



**September 26, 2024**

Office of the New York State Attorney General, The Honorable Letitia James  
New York State Capitol  
State Street and Washington Avenue  
Albany, NY 12224-0341

Submitted electronically at [ProtectNYKidsOnline@ag.ny.gov](mailto:ProtectNYKidsOnline@ag.ny.gov)

**RE: Office of the New York Attorney General’s Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 1500 et seq., the SAFE for Kids Act**

Dear Attorney General James:

On behalf of the Computer & Communication Industry Association (“CCIA”), I write in response to the Office of the New York State Attorney General’s (“the Office’s”) Advanced Notice of Proposed Rulemaking (“ANPRM”) pursuant to New York General Business Law section 1500 et seq., the SAFE for Kids Act (hereafter referred to as “the Act”).

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.<sup>1</sup> CCIA holds a firm conviction that children are entitled to a higher level of security and privacy in their online experiences. Our members are actively engaged in various initiatives to integrate robust protective design features into their websites and platforms.<sup>2</sup> CCIA’s members have been leading the effort to implement settings and parental tools to individually tailor younger users’ online use to the content and services that are suited to their unique lived experience and developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools to allow parents to block specific sites entirely.<sup>3</sup>

Responsible digital service providers also already take aggressive steps to moderate dangerous and illegal content, consistent with their terms of service and existing law. The companies deliver on the commitments made to their user communities with a mix of automated tools and human review. Doing so is an evolving industry practice; for example, since launching in 2021, the Digital Trust & Safety Partnership (DTSP) has quickly developed

---

<sup>1</sup> For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at <https://www.ccianet.org/members>.

<sup>2</sup> Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children’s Safety Online*, Disruptive Competition Project (Feb. 7, 2023), <https://www.project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/>.

<sup>3</sup> Competitive Enterprise Institute, *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/>.



and executed initial assessments of how participating companies implement the DTSP Best Practices Framework,<sup>4</sup> which provides a roadmap to increase trust and safety online.

CCIA and its members commend the Office for its efforts to implement the requirements under the Act swiftly and transparently. CCIA's enclosed responses are intended to reflect and focus on the Association's specific areas of expertise and do not represent an exhaustive response to each of the questions proposed by the Office.

We appreciate the opportunity to provide input as the rulemaking process is in its early stages and look forward to additional opportunities to engage with the Office.

## 1. “Commercially reasonable and technically feasible age determination methods”

As the Office considers regulations concerning age determination methods, CCIA stresses that every approach to age determination presents trade-offs, especially between accuracy and privacy, as is correctly noted in the ANPRM. There is also no one-size-fits-all approach as the nature of the content and risks varies widely across online services. Therefore, different services opt for different approaches based on a variety of factors, including but not limited to the users of the service, the type of service offered, risk calculation, privacy expectations, and economic feasibility.<sup>5</sup> There are also significant differences and dynamics tied to various levels of conducting age assurance, including attestation, estimation, and verification.<sup>6</sup> For many of the questions in the ANPRM, CCIA suggests referring to a recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, for more information regarding guiding principles for age assurance in addition to more information about how companies have used such principles to develop example best practices for age assurance.<sup>7</sup>

### **Consistency with federal law and the U.S. Constitution**

The Children's Online Privacy Protection Act (COPPA) and associated rules at the federal level currently regulate how to address users under 13, a bright-line that was a result of a lengthy negotiation process that accounted for the rights of all users, including children, while also considering the compliance burden on businesses. To avoid collecting data from users under 13, some businesses chose to shut down various services when COPPA went into effect due to regulatory complexity — it became easier to simply not serve internet users under the age of 13..

<sup>4</sup> Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), <https://www.axios.com/2021/02/18/tech-giants-list-principles-for-handling-harmful-content>.

<sup>5</sup> *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), [https://dtspartnership.org/wp-content/uploads/2023/09/DTSP\\_Age-Assurance-Best-Practices.pdf](https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf).

