



**Computer & Communications
Industry Association**
Open Markets. Open Systems. Open Networks.

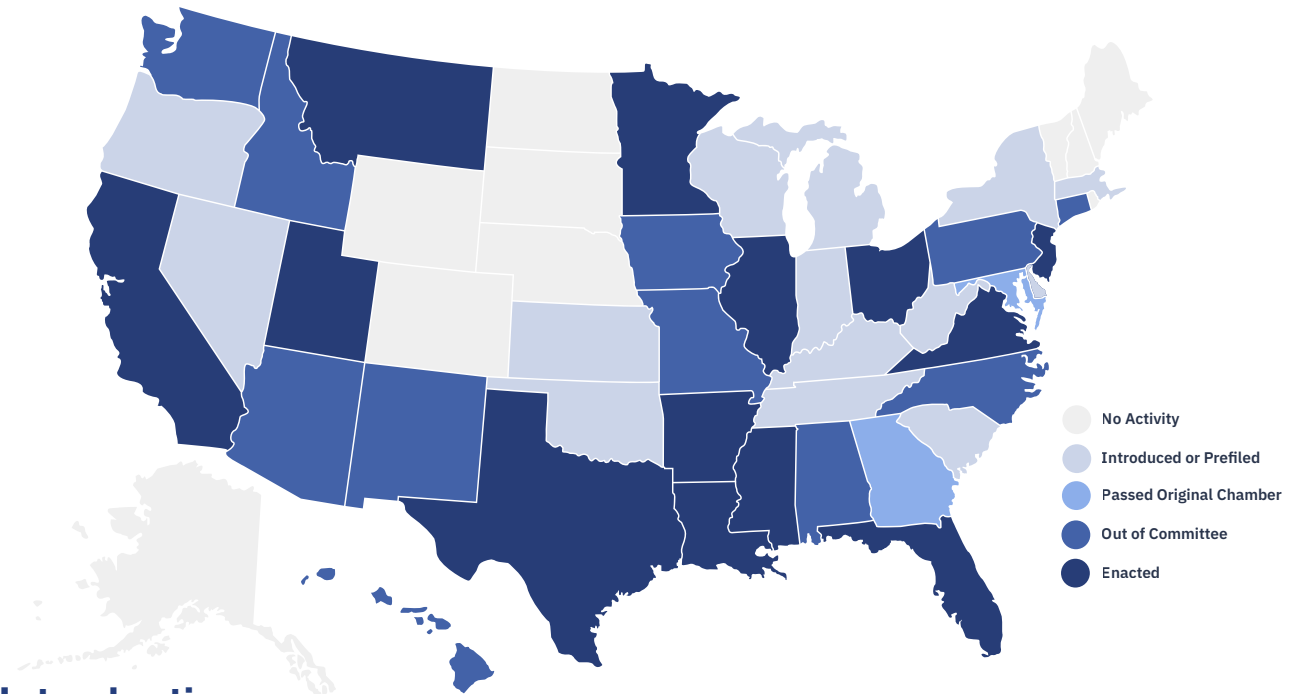
ccianet.org



State Landscape Children's Online Safety



2023 State
Landscapes



Introduction

Addressing the impacts online activities may have on [younger users](#) and preventing harms is an important policy consideration, but the means to achieve that goal are just as important as the goal itself. Many proposals aimed at providing additional online protections for children actually risk introducing [additional privacy concerns](#), or barriers to accessing communities of support and information online.

Last year, California passed the [Age-Appropriate Design Code](#) (AADC), a law modeled from a United Kingdom framework that creates data privacy and constitutional concerns, which is now facing a [legal challenge](#). While that challenge did not deter other states like [Maryland](#), [Minnesota](#), [New Mexico](#), and [New Jersey](#) from introducing their own similar proposals, no other state legislature to date has passed a law akin to California’s AADC.

In other states, like [Arkansas](#) and [Utah](#), lawmakers enacted even more invasive measures, including requirements for mandatory age verification and limiting access hours. These laws present additional challenges and issues surrounding data privacy, open access to information on the internet, and government overreach. Arkansas’ law is also facing a [legal challenge](#), contending that it violates the First Amendment. Additionally, states like [Ohio](#) and [Pennsylvania](#) passed or are considering legislation that requires parental consent either electronically,

via facsimile, or via mail service. These policies not only provide for serious consumer data privacy and compliance concerns but also present operational challenges when it comes to verifying whether a parent or legal guardian is, in fact, a child’s legal parent or legal guardian.

