# The Online Safety Act: A Critical Examination of its Promises, Perils, and Unintended Consequences

## Executive Summary

The Online Safety Act (OSA), enacted with the stated aim of safeguarding children and adults online, presents a compelling case of legislative overreach that risks undermining the very safety and freedoms it purports to protect. While framed as a necessary measure against online harms, a rigorous examination of its provisions, particularly mandatory age verification, reveals significant flaws in its practical implementation. This report details how the Act inadvertently constructs a vast "gold mine" of sensitive personal data, making users highly vulnerable to breaches, blackmail, and identity theft. Furthermore, the legislation's reliance on technical barriers proves futile against determined users, leading to a surge in circumvention tools like Virtual Private Networks (VPNs) and an unintended push towards unregulated "shadow sites" that pose greater risks.

The Act's approach also exacerbates existing privacy threats, notably by failing to adequately address the pervasive commercial stalkerware industry, which thrives on legal ambiguities and inadequate enforcement. Broader implications include a chilling effect on legitimate speech and information access, exemplified by the Wikimedia Foundation's legal challenge, which highlights the Act's collateral damage to public interest platforms. Fundamentally, the OSA's design appears driven more by a desire for performative solutions than by a nuanced understanding of digital dynamics, potentially normalizing pervasive digital monitoring and eroding foundational principles of privacy and free expression. The analysis concludes that genuine online safety necessitates a shift from restrictive, data-intensive legislation towards comprehensive digital literacy education, enhanced parental involvement, and the adoption of privacy-preserving technologies.

# 1. Introduction: The Online Safety Act's Ambitions and Realities

## 1.1 Overview of the Online Safety Act (OSA) and its Stated Goals

The Online Safety Act 2023 (OSA) represents a significant legislative endeavor in the United Kingdom, having officially passed on October 26, 2023.[1] Its primary objective, as articulated by the government, is to establish a safer online environment for both children and adults by regulating internet content.[2] This comprehensive legislation imposes a series of new legal duties on a wide array of online services, including social media platforms and search engines. These duties compel providers to implement robust systems and processes designed to mitigate the risks associated with illegal online activities and to ensure the swift removal of illegal content once identified.[2]

A cornerstone of the Act's child protection framework is the mandate for "highly effective age assurance".[2] This requirement applies specifically to services that host pornography or other categories of content deemed harmful to children, with a firm deadline for pornography services to introduce these age checks by July 2025.[3] Beyond content regulation, the OSA also introduces new criminal offenses, notably addressing the non-consensual sharing of intimate images, often referred to as 'revenge porn,' and the creation of sexually explicit deepfakes.[5]

Ofcom, the designated independent regulator for Online Safety, is vested with extensive powers to oversee and enforce compliance with the Act.[1] These powers are substantial, encompassing the authority to conduct investigations into non-compliance, levy significant fines that can amount to up to 10% of a company's qualifying worldwide revenue or £18 million (whichever is greater), and, in the most severe instances of non-compliance, seek court orders to block services from operating within the UK.[2] This regulatory framework highlights a clear intent to exert considerable control over the digital landscape.

The Act's stated goals, such as protecting children and combating illegal content, are inherently positive and widely supported. However, a critical examination immediately reveals a tension between these aspirational intentions and the foreseeable practical outcomes of the proposed solutions. While Ofcom's guidelines detail specific

methods and deadlines, implying a robust and effective system [3], concerns persist that these methods are fundamentally flawed or easily circumvented.[9] This discrepancy suggests that the Online Safety Act, despite its commendable intentions, may be structurally predisposed to fall short of its primary objectives. This potential shortfall stems from an overestimation of technological solutions and a fundamental misunderstanding of complex internet dynamics and user behavior, leading to the creation of new, unforeseen problems rather than genuine safety.

### 1.2 The "Hammer to Crack a Walnut" Premise: Initial Critique of the Act's Approach

The user's article characterizes the Online Safety Act, particularly its mandatory age verification provisions, as a "hammer to crack a walnut".[11] This powerful metaphor suggests that the legislative tool chosen is disproportionately blunt and heavy-handed for the intricate and nuanced challenges it purports to address. The Act is thus presented not as a genuine solution, but as a "performative solution to a complex problem".[11]

A significant critique embedded within this premise is the observation regarding the emotional appeal often leveraged in discussions surrounding child protection. The article notes that "the moment any debate centres around 'protecting the children,' a chilling silence often falls over rational discussion. It is the most powerful of all emotional appeals, an invocation of fear that, as history has shown, can justify any measure, however extreme".[11] This observation points to a potential strategy wherein public sentiment is manipulated to push through legislation without rigorous critical scrutiny. This framing allows policymakers to bypass robust, rational discussion about the actual efficacy, proportionality, and potential negative externalities of the proposed measures. By invoking such a potent emotional trigger, any opposition to the Act can be easily painted as being against child safety, effectively silencing dissent and limiting comprehensive public debate.

The article directly challenges the underlying assumptions of the Act by posing critical questions: "will this new regulation actually work, or will it create far greater dangers than it purports to solve?".[11] This sets the stage for a detailed, evidence-based examination of the Act's real-world efficacy and its potential for unintended, detrimental consequences. This suggests that the Act's design may be driven more by

political expediency and a desire to be

*seen* as "doing something" about online harms, rather than by sound policy analysis, empirical evidence, or a deep, nuanced understanding of the modern internet. This political motivation risks creating legislation that is fundamentally flawed, prioritizing headlines and public perception over genuine digital security and individual rights.

## 2. The Illusion of Safety: Mandatory Age Verification and Data Risks

### 2.1 The "Gold Mine" of Personal Data: Types of PII Collected for Age Verification

The Online Safety Act's mandate for "highly effective age assurance" [2] on services hosting age-restricted content directly necessitates the collection of sensitive personal data. Ofcom's guidance outlines various methods considered "highly effective," all of which involve the processing of personal information.[4] These methods include:

- **Photo ID Matching:** Users are required to upload images of government-issued identification, such as passports or driving licenses, often accompanied by a real-time selfie for biometric verification.[3]
- **Facial Age Estimation:** This method uses AI-powered technology to analyze a person's facial features from a photo or video to estimate their age.[3]
- **Open Banking:** With user consent, age-check services can securely access banking information to confirm if an individual is over 18, without revealing specific financial details.[3]
- **Credit Card Checks:** Age verification can occur by validating a provided credit card, as credit cards typically require the holder to be over 18.[3]
- **Email-based Age Estimation:** This involves analyzing an email address's usage patterns across other online services, such as banking or utility providers, to infer age.[3]
- **Mobile Network Operator Age Checks:** Age confirmation can be achieved by checking if a mobile phone number has age filters applied to its account.[3]