<sup>6</sup> Khara Boender, *Children and Social Media: Differences and Dynamics Surrounding Age Attestation, Estimation, and Verification*, Disruptive Competition Project (May 10, 2023), <https://www.project-disco.org/privacy/children-and-social-media-differences-and-dynamics-surrounding-age-attestation-estimation-and-verification>.

<sup>7</sup> *Age Assurance: Guiding Principles and Best Practices*, supra note 5.



Any age determination requirement associated with an online website or service collecting additional information could deter users from accessing constitutionally protected speech. When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.<sup>8</sup> After 25 years, age authentication still remains a vexing technical and social challenge.<sup>9</sup> California, Arkansas, Ohio, Mississippi, and Utah recently passed legislation requiring parental consent, along with age verification and estimation measures. Judges have recently paused the enforcement of these laws pending a full review of the legal challenges.<sup>10</sup> CCIA anticipates that forthcoming rulings from the judiciary may be instructive in determining how, or whether, age determination requirements can be tied to granting user access to online speech.

### **Concerns associated with user privacy and data needed to determine user age**

Any commercially available age verification method carries serious privacy and security concerns for users. Notably, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification technologies 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.<sup>11</sup>

When businesses are required to determine a user's age, they are effectively required to collect additional information. This is itself likely to conflict with data minimization principles inherent in typical federal and international privacy and data protection compliance practices. Requiring such data to be collected may also be inconsistent with consumer expectations. For example, a recent study from the Pew Research Center found that many Americans worry about children's online privacy but when asked about who is responsible for protecting children's online privacy, most (85%) say parents hold a great deal of responsibility for protecting kids' online privacy. Additionally, 59% also say that tech companies bear the responsibility while 46% believe the government does. The study also highlights why it is important to consider the trade-offs associated with age determination and consent proposals that would require the additional collection of data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.<sup>12</sup>

### **Accuracy of age determination methods**

The ANPRM notes that the Office is considering a framework that would provide users with a variety of options from which to select in order to conduct age determination. These options

<sup>8</sup> *Reno v. ACLU*, 521 U.S. 844 (1997).

<sup>9</sup> Jackie Snow, *Why age verification is so difficult for websites*, The Wall Street Journal (Feb. 27, 2022), <https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728>.

<sup>10</sup> *NetChoice, LLC v. Bonta* (N.D. Cal. 22-cv-08861); *NetChoice, LLC v. Griffin* (W.D. Ark. 23-cv-05105); *NetChoice, LLC v. Yost* (S.D. Ohio 24-cv-00047); *NetChoice, LLC v. Fitch* (S.D. Miss. 24-cv-00170); *NetChoice, LLC v. Reyes* (D. Utah 23-cv-00911).

<sup>11</sup> *Online age verification: balancing privacy and the protection of minors*, CNIL (Sept. 22, 2022), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

<sup>12</sup> Colleen McClain, *How americans view data privacy*, Pew Research Center: Internet, Science & Tech (Oct. 18, 2023), <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.



include: biometric assessment; assessment based on analyzing user activity; requiring users to submit government-issued identification; attestation from a reliable third-party business with pre-existing information, such as a bank or credit card; attestation from other users; self-attestation; and cognitive tests. As previously noted, each of these options carry trade-offs, especially concerning accuracy.

For example, the National Institute of Standards and Technology (“NIST”) recently published a report examining the performance of six software-based age estimation and age verification tools that estimate a person’s age based on the physical characteristics evident in a photo of their face. The report notes that facial age estimation accuracy has improved since NIST first measured it in 2014. However, recent research has shown that accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors. This research indicates that the lowest false positive rates (“FPRs”) are observed among Eastern Europeans, though these rates vary for women and men of different ages, with FPRs generally being higher in women compared to men.<sup>13</sup> While the authors of the report note that improvements to such technologies are anticipated to rapidly evolve and that NIST intends to update and expand their test methods, CCIA encourages the Office to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

### ***Third-party age determination services and self-attestation***

Currently social media platforms rely upon self-attestation as the mechanism for determining user age. The use of any third-party age determination services by a social media platform would necessitate the sharing of a tremendous amount of personal sensitive data of users of such a platform. There does not currently exist a trusted, proven third-party entity that can conduct age determination in a reliable manner that avoids bias, discrimination, while also protecting users’ sensitive identifying information.<sup>14</sup> Therefore, any such requirement for users to undergo an age determination exercise with a third-party entity should include clear notice language that outlines the processes in which their sensitive data will be used as well as outlines the demonstrated data privacy risks associated with conducting age-determination.

### ***Variation among social media platforms’ commercial and technical capabilities***

The ANPRM correctly acknowledges that there is significant variation among social media platforms’ commercial and technical capabilities. These differences are also inherent given the variation in the nature and audience for a particular service. Therefore any implementing regulations under the Act should consider the potential impact to online operators of all sizes acknowledging that resources are not equal across companies. Requiring a significant increase in the collection, processing, and storage of sensitive data of all users would result in a

---

<sup>13</sup> Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525)*, National Institute of Standards and Technology (May 30, 2024), <https://doi.org/10.6028/NIST.IR.8525>.

<sup>14</sup> Sarah Forland, Nat Meysenburg, Erika Solis, *Age Verification: The Complicated Effort to Protect Youth Online.*, New America Open Technology Institute (Apr. 23, 2024), <https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/challenges-with-age-verification>.

tremendous increase in costs for operators, particularly when considering the security protocols that would need to be deployed to secure such sensitive information. These increased costs would have an outsized impact on smaller operators, many of whom may not be able to withstand an increase in operating costs and be unable to comply with the law.<sup>15</sup>

### ***Impacts to classes of users***

Several communities that call New York home may be uncomfortable or unable to provide any additional information, particularly sensitive information, to social media platforms or third-parties. Undocumented populations, which may use social media to connect with family in their home nations, may not have government-issued ID or the ability to access banking. When parental consent is required, LGBTQ+ individuals from unsupportive households may be denied access to online platforms that offer safe spaces, as their parents might withhold consent and prevent them from finding the support they need.

It would be virtually impossible to fully mitigate concerns and prevent potential data breaches including sensitive personal information used for age determination. As we've seen around the world, data breaches happen often and in the case of Australia, where the government started a pilot program to conduct online age verification for club-goers in the country. Soon after that program was started, a data breach occurred and over 1 million customers had their sensitive information stolen based on the data collected from their drivers licenses<sup>16</sup>.

### ***Potential trade-offs between user security and documenting compliance with the Act***

The Act would hold covered businesses liable for failing to perform age verification. Therefore any regulations that would mandate the deletion of data related to age verification would leave businesses without a means to document their compliance. This becomes especially problematic in instances where a user decides to use deceptive verification information such as using an identification card that is not their own.

### ***Data security considerations to ensure the security of data used in age determination***

A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*,<sup>17</sup> details several principles that should be considered to best secure data used in any age determination process. Among others detailed in the report, these include: minimizing the collection of personal data for age assurance, in a manner proportionate to the assessed risk, and design-tailored practices regarding the retention, deletion, and use of data; using sensitive data collected for age assurance solely for that purpose; using age estimation methods reliant on data that is already collected as a function of the service, rather than requiring the collection of new personal data; requiring third-party vendors to apply high

---

<sup>15</sup> *More than just a number: How determining user age impacts startups*, Engine (Feb. 2024), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d8b6ab876bfd5b70f8795e/1708701355604/FINAL+-+2024+More+Than+Just+A+Number.pdf>.

<sup>16</sup> Jessica Kidd, Isobel Roe, Jesse Hyland. *Cybercrime detectives arrest man following alleged data breach involving more than 1 million NSW clubs customer records* <https://www.abc.net.au/news/2024-05-02/clubs-nsw-cybersecurity-potential-data-breach-venues/103793584>

<sup>17</sup> *Age Assurance: Guiding Principles and Best Practices*, supra note 5.



privacy and security standards; and providing transparency to users about how their data is collected, used, and retained.

The ANPRM considers several data privacy and security concerns, including how to best protect against first- and third-party mismanagement, how to ensure that data collected for one purpose is not used for another purpose, potential data minimization regimes, and how to ensure that covered entities delete user information. Many other states have considered such issues and adopted comprehensive consumer data privacy frameworks to establish baseline protections for all users — these laws could serve as a good baseline for the Office to consider.

CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to exercise their rights. In the absence of a comprehensive law at the federal level, a growing number of states have enacted their own laws. The majority of these laws harmonize a key set of definitions and concepts related to privacy.<sup>18</sup> CCIA would encourage the Office to align and harmonize any new regulations concerning consumer data privacy rights and associated business compliance obligations with existing frameworks to allow for interoperability.

## 2. “Parental consent”

Generally, consent refers to a clear affirmative act that represents a consumer’s freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including through electronic means, or any other unambiguous affirmative action such as a verbal statement if using a home smart device.

The particular method a business chooses to implement to obtain consent from a consumer, including a parent or guardian, will depend upon a variety of considerations: security and privacy, accessibility and equity, and other risks such as user hesitancy to provide certain personal information. However, in some circumstances, there is no explanation of how a company can verify the relationship between a young user and the consenting adult, especially if the consenting parent or guardian does not have an account.

### **Parental notice requirements**

As detailed more extensively later in CCIA’s comments (Section 3 regarding “Addictive Social Media Platform”) several studies examining have resulted in mixed conclusions about whether there is a causal link between social media and negative impacts to youth mental health.

---

<sup>18</sup> Computer & Communications Industry Association, *Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices* (January 2022), <https://www.ccianet.org/wp-content/uploads/2022/02/CCIA-State-Privacy-Principles.pdf>



Therefore, CCIA advises against issuing regulations that would require businesses to disclose potential harms associated with algorithmic feeds until there is a consensus among experts in the field.

CCIA also stresses that the perceived harms associated with social media should not be treated as an equivalent comparison to other products like cigarettes, alcohol, and gambling. Therefore, CCIA advises against promulgating regulations that would impose similar requirements to communicate harms and limit promotion to children. Such other products all have long-standing documented negative impacts to the physical and psychological health of humans. Additionally, each of the other products mentioned have a federal age limitation that prohibit the sale of such products to anyone under the age of 21. Given that no such similarities exist for social media, it should not be treated in the same way.

### ***Parental consent methods consistent with federal law***

Websites and online services employ a variety of methods to determine whether an individual is the parent or guardian of a given user consistent with compliance requirements established under COPPA. These methods might include uploading a government-issued photo identification card; using a credit, debit, or other online payment method; or verification via video conferencing to confirm identity. CCIA encourages the Office to craft regulations that align with the methods that are currently used in the parental verification process for compliance with COPPA. The costs associated with different verification methods vary depending on the type of service and the necessary mechanisms required to successfully implement them. However, given that many businesses already have mechanisms in place to comply under COPPA, this would present the most frictionless framework for businesses to comply with under the Act. Should the Office want to ensure that parents are able to give, reject, or withdraw consent without having to create a social media account, several of these methods could be achieved without them having to create their own account.

### ***Other factors or considerations related to obtaining parental consent***

CCIA encourages the Office to consider how covered businesses under the Act would operationalize parental consent requirements and associated equity concerns. There are significant challenges associated with verifying whether a “parent or guardian” is a specific minor’s legal parent or guardian. Many parents and legal guardians do not share the same last name as their children due to remarriage, adoption, or other cultural or family-oriented decisions. If there is no authentication that a “parent or guardian” is that specific minor’s legal parent or guardian, this may incentivize minors to ask other adults who are not their legal parent or guardian for consent. It is also unclear who would be able to give consent to a minor in foster care or other nuanced familial situations, creating significant equity concerns. Further, scenarios where a legal parent or guardian is not located in New York or is not a resident of the state create significant confusion for consumers and businesses.

Additionally, some individuals may lack access to essential resources for conducting these methods, such as government identification or banking services. Furthermore, there are also

populations that have knowledge limitations when it comes to navigating online spaces and therefore could be incapable of navigating through any such verification process. Any such requirements in place should avoid unduly burdening parents, as parents too can become susceptible to consent fatigue, which may end up hindering the ability of younger individuals to access the internet.

### 3. “Addictive Social Media Platform”

#### ***Algorithmic feeds should not be presumed as inherently harmful or “addictive”***

CCIA has significant concerns that the Act presumes that algorithmic feeds are inherently harmful or “addictive”, given the lack of conclusive evidence to support such a conclusion. Like any product, there are risks and benefits inherent to algorithmic feeds. However, CCIA cautions against pursuing measures that inherently presume only negative impacts or that associates user engagement with such feeds as necessarily “addictive”.

For example, algorithmic feeds serve content with increased relevance to individual users, prioritizing content that is more likely to be appropriate and of interest. By analyzing past interactions, browsing history, and other factors, algorithms contribute to curating a relevant and personalized experience. While algorithms personalize a user’s experience, they can also help to introduce new topics and interests allowing users to discover creators, ideas, and communities they would not have found otherwise. And algorithms are able to do this efficiently — with vast amounts of content available, algorithms help users navigate information overload through prioritizing content and allowing users to find what they’re looking for faster and with less effort.

Algorithms can also be used to encourage more positive experience online, including through the use of tools to identify and report inappropriate content such as CSAM or guiding users to helpful resources if they search for material related to self-harm, suicide, or depression.

On a daily basis, humans engage in a variety of compulsive and repetitive behaviors — some of these can have decidedly negative impacts on physical and/or mental health. For example, compulsive behaviors could range from binge eating unhealthy foods to exercising in excess to watching favorite shows for hours on end. It is important to consider whether certain compulsive behaviors amount to an “addiction”. The Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-V) does not include a definition for “algorithmic addiction” or “internet addiction” as it attempts to lay out the distinction between “substance use disorders” and the term “behavioral addictions”. “Behavioral addictions” is used to refer to behaviors such as “shopping addictions”. Such behaviors were excluded from the DSM-V due to the lack of peer-reviewed evidence to establish diagnostic criteria used to classify the behaviors as mental disorders.<sup>19</sup>

There is also a lack of conclusive evidence regarding the relationship between social media use and youth mental health. When the U.S. Surgeon General released an Advisory entitled Social

---

<sup>19</sup> See *Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition*, American Psychiatric Association, at 481.





Media and Youth Mental Health<sup>20</sup>, many were quick to highlight only the harms and risks that it charged. However, the report is much more nuanced and also discusses many potential benefits of social media use among children and adolescents. For example, the report concludes that social media provides young people with communities and connections with others who share identities, abilities, and interests. It can also provide access to important information and create a space for self-expression. The Surgeon General's report further details that the buffering effects against stress that online social support from peers provides can be especially important for youth who are often marginalized, including racial, ethnic, sexual, and gender minorities.<sup>21</sup> An online central meeting place where kids can share their experiences and find support can have positive impacts. It should also be highlighted that the report provides evidence that social media-based and other digitally-based mental health interventions may also be helpful for some children and adolescents by promoting help-seeking behaviors and serving as a gateway to initiating mental health care.

A study published by the National Academy of Sciences, *Social Media and Mental Health*, noted that a literature review "did not support the conclusion that social media causes changes in adolescent health at the population level". The report went on to describe additional nuances related to how certain individuals, such as those with "clinically meaningful depression" may engage with social media in different ways than those who do not. The report went on to highlight "...the relationship between social media use and depression might vary among different demographic or identity groups. Among LGBTQ+ teens, for example, social media use is associated with fewer depressive symptoms but an increased risk of bullying."<sup>22</sup> The report goes on to describe approaches, including establishing comprehensive digital media literacy standards in education curriculum, to address the potential harms that certain individuals may experience while acknowledging the complex nature.

Further, the U.S. Surgeon General's report notes the lack of evidence to support a causative relationship between social media and anticipated negative impacts on younger users. For example, the research openly acknowledges that "...social media use may be a risk factor for mental health problems in adolescents. However, few longitudinal studies have investigated this association, and none have quantified the proportion of mental health problems among adolescents attributable to social media use."<sup>23</sup> It is also reasonable to examine that compared to previous decades, young people face increased financial pressure, greater competition, more complex tertiary education pathways, and increased loneliness specifically due to the COVID-19 pandemic. Factors such as increased mental health resources and the general

---

<sup>20</sup> U.S. Surgeon General, *Social Media and youth mental health*, U.S. Department of Health and Human Services (May 23, 2023), <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>.

<sup>21</sup> Jennifer Marino, Matthew Berger, Megan Lim, Melody Taba, Rachel Skinner, *Social Media use and health and well-being of lesbian, gay, bisexual, transgender, and Queer Youth: Systematic Review*, *Journal of Medical Internet Research* (Sept. 22, 2021), <https://www.jmir.org/2022/9/e38449>.

<sup>22</sup> *Social Media and Mental Health*, National Academy of Sciences (2023), <https://nap.nationalacademies.org/catalog/27396/social-media-and-adolescent-health>.

<sup>23</sup> Kayla Tormohlen, Kenneth Feder, Kira Riehm, *Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth*, *JAMA Psychiatry* (Sept. 11, 2019), <https://jamanetwork.com/journals/jamapsychiatry/fullarticle/2749480>.



acceptance of having and reporting mental health conditions also play a role. In order to take a measured approach to these complicated and sensitive issues, it is imperative to remember that correlation does not equal causation.

Still other studies point to the nuances of mental health impacts and use of certain online products. This research shows that social media effects are nuanced,<sup>24</sup> individualized, reciprocal over time, and gender-specific. Another study conducted by researchers from Columbia University, the University of Rochester, the University of Oxford, and the University of Cambridge found that there is no evidence that associations between adolescents’ digital technology engagement and mental health problems have increased.<sup>25</sup> Particularly, the study shows that depression has virtually no causal relation to TV or social media. And, one of the researchers, Professor Andrew Przybylski of the Oxford Internet Institute, stated in a press release, “We looked very hard for a ‘smoking gun’ linking technology and well-being and we didn’t find it.”<sup>26</sup>

\* \* \* \* \*

We appreciate the consideration of these comments and stand ready to provide additional information regarding technology policy. Should you have any questions, please do not hesitate to reach out to me at [aspyropoulos@ccianet.org](mailto:aspyropoulos@ccianet.org).

Sincerely,

Alexander Spyropoulos  
Regional Policy Manager, Northeast  
Computer & Communications Industry Association

<sup>24</sup> Amy Orben et al., *Social Media’s enduring effect on adolescent life satisfaction*, PNAS (May 6, 2019), <https://www.pnas.org/doi/10.1073/pnas.1902058116>.

<sup>25</sup> Amy Orben, Andrew K. Przybylski, Matti Vuorre, *There Is No Evidence That Associations Between Adolescents’ Digital Technology Engagement and Mental Health Problems Have Increased*, Sage Journals (May 3, 2021), <https://journals.sagepub.com/doi/10.1177/2167702621994549>.

<sup>26</sup> Regina Park, *The Internet Isn’t Harmful to Your Mental Health, Oxford Study Finds*, Disruptive Competition Project (Jan. 29, 2024), <https://www.project-disco.org/innovation/the-internet-isnt-harmful-to-your-mental-health-oxford-study-finds/>.