Still, other [bills](#), like those introduced in states like [Alabama](#), [Idaho](#), [Montana](#), and [Tennessee](#), proposed technically impossible default “content filters” for smartphones and tablets. These proposals, branded to prevent children from accessing pornography, would restrict online access and apply child-specific controls on devices often bought by adults. Existing solutions, like [parental device settings and controls](#), already address many of these concerns.

Notably, all of these proposals diverge from the current [Children’s Online Privacy Protection Act \(COPPA\)](#), the federal law protecting users under 13 online. COPPA relies on self-attestation, where users verify their own age when creating accounts. This method requires the user to be forthcoming and honest about their age and does not hold online businesses liable if a user’s age assertion is not accurate. It is unlikely that such self-attestation mechanisms would continue to be acceptable means for determining a user’s age under recently established laws and proposals.

Types of Children’s Online Safety Measures

Age Verification

In 2023, some states passed laws explicitly mandating the use of age verification for online users ranging from ages 16-18. To verify a user’s age, these laws suggest obtaining additional information, such as submitting a driver’s license or credit card or requiring parental consent. Some third-party vendors offer age verification services, though none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals’ data, privacy, and security.

Examples:

- [Arkansas SB 396](#)
- [Utah SB 152](#)
- [Louisiana SB 162](#)

Impact:

Age verification requirements raise serious questions regarding conflicts with data minimization principles and other consumer data privacy protection measures. To effectively conduct age verification, businesses would be required to collect additional data — including collecting and storing their geolocation data to ensure they do not reside outside of the state when confirming that they are of age to be using these services, which would result in additional volumes of data specifically about children. However, the need to collect additional volumes of data would effectively apply to all users by nature of needing to discern between adult and “minor” users. Further, parents or guardians of younger users would likely be required to provide sensitive financial information and personal identifiable information when consenting to and providing age-verification on behalf of younger users.

Age-Appropriate Design Code/Age Estimation

In 2022, California Governor Gavin Newsom (D) signed [AB 2273](#), “the [Age-Appropriate Design Code](#)” (AADC) into law. The AADC is modeled on the United Kingdom’s AADC, and has now been introduced in at least similar form (but not enacted) in several other states. This framework requires “a business that provides an online service, product, or feature likely to be accessed by children” to “estimate the age of child users with a reasonable level of certainty”. Some third-party vendors offer age estimation or similar services that employ facial analysis or other technological means.

Examples:

- [Nevada AB 320](#)
- [Maryland HB 901/SB 844](#)
- [Minnesota HF 2257/SF 2810](#)

Impact:

There are considerable concerns about whether and how third-party age verification vendors or digital services themselves collect or retain personal identifiable information or use other facial recognition tools. It is also worth noting the distinction between the enforceability of California’s AADC vs. the UK AADC. In the UK, it is possible for a business to comply with UK law while not following the UK AADC. In fact, the UK Data Protection Act (DPA) explicitly states that “the [code](#) was designed by the UK Information Commissioner’s Office to meet its obligations under the UK DPA to prepare a code or suggestions for safe practice but explicitly states that a “failure by a person to act in accordance with a provision of a code issued under section 125(4) does not of itself make that person liable to legal proceedings in a court or tribunal.” Additionally, since age estimation does not provide complete accuracy in order for business to comply with the law without being held liable, it is likely that age estimation would amount to age verification.

Child Sexual Abuse Material (CSAM)

Child sexual abuse material (CSAM) generally refers to any visual depiction of sexually explicit conduct involving a minor. Policies have been introduced that would require social media platforms to provide a reporting mechanism for suspected CSAM and require them to remove that material. Although CSAM accounts for a very small portion of internet content, due to the amount of users on these platforms worldwide, it has become overwhelming for online businesses to eradicate every instance of CSAM. However, many of these responsible online businesses are referring instances to the National Center for Missing and Exploited Children (NCMEC) and using technology like hash matching or artificial intelligence to detect and remove CSAM.