- **Digital Identity Services:** These services leverage digital identity wallets that securely store and share verified age information in a digital format.[3]

The assertion that this process involves collecting a "treasure trove of sensitive personal data" and is the "deliberate construction of a gold mine for cyber criminals" [11] is directly supported by the nature of the data required by these methods. Ofcom acknowledges that all age assurance methods process personal data and require service providers to adhere to data protection regulations, advising a "data protection by design" approach.[4] Conversely, simpler methods like self-declaration of age or online payments that do not require an individual to be 18 are explicitly deemed "not highly effective" by Ofcom and are therefore insufficient for compliance.[3]

The directive for "highly effective" age assurance inherently leads to the adoption of methods that, by their nature, require the collection of highly sensitive Personally Identifiable Information (PII), such as government IDs, biometric data, or financial linkage.[3] This creates a fundamental tension: to achieve a higher degree of verification accuracy, a larger and more sensitive dataset must be collected. This directly contradicts the principle of data minimization, a cornerstone of privacy by design, which advocates for collecting the least amount of data necessary. The pursuit of robust age verification, while ostensibly beneficial for child protection, inherently creates a massive new privacy risk by compelling the collection and storage of unprecedented quantities of sensitive personal data across a multitude of online platforms. This design choice prioritizes a perceived level of "effectiveness" over the fundamental principle of data privacy, potentially exposing users to greater harm than the Act purports to prevent.

**Table 1: Personal Data Collected for Age Verification Methods and Associated Privacy Concerns**

| Method | Data Collected/Accessed | Privacy Concerns |
|---|---|---|
| Photo ID Matching | Passport/Driving License details, Facial biometric data | Direct exposure of highly sensitive PII, biometric data risks, potential for re-identification |
| Facial Age Estimation | Facial biometric data | Biometric data risks, accuracy concerns, potential for re-identification |

| | | |
|---|---|---|
| Open Banking | Bank account status (binary: over 18/under 18) | Indirect data inference, linkage to financial identity |
| Credit Card Checks | Credit card validity (binary: over 18/under 18) | Potential for purchase trail growth, linkage to financial identity |
| Email-based Age Estimation | Email usage patterns/linked services (e.g., banking, utility providers) | Digital snooping, indirect data inference, linkage of identity to online behavior |
| Mobile Network Operator Age Checks | Mobile account age filters (binary: restricted/unrestricted) | Linkage to telecommunications identity, potential for broader data access |
| Digital Identity Services | Digital ID wallet attributes (e.g., verified age) | Centralized data storage, potential for single point of failure, linkage of identity to online behavior |

### 2.2 The Inevitable Threat: Data Breaches, Blackmail, and Identity Theft

The user's article warns that storing sensitive data across "a multitude of websites, many of them with a vested interest in remaining anonymous," represents a "terrifying prospect" and a "deliberate construction of a gold mine for cyber criminals, a honeypot of unparalleled value".[11] This concern is strongly supported by current cybersecurity trends and empirical evidence. Data breaches are not merely hypothetical; they are a pervasive and escalating threat, frequently occurring on an almost weekly basis.[11]

In 2023 alone, there were 3,205 publicly reported data compromises, affecting an estimated 353,027,892 individuals, marking a significant 78% increase over 2022.[15] A critical finding is that nearly half (46%) of all data breaches involve customer Personal Identifiable Information (PII), which includes highly sensitive data such as tax identification numbers, emails, phone numbers, and home addresses.[15] Compromises involving sensitive personal information consistently remain the most common type of data breach.[15] The healthcare sector, in particular, illustrates the severe impact of

such breaches, with over 276 million records compromised in 2024, including the largest-ever healthcare data breach (Change Healthcare) affecting an estimated 190 million individuals.[16]

The financial consequences of these incidents are substantial, with the average cost of a data breach reaching an all-time high of $4.88 million in 2024.[15] The methods of attack are also evolving, with cyberattacks using stolen or compromised credentials increasing by 71% year-over-year, and 86% of all breaches involving the use of stolen credentials.[15] This highlights a direct pathway for criminals to exploit collected PII. Compounding the risk, a staggering 98% of organizations report having at least one third-party vendor that has suffered a data breach.[15] This is particularly relevant given that age verification often relies on third-party age assurance providers.[12]

The user's article expresses concern about "a multitude of websites... storing such information".[11] The reality that 98% of organizations have experienced a data breach through a third-party vendor [15] is critical. Given that age verification often relies on specialized third-party age assurance providers [12], this creates a significant vulnerability. A breach at one of these central age verification services could compromise sensitive data collected on behalf of

*numerous* websites, leading to a cascading effect across the digital ecosystem. The recent AU10TIX hack, an identity verification company reportedly used by major platforms like TikTok and X, serves as a real-world illustration of this exact threat, exposing sensitive user data.[17] The distributed nature of data collection under the OSA, where sensitive PII is funneled through specialized third-party age verification services, inadvertently creates a highly attractive and centralized target for cybercriminals. This design choice, while perhaps intended to streamline verification, effectively concentrates risk, making widespread identity theft and blackmail a more probable outcome, thereby fulfilling the "terrifying prospect" warned by the article.

**Table 2: Recent Data Breach Statistics (Focus on PII and Sensitive Data)**

| Metric | Value (Year/Period) | Source |
|---|---|---|
| Total Reported Breaches | 3,205 (2023) | [15] |
| Individuals Affected | ~353 million (2023) | [15] |

| | | |
|---|---|---|
| Individuals Affected (Healthcare) | >276 million (2024) | [16] |
| Percentage of Breaches Involving Customer PII | 46% (IBM, 2024) | [15] |
| Percentage of Breaches Involving Employee PII | 40% (IBM, 2023) | [15] |
| Percentage of Breaches Involving Stolen Credentials | 86% (Verizon, 2023) | [15] |
| Increase in Breaches (2023 over 2022) | 78% | [15] |
| Average Cost of Data Breach | $4.88 million (2024) | [15] |
| Average Time to Identify Breach | 204 days | [15] |
| Average Time to Contain Breach | 73 days | [15] |
| Organizations with Third-Party Vendor Breaches | 98% | [15] |
| Largest Healthcare Breach | Change Healthcare (190 million individuals, 2024) | [16] |

### 2.3 Expert Opinions on Age Verification Data Honeypots and Blackmail Risks

Leading experts in cybersecurity and privacy have voiced significant concerns that directly echo the user's article regarding the dangers of age verification data collection. Tech lawyer Neil Brown cautioned against the act of submitting identity documents, specifically warning of "mistyped URLs and other scams, trying to obtain your personal data for phishing or blackmail purposes".[18] This highlights the immediate, user-level risks of interacting with such systems.

Sarah Forland, a policy analyst at New America's Open Technology Institute (OTI), explicitly stated that "many online age verification practices require people to share their personal data, which ultimately endangers that information".[19] She critically argues that the Supreme Court's decision to uphold age verification laws "ignores the very real risks online age verification poses to individuals' privacy and security online" [19], indicating a disconnect between legal rulings and practical cybersecurity realities.

Jason Nurse, a cyber expert at the University of Kent, expressed profound concern about the mandated use of digital ID services for age checks, particularly for adult content. He warned that "These sites will be entrusted with storing large amounts of personally identifiable information from potentially vast segments of the population. How can we be confident this data won't be misused?" He further elaborated that "Such centralised databases create attractive targets for attackers seeking information for blackmail, extortion or other malicious purposes, particularly if individuals wish to keep their access to certain content or websites private".[21]

The Electronic Frontier Foundation (EFF), a prominent digital rights organization, has unequivocally stated that "online age verification is incompatible with privacy." They emphasize that hacks and data breaches of sensitive information, such as government-issued IDs, are "not a hypothetical concern; it is simply a matter of when the data will be exposed".[17] EFF explicitly lists data breaches as leading to dangers like "phishing, blackmail, or identity theft, in addition to the loss of anonymity and privacy".[17]

Beyond the immediate threats of data breaches and blackmail, the consistent warnings from experts like Jason Nurse and EFF about centralized databases and the inevitability of breaches point to a deeper, systemic issue.[17] OTI's broader critique that age verification "should not be overused" and "poses great risks to free, open, and anonymous web use" [20] suggests that the widespread implementation of such systems could normalize the routine collection of highly sensitive PII for accessing common online services. This normalization erodes the expectation of online anonymity and privacy, making individuals more susceptible to surveillance, whether by state actors or malicious entities. The article's reference to an "Orwellian instinct" [11] is directly pertinent here, as it speaks to a societal shift towards ubiquitous digital monitoring. The Online Safety Act, by mandating data-intensive age verification, inadvertently contributes to a societal trend where privacy becomes a privilege, not a right, for online engagement. This could have a chilling effect on free expression [9] by creating a traceable link between an individual's identity and their online activities, potentially deterring users from accessing legal but sensitive content or expressing unpopular opinions, thereby undermining the very democratic principles a free

internet is meant to uphold.

## 3. A Futile Effort: Circumvention, Shadow Sites, and the Streisand Effect

### 3.1 The VPN Paradox: Bypassing Age Verification and Surging VPN Use

The user's article directly challenges the efficacy of the OSA's age verification, asserting its "utter futility" because "most tech-savvy children know how to use a VPN, a tool that renders any country-specific age verification completely pointless".[11] This prediction has been rapidly substantiated by real-world data, demonstrating a significant flaw in the Act's design.

Immediately following the OSA's implementation on July 25, 2025, the use of Virtual Private Network (VPN) services in the UK dramatically skyrocketed. Top10VPN, a service monitoring global VPN traffic, reported an astounding 1,327% spike in UK VPN traffic on July 25 compared to the prior four-week daily average. This surge continued, increasing by 1,712% on July 26 and nearly 2,000% by July 27.[23] Other prominent VPN providers, like Proton VPN and Windscribe, also reported massive spikes in UK sign-ups and traffic, further confirming the widespread adoption of these circumvention tools.[23]

Despite UK Science Secretary Peter Kyle's attempts to downplay the significance of VPN use, Ofcom's own data indicates a substantial demand for adult content among minors: 8% of children aged 8-14 in the UK access online pornography monthly, with this figure rising to one in five boys in that age bracket.[23] This directly contradicts the notion that "very few children" are seeking harmful content online and underscores the underlying motivation for circumvention. VPNs function by changing a user's virtual location and masking their IP address, thereby allowing them to appear as if they are browsing from a country without strict age verification requirements.[24] This technical capability renders country-specific age-gating measures largely ineffective. This phenomenon is not unique to the UK; similar effects have been observed in the United States. Following the passage of age verification laws in states like Texas and

Louisiana, VPN service providers reported significant increases in traffic (275% and 210% respectively), demonstrating a consistent pattern of circumvention.[24]

The immediate and massive surge in VPN usage directly after the OSA's implementation demonstrates that users, particularly those determined to access restricted content, will quickly find and adopt technical workarounds.[23] The article itself predicts this, stating, "This loophole will doubtless be closed, but new ones will be found just as quickly".[9] This highlights a fundamental "whack-a-mole" dynamic inherent in attempts to control online content through technical barriers: for every restriction imposed, a new method of circumvention emerges. This renders the initial regulation ineffective in its core goal of preventing access. The Online Safety Act's reliance on technical barriers for age verification is fundamentally flawed because the decentralized and rapidly evolving nature of the internet will always provide means of bypass. This leads to an endless, costly, and ultimately ineffective cycle of regulation and circumvention, failing to address the underlying issues of online safety and instead fostering a cat-and-mouse game with users.

### 3.2 The Rise of "Shadow Sites": Unregulated Content and Malware Risks

The user's article warns that the Online Safety Act, rather than creating a safer online environment, will likely achieve the opposite by forcing young people to find "alternative, and often far more dangerous, ways to bypass the restrictions".[11] This will lead to the proliferation of "the most depraved, extreme, and malware-ridden sites—those outside the jurisdiction of Ofcom".[11]

Commentators have echoed this concern, noting that the policy will result in a rise in "shadow sites" from countries outside UK jurisdiction that "don't care about the laws regarding model consent/age verification either".[11] This implies a shift towards platforms with even fewer ethical or legal safeguards. The risks associated with such unregulated "shadow sites" are well-documented in cybersecurity literature. Similar to "shadow IT" or "shadow AI," these unauthorized tools and services often operate outside an organization's (or in this case, a country's regulatory) security standards, thereby introducing significant vulnerabilities that can lead to data breaches, malware infections, or ransomware attacks.[26] Specifically, these unregulated sites are prone to lacking strong authentication mechanisms, utilizing insecure data transmission methods (such as unencrypted connections), and having inadequate logging and monitoring capabilities. These deficiencies collectively increase the risks of

unauthorized access to sensitive information and broader data leakage.[26]

By making mainstream, regulated sites difficult to access for minors through stringent age verification, the Online Safety Act does not eliminate the underlying demand for age-restricted content. Instead, it displaces this demand to less regulated, more dangerous corners of the internet.[9] This is a classic example of risk displacement, where an attempt to control a problem in one area merely pushes it into another, often more harmful, domain. These "shadow sites" are inherently less secure, more likely to host malware, and operate without the ethical or legal constraints of regulated platforms.[26] The Act, in its attempt to "protect" children by restricting access to certain content on regulated platforms, may perversely expose them to

*greater* and more insidious harms. This includes increased exposure to extreme content, malware, and exploitation in environments where there are no safeguards, no content moderation, and significantly elevated cybersecurity threats, directly contradicting the Act's stated purpose of enhancing online safety.

### 3.3 The Streisand Effect: Unintended Amplification of Restricted Content

The user's article posits that the Online Safety Act will likely achieve the opposite of its stated intent through the well-documented phenomenon known as the "Streisand effect".[11] This effect describes a situation where an attempt to censor, hide, or otherwise draw attention away from something only serves to attract significantly more attention to it.[28] This counterproductive outcome is amplified by the rapid dissemination capabilities of the internet and social media.

Classic examples powerfully illustrate this effect:

- In 2003, Barbra Streisand's lawsuit to remove an aerial photograph of her house from a public online database inadvertently caused the photo, which had only been downloaded six times (twice by her own lawyers), to be viewed over 400,000 times and widely reposted across news sites and the internet.[29]
- Similarly, in 2012, a UK high court order to ban access to The Pirate Bay, a Swedish file-sharing site, resulted in a dramatic increase of more than 10 million visits to the site following extensive media coverage of the ruling.[29]
- In 2013, the French domestic spy agency's attempt to force Wikipedia to delete an article about a French air force base ultimately led to the article becoming the most-viewed entry on the French version of Wikipedia, as news of the censorship

attempt spread across the internet.[29]

Scholars and commentators note that censorship often backfires when the public perceives an attempt by a powerful person or organization to repress free speech. This perception can incite public outrage, particularly if the story involves an underdog, and often spurs curiosity, driving people to seek out the very content that has been singled out for suppression.[29]

The Streisand Effect is not merely a technical bypass mechanism; it is a profound psychological and sociological phenomenon. When content is explicitly restricted or attempts are made to hide it, it gains a "forbidden fruit" appeal, and the act of censorship itself can be perceived as an overreach by powerful authorities.[29] This perception can trigger public outrage, especially when framed as an attack on free speech, and significantly spur curiosity among users who might not have otherwise sought out the content.[29] The article's mention of "emotional blackmail" and the government's "moralizing lecture" [11] implies this very dynamic. The Online Safety Act's restrictive approach risks generating a significant cultural and psychological backlash. By attempting to control access to certain content, the Act could inadvertently legitimize, amplify, and make more appealing the very material it seeks to suppress, particularly among young people. This counterproductive outcome directly undermines the Act's foundational goal of protecting children by making restricted content more desirable and sought after.

## 4. The Insidious Underbelly: Stalkerware, Cybercrime, and Legal Loopholes

### 4.1 The Commercial Stalkerware Industry: Scale and Accessibility

The user's article accurately characterizes the commercial stalkerware industry as a "multi-billion dollar industry".[11] This assessment is corroborated by Digital Forensics Instructor Lodrina Cherne, who confirms that the spyware industry is "on the rise" and generates "around five billion dollars a year".[30] Cherne further details that a significant portion of this revenue is "supported by individual people: overbearing parents,

authoritarian bosses, and most of all, jealous and abusive romantic partners" [30], directly aligning with the article's "dark trifecta" description.[11]

Stalkerware is commercially available software designed for covert surveillance, allowing perpetrators to secretly monitor an individual's private life via their mobile device without their knowledge or consent.[31] The capabilities of such software are extensive, enabling the tracking of a victim's location, monitoring of calls, reading text messages and emails, viewing photos and videos, and observing web browsing activity.[32] Crucially, these programs are "easy to buy and install" and are designed to run hidden in the background, making them difficult for victims to detect.[32] This accessibility contributes significantly to their widespread misuse.

The article notes that stalkerware companies "often advertise their software as a 'legitimate' way to monitor children or employees".[11] Lodrina Cherne's observation that a simple Google search for "How do I track my kids?" can lead to a long list of programs that "purport to be legitimate monitoring software," when in fact they are part of the "much shadier stalkerware industry" [11], directly illustrates this deceptive marketing. This facade allows the industry to operate in a legal grey area, exploiting the desire for parental oversight or employee monitoring to sell tools that are fundamentally designed for covert, non-consensual surveillance. The legal ambiguity and the widespread marketing of stalkerware as "legitimate" tools for oversight create a significant regulatory challenge. This deceptive framing enables abusive practices under the guise of safety or management, highlighting a profound hypocrisy where "child safety" is used as a catch-all justification for measures that, in reality, enable privacy violations and abuse, as argued in the user's article.[11]

### 4.2 Stalkerware's Role in Domestic Abuse: Alarming Statistics

The user's article cites a poll by the National Network to End Domestic Violence (NNEDV) finding that "54% of domestic abuse victims were being tracked by their abusers using spyware".[11] This alarming statistic is further substantiated by multiple research findings. NNEDV reports indicate that a staggering 97% of family violence survivors report "experiencing harassment, monitoring, and threats by abusers through the misuse of technology".[35] More specifically, 71% of abusers monitor survivors' activities, and 54% explicitly downloaded stalkerware onto their partners' devices.[35]

Recent data from Kaspersky, a cybersecurity firm, reveals the persistent and growing nature of this problem: 31,031 unique individuals globally were affected by stalkerware in 2023, representing an almost six percent (5.8%) year-on-year increase from 2022's figure of 29,312 affected users.[31] This reversal of a previous downward trend confirms that digital stalking remains a global and escalating issue.[36] While Kaspersky's data is anonymized, other research consistently shows that it is predominantly women who are affected by this form of digital violence.[31]

The user's article argues that the OSA, ostensibly designed to protect the vulnerable, could "become the source of unimaginable harm" by creating a new, massive pool of sensitive data for criminals.[11] The extensive statistics on stalkerware [11] demonstrate that technology-facilitated abuse is a clear, widespread, and escalating danger. If the OSA's age verification provisions lead to more sensitive data being collected and stored, it could inadvertently fuel this existing problem by providing more attractive targets for data theft, which can then be leveraged for stalking, harassment, or blackmail, thus exacerbating a pre-existing severe societal issue rather than mitigating it. The government's legislative focus on age verification for explicit content, while framed as a child protection measure, may be diverting attention and resources from more prevalent and severe forms of digital harm, such as technology-facilitated domestic abuse. This policy choice risks creating a new layer of vulnerability for individuals by increasing the availability of sensitive data, thereby potentially exacerbating the very harms it claims to prevent.

### 4.3 The "Slap on the Wrist": Inadequate Legal Precedent and Enforcement for Stalkerware Vendors

The user's article critically points out that legal cases against commercial stalkerware companies, such as CyberSpy Software and StealthGenie, have seemingly set a judicial precedent that selling such dangerous software warrants only a "slap on the wrist".[11] This suggests a systemic failure in legal accountability.

A specific example supporting this critique is the case of Hamad Akbar, the owner of StealthGenie. He was fined $500,000 and, crucially, "ordered to give the product's source code to the government," rather than having it destroyed.[37] This was a landmark case, being the first criminal case of its kind against a stalkerware vendor.[37] The fact that the source code was

*acquired* by the government rather than eliminated raises questions about potential state interest in the technology itself.

The Electronic Frontier Foundation (EFF), a prominent digital rights organization, has acknowledged that while recent enforcement actions, such as a $410,000 fine against a stalkerware maker and a ban on SpyFone's CEO from the surveillance business, are "welcome," they also emphasize that "more work remains." EFF highlights that the business of selling spyware and stalkerware continues to present "lucrative opportunities" and that many players in this industry are "not as easy to impose penalties on or even identify".[38] This indicates that current legal measures are insufficient to deter the industry effectively.

The legal cases against stalkerware vendors [11] illustrate the profound difficulty in effectively prosecuting companies that market tools with "legitimate" monitoring applications (e.g., parental control) but are frequently misused for abuse.[11] The core issue is that these technologies are "dual-use" [40]—they possess both acceptable and unacceptable applications. The legal system struggles to draw a clear line between the sale of the tool and its subsequent misuse, often resulting in penalties perceived as a "slap on the wrist." The specific outcome of the StealthGenie case, where the source code was handed over to the government instead of being destroyed [11], further complicates this, hinting at a potential strategic interest by state actors in acquiring or understanding such technologies. The current legal framework is demonstrably insufficient to effectively curb the commercial stalkerware industry. This inadequacy is partly due to the inherent dual-use nature of the technologies and a potential systemic reluctance to fully dismantle a market that may offer tangential benefits or insights for state surveillance capabilities. This permissive environment allows the industry to continue thriving, posing ongoing and escalating risks to individual privacy and safety, a systemic problem the OSA fails to address.

## 5. Erosion of Freedoms: Collateral Damage to Expression and Privacy

### 5.1 The Chilling Effect on Legitimate Speech and Information Access

The user's article strongly critiques the Online Safety Act, labeling it "unnecessary, stupid, and orwellian," and questions the rationale behind sacrificing citizens' rights and data for a measure that is unlikely to be effective.[11] This sentiment is widely echoed by civil liberties groups and legal experts.

The Index on Censorship, a prominent free expression advocacy organization, states that the Act "risks overreach, creating a chilling effect on legitimate speech." They warn that it "opens up too many avenues for increased surveillance and monitoring, all of which fosters an environment of self-censorship, stifles open dialogue and erodes the right to free expression and access to information".[9] This highlights the Act's potential to suppress lawful discourse by incentivizing platforms to over-moderate content to avoid hefty fines.[21]

A particularly concerning aspect is the Act's age limitations, which specifically target young people. Critics argue this has the potential to limit minors' access to information and their ability to participate in democratic life, especially pertinent given discussions about lowering the voting age.[9] Legal analysis further corroborates these concerns, indicating that the Bill "will significantly curtail freedom of expression" and grants the Secretary of State "unprecedented powers to curtail freedom of expression with limited parliamentary scrutiny".[22] This concentration of power raises serious questions about checks and balances and the potential for political interference in online content.

The analysis also suggests that the Act enforces "pro-active state-enforced censorship by algorithm," which is deemed to have "questionable legality".[22] This is due to the inherent lack of transparency in algorithmic processes, meaning citizens will be "deprived of the ability to understand how their speech online is being curtailed".[22] The Act's shift of content moderation "under statute" [22] means that private platforms are now exercising public law functions, effectively becoming arbiters of free speech. This, coupled with the explicit push for "pro-active state-enforced censorship by algorithm" [22], represents a profound and troubling transformation of online governance. The inherent opacity of algorithms means that citizens will be "deprived of the ability to understand how their speech online is being curtailed" [22], directly supporting the article's "Orwellian" critique.[11] This lack of transparency and accountability in algorithmic decision-making fundamentally undermines the principles of due process and free expression in a democratic society. This legislative framework risks normalizing a pervasive system of opaque, automated censorship where the boundaries of permissible speech are determined by private

companies under statutory pressure, rather than by clear, publicly debated legal standards. This could have a severe chilling effect on free expression, limit access to diverse information, and disproportionately impact the ability of younger generations to engage in democratic discourse and civic participation, ultimately eroding the foundational principles of an open internet.

### 5.2 Case Study: The Wikimedia Foundation's Challenge to OSA Categorization

The user's article briefly references the legal case involving Wikipedia, where "lawyers floated the idea of a monthly quota for UK users to keep it below the Category 1 threshold".[11] This case serves as a critical real-world example of the Online Safety Act's unintended "collateral damage" to public interest platforms.

The Wikimedia Foundation, the non-profit organization that operates Wikipedia and other Wikimedia projects, has launched a formal legal challenge against the OSA's Categorisation Regulations. They argue that these regulations "endanger Wikipedia and the global community of volunteer contributors who create the information on the site".[41] Despite being a non-profit, public interest project, Wikipedia falls under the Act's most stringent obligations (Category 1) due to its immense volume of monthly users.[43] This categorization is based on "functionalities and user numbers, not perceived risks" [44], illustrating a "one-size-fits-all" regulatory approach that fails to distinguish between commercial platforms and encyclopedic resources.

The core concern is that Category 1 demands would require identity verification of many Wikipedia contributors.[41] The Wikimedia Foundation argues this would "undermine the privacy and safety of Wikipedia's volunteer contributors," exposing them to "data breaches, stalking, lawsuits, or even imprisonment by authoritarian regimes".[41] This requirement also threatens to "expose the encyclopedia to manipulation and vandalism" and divert "essential resources from protecting people and improving Wikipedia".[41] The foundation maintains that the privacy of its volunteers is central to their safety and ability to contribute freely.[41]

The Wikimedia Foundation's legal challenge is particularly significant as it is the first against the OSA's Categorisation Regulations and includes a UK-based volunteer editor as a joint claimant, highlighting the direct impact on individuals.[41] The case underscores how broad legislation can inadvertently penalize and threaten platforms that serve a vital public good, forcing them to adopt measures that contradict their

core principles of open knowledge and anonymity.[43] The judge presiding over the case has even warned of potential "political consequences" if the legislation leads to Wikipedia becoming unavailable for UK users, and the site's lawyers have considered a "monthly quota" for UK users to avoid Category 1 thresholds.[44] This illustrates the absurd lengths to which a public good might have to go to avoid the unintended consequences of the Act.

The Wikimedia case highlights a critical flaw in the OSA's design: its broad scope and categorical approach fail to differentiate between platforms based on their function, content, or risk profile. By applying the same stringent obligations to a non-profit, public knowledge platform as to high-risk commercial sites, the Act demonstrates a fundamental misunderstanding of the internet's diverse ecosystem. This lack of nuance means that well-intentioned legislation can inadvertently impose disproportionate burdens and create severe, unforeseen risks for beneficial online services. This failure to adequately distinguish between different types of online services can lead to the suppression of valuable, legitimate content and activities, thereby undermining the very principles of free expression and access to information that are crucial for a healthy digital society.

## 6. The Broader Critique: Orwellian Instinct and Intertwined Surveillance

### 6.1 Government's "Orwellian Instinct" and Corporate Responsibility

The user's article describes the Online Safety Act as a symptom of a larger, troubling trend, characterizing the government's default attitude towards online activity as an "Orwellian instinct" to "track it, police it, and restrict it".[11] This perspective suggests a fundamental shift in governance towards pervasive digital monitoring.

A key concern is the government's perceived inclination to "foist the responsibility of policing onto corporations who are ill-equipped for the task and have no vested interest in securing the data they now hold".[11] This approach effectively privatizes censorship and surveillance, placing the burden of enforcement on entities that may

prioritize profit and compliance over user privacy and security. The inherent "wild west" nature of the web means that "things will inevitably go wrong" [11], yet the Act continues to "trample on" citizens' rights and put their data at risk for measures that are unlikely to work.[11]

The Act's broad scope and the significant fines for non-compliance [2] create a strong incentive for platforms to err on the side of caution, leading to over-moderation and a chilling effect on legitimate speech.[9] This dynamic transforms private companies into de facto state enforcers, blurring the lines between corporate responsibility and governmental control. The normalization of algorithmic censorship, as discussed previously, further entrenches this "Orwellian" tendency, where opaque systems determine the boundaries of permissible online expression.

### 6.2 The Intertwined Nature of Government and Commercial Spyware Industries

The user's article posits a "deeper, and more sinister, reason" for the Online Safety Act's flaws, suggesting a vested government self-interest in the commercial spyware market. It cites the Malicious Life podcast, which reveals that there is "no such thing as two separate government and consumer spyware industries; they are 'one industry, continuous, messy, intertwined'".[11] This assertion points to a symbiotic relationship that undermines public trust and privacy.

The evidence supporting this claim is compelling. Shady conventions like the ISS World Conference, which explicitly bar journalists and host negotiations in backrooms [11], serve as marketplaces for surveillance technology. Here, companies like Hacking Team and Gamma International—dubbed the "McDonalds and Burger King of spyware"—sell state-level surveillance tools to a global clientele, including repressive regimes and stable democracies alike.[11]

The critical connection lies in the links between these high-end state surveillance companies and the consumer-level spyware market. Hacking Team, for instance, openly admits to being in business with multiple consumer spyware companies like mSpy and Mobile Spy.[11] They even use consumer apps for market research, "to verify that they don’t introduce any feature we are interested in".[11] This indicates a continuous flow of technology, talent, and intelligence between the two sectors. The commercial spyware industry, therefore, serves as a talent pool for developers and engineers, and a testing ground for new surveillance technologies that can eventually

be scaled up for state use.[11]

This intertwined relationship explains why the law appears "soft on these companies".[11] Legal cases against commercial stalkerware vendors, such as CyberSpy Software and StealthGenie, have resulted in what is perceived as a "slap on the wrist".[11] The case of StealthGenie's owner, Hamad Akbar, who was ordered to hand over his source code to the U.S. government rather than destroy it [11], is particularly telling. This outcome suggests that the government's interest lies not in dismantling the industry, but in acquiring its capabilities and maintaining its viability. This is not mere incompetence; it suggests a system where powerful entities are enabled at the expense of individual privacy and security. The Online Safety Act, in this light, becomes not a genuine solution to online harms, but a convenient and cynical diversion from systemic problems that the government is unwilling to address, possibly due to its own vested interests in the broader surveillance ecosystem.

## 7. The Way Forward

The Online Safety Act, in its current form, represents a legislative misstep, prioritizing a superficial appearance of safety over genuine digital security and fundamental freedoms. The Act's reliance on mandatory age verification, while ostensibly aimed at child protection, inadvertently creates massive repositories of sensitive personal data, transforming user information into a "gold mine" for cybercriminals. The pervasive and increasing threat of data breaches, coupled with the inherent vulnerabilities of third-party age verification services, makes the compromise of this data not a hypothetical risk, but an inevitable consequence. Such breaches can lead to widespread blackmail, identity theft, and the exacerbation of technology-facilitated abuse, particularly through stalkerware, which continues to thrive due to inadequate legal enforcement and its deceptive "legitimate use" facade.

Furthermore, the Act's technical restrictions are demonstrably futile. The immediate and dramatic surge in VPN usage post-implementation illustrates how easily determined users can bypass age-gating measures, leading to a "whack-a-mole" problem that wastes resources and fails to achieve its core objective. Worse, this approach risks displacing users to unregulated "shadow sites" that are inherently more dangerous, lacking any safeguards against extreme content or malware. The chilling effect on legitimate speech and information access, exemplified by the

Wikimedia Foundation's legal challenge, demonstrates how broad, undifferentiated legislation can inadvertently penalize public interest platforms and erode foundational principles of free expression and anonymity. The underlying issue appears to be a systemic "Orwellian instinct" within government, compounded by an intertwined relationship with the commercial spyware industry, where state interests in surveillance may inadvertently perpetuate a permissive environment for privacy-invasive technologies.

Genuine online safety cannot be achieved through a heavy-handed, restrictive, and data-intensive legislative approach. Instead, a more nuanced and effective strategy must focus on empowering individuals and fostering a resilient digital environment.

**Recommendations:**

1. **Prioritize Digital Literacy and Critical Thinking Education:** Instead of erecting technological barriers, invest significantly in comprehensive digital literacy programs for children, parents, and educators. These programs should teach critical thinking skills, responsible online behavior, risk assessment, and how to identify and navigate harmful content.[11] Education empowers individuals to make informed choices and build digital resilience, a far more robust defense than external restrictions.[11]
2. **Promote Parental Involvement and Open Dialogue:** Emphasize and support parental responsibility through resources and guidance that encourage frank, consistent conversations with children about internet safety.[11] Acknowledge the limitations of technological controls and advocate for a mediation-based approach where parental controls are integrated into broader parent-child relationships rather than serving as a standalone solution.[62]
3. **Mandate Privacy-Preserving Age Verification Technologies:** If age verification is deemed absolutely necessary, prioritize and mandate the use of privacy-preserving technologies such as "zero-knowledge proofs".[11] These technologies can verify age without requiring users to disclose sensitive personal identifiers or exact age, thereby minimizing data collection and reducing the risk of creating data honeypots.[19] This would involve a "double-blind architecture" where age verification is separated from content access, ensuring no single entity links identity to browsing behavior.[13]
4. **Strengthen Legal Accountability for Malicious Spyware/Stalkerware:** Implement more robust and deterrent legal frameworks and enforcement actions against commercial stalkerware vendors. This includes clearer definitions for dual-use technologies, stricter penalties for illicit sales or misuse, and a commitment to dismantling rather than acquiring the capabilities of companies

that facilitate abuse.[11]

5. **Re-evaluate the Act's Scope and Proportionality:** Conduct a thorough review of the Online Safety Act's categorization regulations, ensuring that public interest projects, journalistic content, and non-commercial platforms are not unduly burdened or inadvertently harmed by regulations designed for high-risk commercial entities.[41] Legislation should be "narrowly tailored" to avoid infringing on constitutionally protected speech and access to information.[20]
6. **Increase Transparency in Government Surveillance and Corporate Policing:** Demand greater transparency regarding the intertwining of government and commercial surveillance industries. Any legislative framework should include robust safeguards against algorithmic censorship and ensure clear, accessible mechanisms for users to understand and challenge content moderation decisions, thereby upholding democratic principles and freedom of expression.[22]

The internet, in its essence, was built on principles of freedom and exploration. To attempt to "put the genie back in the bottle" now with flawed and dangerous legislation is an act of folly.[11] True protection lies not in new laws that centralize data and restrict access, but in empowering individuals with knowledge, fostering responsible digital citizenship, and upholding the fundamental rights to privacy and freedom of expression in the digital age.

**Works cited**


1. Online Safety Act 2023 - Wikipedia, accessed August 1, 2025, https://en.wikipedia.org/wiki/Online_Safety_Act_2023
2. Online Safety Act - GOV.UK, accessed August 1, 2025, https://www.gov.uk/government/collections/online-safety-act
3. Age checks to protect children online - Ofcom, accessed August 1, 2025, https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-to-protect-children-online
4. Guidance on highly effective age assurance | Ofcom, accessed August 1, 2025, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=395680
5. A safer space – the UK's progress on online safety - Taylor Wessing, accessed August 1, 2025, https://www.taylorwessing.com/de/interface/2025/online-safety-update/a-safer-space-the-uks-progress-on-online-safety
6. Welcome to the Era of Online Age Verification. Are You Ready to Identify Yourself? - CNET, accessed August 1, 2025, https://www.cnet.com/tech/services-and-software/welcome-to-the-era-of-online-age-verification-are-you-ready-to-identify-yourself/

7. Online age checks now in force - Ofcom, accessed August 1, 2025, https://www.ofcom.org.uk/online-safety/protecting-children/online-age-checks-must-be-in-force-from-tomorrow
8. Age checks for online safety – what you need to know as a user - Ofcom, accessed August 1, 2025, https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-for-online-safety--what-you-need-to-know-as-a-user
9. Free expression concerns over Online Safety Act's age verification requirements, accessed August 1, 2025, https://www.indexoncensorship.org/2025/07/free-expression-concerns-over-online-safety-acts-age-verification-requirements/
10. 'Pure madness to share personal data with porn sites': Readers react to new online safety rules | The Independent, accessed August 1, 2025, https://www.independent.co.uk/tech/online-safety-laws-act-uk-porn-data-b2799435.html
11. The Online Safety Act - A Hammer to Crack a Walnut.docx
12. Age Assurance Explained: Ofcom's Online Safety Guidelines - Ondato, accessed August 1, 2025, https://ondato.com/blog/ofcom-age-assurance/
13. Age verification: Child protection or privacy risk? - Malwarebytes, accessed August 1, 2025, https://www.malwarebytes.com/blog/news/2025/07/age-verification-child-protection-or-privacy-risk
14. UK's New Online Safety Act: What Consumers Need to Know | McAfee Blog, accessed August 1, 2025, https://www.mcafee.com/blogs/internet-security/uks-new-online-safety-act-what-consumers-need-to-know/
15. 110+ of the Latest Data Breach Statistics [Updated 2025] - Secureframe, accessed August 1, 2025, https://secureframe.com/blog/data-breach-statistics
16. Healthcare Data Breach Statistics - The HIPAA Journal, accessed August 1, 2025, https://www.hipaajournal.com/healthcare-data-breach-statistics/
17. Hack of Age Verification Company Shows Privacy Danger of Social Media Laws, accessed August 1, 2025, https://www.eff.org/deeplinks/2024/06/hack-age-verification-company-shows-privacy-danger-social-media-laws
18. Age verification for risky sites comes into force in the UK - Computing UK, accessed August 1, 2025, https://www.computing.co.uk/news/2025/age-verification-comes-into-force-in-the-uk-for-risky-sites
19. Are 'zero-knowledge proofs' the future of online age verification? - StateScoop, accessed August 1, 2025, https://statescoop.com/report-zero-knowledge-future-of-age-verification-tech-2025/
20. Age verification needs better privacy protections, report says - Route Fifty, accessed August 1, 2025, https://www.route-fifty.com/cybersecurity/2025/07/age-verification-needs-better

