** AVS Group was fined although it had age checks, because Ofcom did not consider them highly effective. The TikTok investigation tests age estimation at scale.

5. **Prepare for supervision as well as enforcement.** For the largest services, commitments, audits, and quarterly data, as in the X case, may come before or instead of a fine. Data held for Ofcom should be accurate, reconcilable, and ready to be shared.

6. **Map the new obligations of late 2026.** These include: Crisis response protocols; the updated Illegal Content Codes; the new intimate image abuse programme; and, once in force, the strengthened CSAM measures. Category 1 and 2A services also face the transparency expectations attached to the register.

7. **Build a litigation-ready record.** Challenges are decided on judicial review principles, so the strength of a company's position depends on the record it builds during the investigation: representations made, evidence supplied, and proportionality arguments submitted on time.

For senior managers, the direction of travel matters. Ofcom has shown it will name providers, publish detailed decisions, and pursue unpaid debts. Governance of online safety compliance now belongs in the same place as other regulatory risk at board level.

The Outlook for 2027

The House of Lords Library expects the Act to be fully implemented by mid-2027. But 2027 will be about more than completing the original design. Government is now widening the regime through secondary legislation, and Ofcom's open investigations into the largest platforms are reaching the decision stage.

The Scheduled Milestones

Expected	Development
January 2027	Ofcom report on children's use of app stores
First half of 2027, at the earliest	Fraudulent advertising duties in force
Spring 2027	Under-16 social media ban in force; government plans to lay the regulations by the end of 2026
Mid-2027	Final policy statements on the additional duties for categorised services
Summer 2027	First transparency reports from categorised services
No date set	Regulations bringing AI chatbots within the illegal content duties, to be laid at the earliest opportunity

Regulation Widening the Regime

Two 2026 statutes gave ministers powers to reshape the Act without fresh primary legislation. Section 70 of the Children's Wellbeing and Schools Act 2026 inserted a new section 214A into the Act, the vehicle for the under-16 ban. The Crime and Policing Act 2026 inserted a new section 216A, allowing the Act to be amended to capture more kinds of generative AI tools.

The ban will extend the existing highly effective age assurance standard from a question about being over 18 to one about being over 16. For in-scope services, the body of age assurance decisions Ofcom has built against pornography providers will suddenly become directly relevant.

Our Predictions

These are our predictions for where the regime will be tested next.

1. **The first provisional or confirmation decision against a major platform.** The TikTok, X, and Meta investigations will produce at least one provisional or confirmation decision in 2027. Expect the first eight-figure penalty under the Act, and expect it to be challenged.

2. **Age assurance becomes the central compliance issue for social media.** The under-16 ban, the TikTok investigation, and the CSAM measures converge on the same question: can a platform reliably tell who is a child? Enforcement against mainstream platforms on age assurance is likely within months of the ban taking effect.

3. **The next information notice challenge will be about cumulative burden.** The October 2026 judgment closed off general attacks on section 100 notices but left that point open. A platform facing a sustained series of requests is likely to test it.

4. **Categorisation decisions will be litigated.** The *Wikimedia* judgment expressly left room to challenge how the thresholds are applied to a particular service. As the Category 1 duties are finalised, at least one service is likely to challenge its categorisation.

5. **Business disruption measures will be tested, and found wanting.** The suicide forum case showed the current limits. Expect Ofcom's first applications for court orders against non-paying offshore services, and pressure on government to strengthen the regime against them.

6. **The politics will harden, not soften.** The first statutory report on children's exposure gives both sides ammunition. Expect pressure for faster, larger enforcement and continued expansion by regulation, alongside louder transatlantic objections on free speech grounds.

Conclusion

Three years in, the Online Safety Act has its foundations in place: duties in force, a regulator with a growing body of decisions, and a High Court that has upheld its powers. Ofcom's approach to the largest platforms has so far been supervision-heavy, and it has yet to turn that into a decision that changes how a major platform operates. Nor does Ofcom have a reliable answer to services that ignore it from abroad.

For regulated companies, the lesson of 2025 and 2026 is that Ofcom rewards engagement, punishes silence, and builds its cases on the record. Those that prepare for scrutiny, and for the possibility of challenge, will be best placed when their own moment of testing comes. For 2027, the risk moves up the market. The largest platforms should expect decisions, not just dialogue, and every in-scope service should expect the rules themselves to keep changing by regulation.

The test ahead is whether Ofcom can earn the trust of both a public that wants evidence that children are safer and companies that want certainty about how the rules will apply.

Related Lawyers



Joanna Ludlam
Partner
jludlam@jenner.com
+44 330 060 5465

Related Capabilities

Content, Media, and Entertainment

Global Crisis Management and Strategic Risk

Investigations, Compliance, and Defense

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →