SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

MEMORANDUM

Date: 4/20/2023
To: File
From: Albert Fox Cahn, Esq.; Evan Enzer, Esq.

Re: The Unintended Harms of S3281 ("The NY Surveillance Act") To Internet Safety

Few goals are as noble and vital as protecting children, especially as we look at the broad cross-section of threats that technology can fuel for younger users. But, alarmingly, many laws aiming to protect teenagers and younger children only worsen the problem, creating an even more potent threat to their privacy, autonomy, and safety. This proposed New York Surveillance Act (S3281) threatens to do just that. Instead of protecting minors, it would require collecting intimate, chilling, and potentially dangerous information about how children navigate the internet.

Age/Identity Verification Is A Major Privacy Invasion

The New York Surveillance Act includes the same critical flaw made by so many prior iterations of internet legislation: **it ignores how hard it is to verify ages online**. At a high level, the New York Surveillance Act 's restrictions on how surveillance corporations can take, store, and sell teenagers' data might seem like a win for privacy advocates. But as a whole, this bill creates a no-win situation for privacy advocates, minors, and internet services.

The law would impose stringent penalties any time an internet company "**should** know that its product is accessible to and used by children."[1] This standard is so broad that it applies to internet services that regulators merely believe *should* have known that a child was using their site, even if the site never actually does. A company could find itself facing ruinous penalties and the threat of bankruptcy if a single child logs on, even if the company never targeted children and actively took measures to prevent the minor's access.

Since penalties under the law can reach $250 million,[2] companies will take drastic steps in response, but not the steps lawmakers intend. Experience shows that simply asking users to enter their age, provide a credit card, or use other traditional forms of age verification isn't effective. Teenagers routinely circumvent such measures to access adult content and to log onto sites before they reach the required age. This is also particularly frequent with users under 13, who routinely lie about their age to circumvent the Children's Online Privacy Protection Act (COPPA) and play online games.

These past age verification failures will lead companies to mandate government identification and/or invasive biometric scans simply to register an account. This is

[1] S. 3281, N.Y. State Senate, 2023-2024 Reg. Sess. (N.Y. 2023). To be codified at N.Y. Gen. Bus. Law § 899 CC (1)(M).
[2] S. 3281. To be codified at N.Y. Gen. Bus. Law § 899 CC (11)(a).

tantamount to requiring every internet user to register their legal name and personal information with every website and internet service they use. Such a requirement would effectively break many of the privacy-protective options that tech companies recently developed, including features that allow users to install apps with anonymous email addresses to avoid unwanted ads. In practice, features that help New Yorkers protect their personal information would become illegal, ironically making their data more vulnerable in the name of protecting privacy.

Detrimental Impacts on New York's Marginalized Communities

Age and identity verification requirements will also hurt New York's undocumented communities, cutting them off from valuable resources locally, loved ones abroad and remote work at home. Immigration and Customs Enforcement (ICE) routinely weaponizes commercial databases and internet service providers' records to track and deport undocumented families. In recent years, ICE has purchased information about millions of families' utility records while using tens of thousands of subpoenas to grab information from nearly every digital platform. Given the magnitude and persistence of ICE's surveillance, undocumented New Yorkers are increasingly wary of using any digital platform traceable to their legal name and immigration status. But if the New York Surveillance Act were to pass, anonymous internet access would be a thing of the past, and immigrant communities would find themselves trapped in an analog exile.

The New York Surveillance Act wouldn't just harm adult internet users, it would harm children and teens as well. First, the law's broad provisions go beyond leading social media firms to reach most of the internet, potentially impacting access to news and cultural content. And the law's simplistic age cutoff means that all New Yorkers under 18, even those in college, in foster care, or legally emancipated, would lose the right to unfettered online access.

This sort of one-size-fits-all parental access will put countless kids in harm's way. Section 7(B) would require teenagers to obtain parental consent before accessing an internet service. **For LGBTQ+ youth, these mandatory "parental consent" could be** life threatening . LGBTQ+ youth face a heightened risk of violence at home. For those with homophobic or transphobic parents, coming out can mean harassment, the loss of housing, physical assault, and more. For decades, the internet has given LGBTQ+ teens a lifeline, allowing them to connect with peers remotely even when physically isolated at home. But if teens are required to register their internet usage with parents, those lifelines will become a potential threat, posing a risk of outing users to the same parents they may be hiding from.

Overbroad and Potentially Unconstitutional

Beyond threatening New Yorkers' privacy and safety, the New York Surveillance Act would likely face certain defeat in the courts. The law's ambiguous scope, ruinous penalties, and broad grant of discretion to administrative agencies are likely unconstitutional. Broad bans on advertising products "intended primarily for educational purposes" could apply to everything from community blogs to newspapers like the New York Times.[3] Without clarity, these provisions specifically, and the

[3] S. 3281. To be codified at N.Y. Gen. Bus. Law § 899 CC (3)(C). The New York Surveillance Act's ban on collecting, buying and selling child data, but that would include many advertising practices. So this is a strong way to phrase things but I wouldn't say it is technically incorrect

law, would likely violate the First Amendment's overbreadth doctrine, which requires any restrictions on speech to be "narrowly tailored" to only restrict non-protected speech.

Section 4(c) would also likely face Constitutional challenges. The provision allows the Attorney General's Office to ban any aspect of an internet platform "it deems to be designed to inappropriately amplify the level of engagement a child user has with such product." This provision would enable the Attorney General's Office to unilaterally redesign any aspect of the internet it wants, transforming a state attorney general into the Editor-in-Chief of the World Wide Web. **Such a provision would allow the attorney general unfettered discretion to target any speech they disagree with, even if political or religious in nature**. Such a broad grant of power is not only contrary to the New York State and Federal Constitutions, it's antithetical to democracy itself.