-privacy-protections-report-says/406924/
21. The Online Safety Act is a security and compliance minefield - Raconteur, accessed August 1, 2025, https://www.raconteur.net/technology/the-online-safety-act-is-a-security-and-compliance-minefield
22. A LEGAL ANALYSIS OF THE IMPACT OF THE ONLINE SAFETY BILL ON FREEDOM OF EXPRESSION | Matrix Chambers, accessed August 1, 2025, https://www.matrixlaw.co.uk/wp-content/uploads/2022/05/Legal-analysis-of-the-impact-of-the-Online-Safety-Bill-on-freedom-of-expression.pdf
23. VPN use rises following Online Safety Act's age verification controls - Malwarebytes, accessed August 1, 2025, https://www.malwarebytes.com/blog/uncategorized/2025/07/vpn-use-rises-following-online-safety-acts-age-verification-controls
24. Online Safety Laws Could Backfire in Major Ways - R Street Institute, accessed August 1, 2025, https://www.rstreet.org/commentary/online-safety-laws-could-backfire-in-major-ways/
25. Best VPNs to Bypass Age Verification in 2025 - Cybernews, accessed August 1, 2025, https://cybernews.com/best-vpn/vpn-for-age-verification/
26. What Is Shadow IT? - Palo Alto Networks, accessed August 1, 2025, https://www.paloaltonetworks.com/cyberpedia/shadow-it
27. Hidden Risks of Shadow AI - Varonis, accessed August 1, 2025, https://www.varonis.com/blog/shadow-ai
28. The Streisand Effect: Understanding its Impact on Online Reputation Management, accessed August 1, 2025, https://www.netreputation.com/streisand-effect-online-reputation/
29. Streisand effect | Definition, Meaning, Examples, & Origin - Britannica, accessed August 1, 2025, https://www.britannica.com/topic/Streisand-effect
30. Malicious Life Podcast: How is Spyware Even Legal? - Cybereason, accessed August 1, 2025, https://www.cybereason.com/blog/malicious-life-podcast-how-is-spyware-legal
31. Digital violence through stalkerware showing little sign of slowing according to new Kaspersky report, accessed August 1, 2025, https://www.kaspersky.com/about/press-releases/digital-violence-through-stalkerware-showing-little-sign-of-slowing-according-to-new-kaspersky-report
32. How to find and remove Stalkerware - Malwarebytes, accessed August 1, 2025, https://www.malwarebytes.com/stalkerware
33. What is stalkerware? Detect and remove it - ExpressVPN, accessed August 1, 2025, https://www.expressvpn.com/blog/staying-safe-from-stalkerware/
34. Stalkerware: What To Know | Consumer Advice, accessed August 1, 2025, https://consumer.ftc.gov/articles/stalkerware-what-know
35. Technology Abuse - Family Violence Unit - City of Houston, accessed August 1, 2025, https://www.houstontx.gov/police/fvu/technology_abuse.htm
36. Global Kaspersky report reveals digital violence has increased, accessed August 1, 2025,

https://www.kaspersky.com/about/press-releases/global-kaspersky-report-reveals-digital-violence-has-increased
37. Spyware: What you don't know can hurt you | Boothbay Register, accessed August 1, 2025, https://www.boothbayregister.com/print_boothbay_register/article/spyware-what-you-don-t-know-can-hurt-you/47836
38. Stalkerware Maker Fined $410k and Compelled to Notify Victims, accessed August 1, 2025, https://www.eff.org/deeplinks/2023/02/stalkerware-maker-fined-410k-and-compelled-notify-victims
39. Understanding The StealthGenie Indictment - FlexiSPY Blog, accessed August 1, 2025, https://blog.flexispy.com/stealthgenie-vs-united-states-america/
40. Legal and Policy Responses to Spyware: A Primer | TechPolicy.Press, accessed August 1, 2025, https://www.techpolicy.press/legal-and-policy-responses-to-spyware-a-primer/
41. Wikimedia Foundation Challenges UK Online Safety Act Regulations, accessed August 1, 2025, https://wikimediafoundation.org/news/2025/07/17/wikimedia-foundation-challenges-uk-online-safety-act-regulations/
42. Wikimedia Foundation challenges Online Safety Act Regulations | Scottish Legal News, accessed August 1, 2025, https://www.scottishlegal.com/articles/wikimedia-foundation-challenges-online-safety-act-regulations
43. Wikipedia seeks to shield contributors from UK law targeting online anonymity, accessed August 1, 2025, https://www.courthousenews.com/wikipedia-seeks-to-shield-contributors-from-uk-law-targeting-online-anonymity/
44. UK high court hears Wikipedia suit against Online Safety Act category rules, accessed August 1, 2025, https://www.biometricupdate.com/202507/uk-high-court-hears-wikipedia-suit-against-online-safety-act-category-rules
45. Surveillance trade shows: which government agencies attend? | News | theguardian.com, accessed August 1, 2025, https://www.theguardian.com/news/datablog/2012/feb/07/surveillance-shows-attendees-iss-world
46. ISS WORLD Americas - Conference Agenda, accessed August 1, 2025, https://www.issworldtraining.com/iss_wash/
47. Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights - Atlantic Council, accessed August 1, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/
48. Print - National Security Institute - George Mason University, accessed August 1, 2025, https://nationalsecurity.gmu.edu/media-appearances/print/

49. Monitoring the Lines - Collin Anderson, accessed August 1, 2025, https://cda.io/notes/monitoring-the-lines/
50. Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim, accessed August 1, 2025, https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim
51. Mapping Hacking Team's “Untraceable” Spyware - The Citizen Lab, accessed August 1, 2025, https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/
52. misp-galaxy/clusters/surveillance-vendor.json at main - GitHub, accessed August 1, 2025, https://github.com/MISP/misp-galaxy/blob/main/clusters/surveillance-vendor.json
53. [UPDATED] Mobile spying software company mSpy hacked – customer data posted on deep web - IT Governance USA Blog, accessed August 1, 2025, https://www.itgovernanceusa.com/blog/mobile-spying-software-company-mspy-hacked-customer-data-posted-on-deep-web
54. Dangerous monitoring tool mSpy suffers data breach, exposes customer details, accessed August 1, 2025, https://www.malwarebytes.com/blog/news/2024/07/dangerous-monitoring-tool-mspy-suffers-data-breach-exposes-customer-details
55. Popular mSpy Smartphone Parental Control App gets Hacked | Pinnacle Financial Partners, accessed August 1, 2025, https://pnfp.com/learning-center/fraud-and-security/fraud-and-security-alerts/popular-mspy-smartphone-parental-control-app-gets-hacked/
56. Teaching online safety in schools - GOV.UK, accessed August 1, 2025, https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools
57. Online safety education - POST Parliament, accessed August 1, 2025, https://post.parliament.uk/research-briefings/post-pn-0608/
58. Digital Citizenship - Intuitive Thinking Skills, accessed August 1, 2025, https://www.intuitivethinkingskills.co.uk/digital-citizenship/
59. About the programme - Childnet Digital Leaders Guest Platform, accessed August 1, 2025, https://digital-leaders.childnet.com/about-the-programme/
60. Case studies - UKCIS Digital Resilience Working Group, accessed August 1, 2025, https://www.drwg.org.uk/case-studies
61. Was bored so here's two reasons parental controls are bad for kids. - Reddit, accessed August 1, 2025, https://www.reddit.com/r/parentalcontrols/comments/1l9kp3q/was_bored_so_heres_two_reasons_parental_controls/
62. Do parental control tools fulfil family expectations for child protection ..., accessed August 1, 2025, https://www.tandfonline.com/doi/full/10.1080/17482798.2023.2265512
63. Petition: Repeal the Online Safety Act : r/Scotland - Reddit, accessed August 1, 2025, https://www.reddit.com/r/Scotland/comments/1m7j02v/petition_repeal_the_online

_safety_act/
64. Age assurance and privacy: Regulatory trends in youth online protection | IAPP, accessed August 1, 2025, https://iapp.org/news/a/age-assurance-and-privacy-regulatory-trends-in-youth-online-protection