Example:

- [California AB 1394](#)

Impact:

Many of these policies do not account for stakeholder abilities. Since the policy is not written within the constraints of what online businesses are capable of, much of the requirements in these bills are not practicably feasible for compliance. Additionally, these policies do not hold those who upload CSAM content liable but rather hold the platforms themselves liable. This approach does not address the root cause of bad actors generating and disseminating such content.

Parental Consent/Access

Such proposals would require a minor user (18 and younger) to receive permission from their legal parent or guardian before they can open an account and make a profile on a social media platform. Ways to verify child-parent relationships and provide consent to platforms have ranged from parents providing their government-issued identification, through a consent form to be signed by the parent and returned via mail, fax or scanning, and having a parent call or video conference a central phone number. Arkansas SB 396 is currently facing a legal challenge due to constitutional concerns.

Examples:

- [Utah SB 152](#)
- [Louisiana SB 162](#)
- [Arkansas SB 396](#)

Impact:

Serious concerns arise from these policies on multiple fronts. First, this type of data collection provides possible bad actors with sensitive information about parents and their children. If online businesses are forced to delete this data, there is no proof of compliance, therefore putting these businesses in a catch-22. Further, it is unclear what impact users' employment of virtual private networks (VPNs) and other mechanisms to evade location-specification age verification requirements could have on organizations' liability. Additionally, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.

Device Filtering

Typically introduced by Republican lawmakers, these bills require manufacturers that sell internet-connected smartphones and tablets to automatically enable a filter that prevents a user from accessing certain online material deemed “harmful to minors.” This is typically referred to as an “obscenity filter.” If the manufacturer fails to comply and a minor accesses material deemed “harmful,” the manufacturer is liable for a whole host of penalties, including civil penalties for each individual device that does not have a filter automatically enabled.

Examples:

- [Montana HB 349](#)
- [Tennessee SB 138/ HB 761](#)
- [Pennsylvania HB 1501](#)

Impact:

Requiring a state-specific default filter would present significant technical difficulties for businesses. Typically, internet service providers (ISPs) govern which websites users can access. It is also unknown how this type of policy would apply to devices that do not have precise location-tracking technology or only connect via Wi-Fi. Similarly, this policy raises questions surrounding how to account for devices purchased online from an out-of-state location, or for devices purchased on the secondary market. Additionally, a mandatory device filter would remove a user’s individual ability to tailor preferences regarding content and services.

Duty of Care to Prevent Harm/“Addiction”

These bills seek to regulate online speech through the use of a design, algorithm, or feature that “knows or reasonably should have known causes a child user harm.” In these cases, “harm” can include designs or features that cause a child user to inflict harm on themselves or others, develop an eating disorder, or experience addiction to the social media platform. Many of these bills also mandate “audits” which require a systematic review or appraisal by a social media platform that describes and analyzes each of the social media platform’s current and forthcoming designs, algorithms, and features that have the potential to cause a violation and their plans to change any of these “designs, algorithms, and features that pose more than a de minimis risk of a violation.”

Examples:

- [California SB 287/ SB 680](#)
- [Utah HB 311](#)
- [Texas HB 18](#)

Impact:

Protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. The lack of narrowly tailored definitions could create an incentive to simply prohibit minors from using digital services rather than face potential legal action and hefty fines for non-compliance. The First Amendment, including the right to access information, is applicable to teens. Speech cannot be suppressed in the name of “protecting” minor users online nor is a state legislative body the arbiter of what information is suitable for younger users to access. Additionally, in the absence of any medical consensus on the topic, private businesses will not be able to coherently or consistently make diagnostic assessments of users. It is also very difficult to reliably describe what may “cause physical, mental, emotional, developmental, or material harms” to a child user. Human beings in general, especially children, have very nuanced opinions surrounding what may be harmful to them. The lived experiences of children, teens, and adults differ immensely, and businesses do not have a roadmap to users’ lived experiences, and what could potentially cause them harm. Furthermore, such measures could adversely undermine businesses’ use of algorithms that help protect users and provide age-appropriate experiences.

Digital Citizenship

Typically a bipartisan policy, digital citizenship bolsters industry efforts to support child safety and privacy online by providing educational curricula focused on how to be a good online citizen. This policy provides a more holistic approach to fostering children's online safety by teaching students how to properly identify standards of appropriate, responsible, and healthy online behavior, including cyberbullying prevention and response. This type of curriculum also teaches social-emotional skills like empathy, kindness, and personal responsibility to enhance online interactions.

Examples:

- [California AB 787](#)
- [Texas HB 99](#)
- [Washington SB 5626](#)

Impact:

Given the complexity of tackling this critical issue, existing industry efforts coupled with educational curricula focused on how to be a good citizen online can have positive impacts. Due to the many positive impacts social media and online services as a whole have had on connecting with loved ones, education, resources, and much more, it is imperative to educate young people on how to appropriately and effectively navigate these spaces to further facilitate positive outcomes from internet use while also giving them the tools to protect themselves if negative occurrences arise. Instead of barring younger users from using the online tools and services that are increasingly critical to the economy and workforce, they can instead learn how to productively and safely engage in the digital world.


Key States

California



In 2023, California introduced seven bills relating to children's online safety ranging from measures involving [CSAM prevention](#) and [algorithmic moderation](#). Given the traction such bills also achieved in 2021 and 2022, California is likely to continue exploring proposals concerning online safety in 2024. Additionally, with the CA Age-Appropriate Design Code currently enjoined due to pending litigation, it is likely that California lawmakers will try to achieve the goal of that bill through other means.

Iowa



Lawmakers in Iowa introduced several bills regulating online businesses this session with most of those efforts relating to children's online safety. Some of these efforts included [requiring a mandatory "obscenity filter" on new mobile devices](#) in the state and even [banning all children from having their own social media account](#) until 18 years of age. Though none of these bills passed this session, it is likely that children's online safety will be top of mind for legislators going into 2024.

Key States

Maryland



Though no children’s online safety bill was passed in Maryland in 2023, the discussions surrounding children’s online safety were prevalent and are likely to continue in 2024. Notably, the Legislature considered [their version of the Age-Appropriate Design Code](#) which passed the House but did not pass the Senate Finance Committee. Since then, deliberations have been underway regarding the enactment of a comprehensive data privacy bill encompassing online safety measures for children, with anticipation that it will be formally introduced in 2024.

Minnesota



Lawmakers debated several approaches seeking to address children’s online safety during the 2023 session. Democrats advanced the [Minnesota Age-Appropriate Design Code](#) while Republicans focused on regulating the [use of algorithms](#) by platforms with child users. Though both approaches have serious First Amendment concerns, it is foreseeable that there is an appetite by Minnesota lawmakers to pass legislation on children’s online safety in 2024.

New Jersey



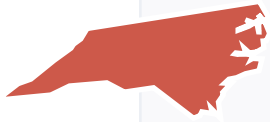
This year New Jersey’s legislature took up several bills pertaining to children’s online safety with a focus on social media platforms. While New Jersey’s legislature will continue to meet through the end of the year, thus far (9/5) the Assembly has passed [A. 5069](#), which attempts to curb the use of “addictive practices or features” by social media companies, and [S. 715](#), which creates a commission to study the use of social media by students, was passed and enacted into law. Additionally, two new pieces of legislation were recently introduced: [A.5750](#), which would require age verification and parental consent for minors’ use of social media, and [A.5744](#), which establishes a public awareness campaign on the dangers of social media use by minors. While further developments may occur in the remaining months of 2023, online safety proposals are likely to be prominent as the legislature kicks off its next biennium in 2024.

New York



The New York legislature once again considered legislation pertaining to children’s online safety, [S. 3281](#), which ultimately failed to move forward during the 2023 legislative session. Notably, Governor Hochul, Attorney General James, along with Senator Gounardes and Assemblymember Rozic [announced](#) two new pieces of legislation aimed to address children’s online safety. Notably, [A. 8148/S. 7694](#) would prohibit users under 18 from being served algorithms on social media platforms. These pieces of legislation figure to be a central topic of discussion during the 2024 legislative session.

Key States



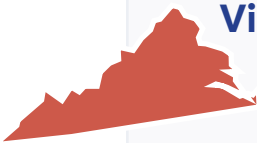
North Carolina

Lawmakers in North Carolina introduced a few different proposals aimed at providing additional online protections for younger users, including through [algorithmic regulation](#) and by requiring a [third-party software provider to manage a child's online interactions, content, and account settings](#). These measures raise many serious privacy and security concerns. While no children's online safety legislation passed in 2023, it is likely lawmakers will revisit this topic when they reconvene in 2024.



Texas

On June 13, 2023, Governor Greg Abbott (R) signed [HB 18](#), the “Securing Children Online through Parental Empowerment (SCOPE) Act”. The law is framed to address “the protection of minors from harmful, deceptive, or unfair trade practices in connection with the use of certain digital services and electronic devices” by establishing that a violation of HB 18 would constitute a violation of the Texas Deceptive Trade Practices Act. Among other provisions, the law establishes several requirements concerning data privacy for “digital service providers” that enter into an agreement with a “known minor”, defined as a child who is younger than 18 years of age. The law also requires a digital service provider to “develop and implement a strategy to prevent” a known minor’s “exposure to harmful material and other content that promotes, glorifies, or facilitates suicide, self-harm, eating disorders, substance abuse, stalking, bullying, harrasment, grooming, trafficking, child pornography, or other sexual exploitation or abuse.” Some of the law’s requirements, including the requirement to verify a user’s age before a digital service provider is allowed to serve a user, raise constitutional concerns under the First Amendment. The SCOPE Act is set to go into effect on September 1, 2024.



Virginia

During the 2023 legislative session, lawmakers considered several proposals intended to amend the Commonwealth’s comprehensive data privacy law and add additional provisions specific to younger users online. [HB 1688](#) and [SB 1026](#) failed to pass the legislature, largely due to opposition from Senate Democrats. The Governor’s office has made it clear that the issue is a priority as well — Gov. Youngkin (R) proposed several [amendments](#) mirroring the language included in HB 1688 and SB 1026 in an unrelated bill, [SB 1515](#), that successfully made its way through the legislature. The amended language was ultimately rejected by the Senate. In September, the Joint Commission on Technology and Science began convening meetings regarding children’s online protections as well. The multitude of venues in which this topic has emerged in Virginia leaves no doubt that conversations will continue during the next legislative cycle. However, the dynamics are likely to shift slightly as Democrats now control both houses of the legislature.

Litigation Likely to Impact State-Level Conversations

Arkansas

Summary:

In June 2023, NetChoice filed suit against the Arkansas Attorney General over a children’s online safety bill, SB 396, arguing that the law violates the First Amendment and other provisions of the Constitution.

Timeline:

- ⌘ **June 29, 2023:** NetChoice filed a [complaint](#) against SB 396.
- ⌘ **July 2023:** NetChoice filed a [motion](#) for a preliminary injunction.
- ⌘ **August 31, 2023:** The court [granted](#) the preliminary injunction on First Amendment and due process grounds, blocking the law from going into effect.
- ⌘ **November 28, 2023:** NetChoice [filed](#) a motion for summary judgment.

California

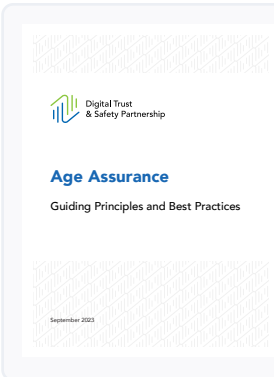
Summary:

In December 2022, NetChoice filed suit against the California Attorney General over a children’s online safety bill, AB 2733, arguing that it violates the First Amendment, Fourth Amendment, Due Process, Commerce Clause, and the Supremacy Clause.

Timeline:

- ⌘ **December 14, 2022:** NetChoice filed a [complaint](#) against AB 2733.
- ⌘ **February 2023:** NetChoice filed a [motion](#) for a preliminary injunction.
- ⌘ **March 2023:** CCIA [filed](#) an amicus brief in support of NetChoice. The brief argues that the bill violates service providers’ First Amendment rights to display and recommend content as well as compels speech in violation of the First Amendment.
- ⌘ **September 18, 2023:** The court [granted](#) the preliminary injunction on First Amendment grounds, blocking the law from going into effect.
- ⌘ **October 18, 2023:** Attorney General Rob Bonta [filed a notice](#) of appeal to overturn the preliminary injunction.

Collected Analysis

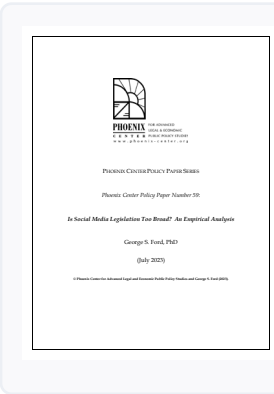


Age Assurance: Guiding Principles and Best Practices

The Digital Trust & Safety Partnership

In September 2023, DTSP released a [report](#) on guiding principles and best practices for age assurance online. DTSP identified overarching age assurance principles and practices that may be deployed as part of the overall [DTSP Best Practices Framework](#).

This report is available at: https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf

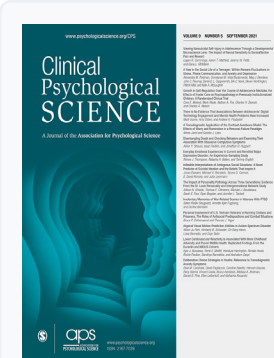


Is Social Media Legislation Too Broad? An Empirical Analysis

Phoenix Center for Advanced Legal and Economic Public Policy Studies

George S. Ford, PhD along with the Phoenix Center published a [report](#) entitled *Is Social Media Legislation Too Broad? An Empirical Analysis*. This policy paper provides a policy-relevant assessment of the relationship between teen screen time use and mental health to guide the reasonable breadth of coverage for legislation.

This report is available at: <https://subscriber.politicopro.com/f/?id=00000189-3376-d8dd-a1ed-7b779c920000>



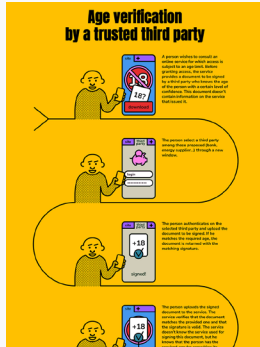
There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased

SAGE Journals

UK Researchers Matti Vuorre, Amy Orben, and Andrew K. Przybylski published an [empirical article](#) entitled *There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased*. They examined changes in associations between technology engagement and mental health focused on three large nationally representative data sets from the United States and the United Kingdom. The surveys included a variety of health and well-being measures ranging from subjective well-being, such as loneliness and self-esteem, to constructs that are typically thought to indicate more objective mental health problems, such as depression and suicidality. Particularly, depression's relation to both TV and social media was practically zero. The results showed that technology engagement had become less strongly associated with depression in the past decade. They concluded that there is little evidence for increases in the associations between adolescents' technology engagement and mental health.

This report is available at: <https://journals.sagepub.com/doi/epdf/10.1177/2167702621994549>

Collected Analysis

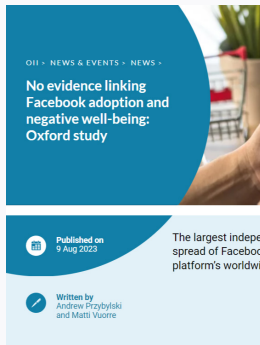


Online age verification: balancing privacy and the protection of minors

Commission Nationale de l'Informatique et des Libertés (CNIL)

CNIL analyzed the main types of age verification systems in order to clarify its position on age verification on the internet. The [research](#) found that the current age verification systems out there are circumventable and intrusive. Due to these findings, CNIL calls for the implementation of more privacy-friendly models.

This report is available at: <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>



No evidence linking Facebook adoption and negative well-being: Oxford study

Oxford Internet Institute

The Oxford Internet Institute conducted the [largest independent scientific study ever conducted](#), investigating the spread of Facebook across the globe. The independent Oxford study used well-being data from nearly a million people across 72 countries over 12 years and harnessed actual individual usage data from millions of Facebook users worldwide to investigate the impact of Facebook on well-being. They found that there was no evidence that the social media platform's worldwide penetration is linked to widespread psychological harm.

This report is available at: <https://www.oii.ox.ac.uk/news-events/no-evidence-linking-facebook-adoption-and-negative-well-being-oxford-study/>