THE KIDS WON'T BE ALRIGHT

THE LOOMING THREAT OF CHILD SURVEILLANCE LAWS

ALBERT FOX CAHN
ANNIE DEVOE
CYRA PALADINI
EVAN ENZER
LULA KONNER
SAMVIT GANESH

SEPTEMBER 28, 2023

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

I. Introduction

Across the country, an array of new state and federal surveillance bills pose an unprecedented and existential threat to privacy, safety, and the promise of an open internet. This legislative wolf dressed in sheep's clothing is framed around a noble goal: protecting children. Sadly, these laws are just the latest example of misguided tech policies built on a fundamental misunderstanding of the thing lawmakers seek to regulate—harming the very communities officials seek to protect.

The key flaw of these state surveillance bills is that they create a two-tiered internet, one for children, and one for adults. This is an intuitive step, but one that simply cannot be implemented in practice, as there is no effective, let alone privacy-preserving way, to determine users' identities. These laws mandate or coerce the use of new, invasive measures that verify users' legal name, age, and address for nearly every internet service they use. Suddenly, every online purchase and search engine query will come with state-mandated tracking, and anonymity will be a thing of the past. This change would be invasive and insecure for every user, but it would pose a particularly potent threat to undocumented communities, LGBTQ+ communities, and those seeking reproductive care. The data would be a ticking time bomb, a powerful new surveillance source for police, prosecutors, Immigration and Customs Enforcement (ICE), and private anti-choice groups.

In a sad, ironic twist, state surveillance bills pose the gravest danger to children. The bills view parental surveillance of young adults' online activity as a safeguard, but the legislation ignores the painful truth that for countless kids, parents pose a threat. For LGBTQ+ young people living with abusive, homophobic, or transphobic parents, these laws could lead to violence or homelessness. And for those teens who self-censor their online activity to protect their privacy, it could mean losing access to life-saving support and resources. For so many LGBTQ+ youth, online anonymity is the only thing that lets them access spaces where they can be themselves, and new parental consent requirements could further isolate children in unsafe households.

Introduced in early 2023, S3281 (or what advocates have called "the New York Surveillance Act") makes many of the same missteps as other surveillance laws around the country. 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 did. 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. The effect of this broad standard with high penalties, reaching in some cases up to 250 million dollars,[2] is that all internet services will take drastic, invasive measures to prevent young adults from accessing their sites and/or to identify those who do.

Companies will respond almost identically to the ways they have in states that passed similar laws, requiring government ID, biometric scans, and other invasive and biased tools to screen users. These corporate policies will likely extend far beyond the Empire State. Liability is so steep that

[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).

companies will be incentivized to extend surveillance globally. Because location verification is easy to circumvent, if companies were to only implement security measures within New York state lines, they could find themselves up against hefty fines for young adults who use virtual private networks (VPNs) and other tools to impersonate users from another state.

II. Reviewing the legislative state of play

U.S. child privacy legislation primarily centers on the Children's Online Privacy Protection Act (COPPA). Passed in 1998, COPPA was meant to curb the ways online services could collect and monetize children's data. COPPA broadly limits most forms of data collection when children under 13 use online services, entertainment, and websites, with exceptions for education technology and other specified uses. Companies face limits on how they can use a child's name, address, email address, phone number, social security number, geolocation information, photos, videos, and other identifying details. COPPA also requires parental consent for companies to access or store children's information. While COPPA does not specify how firms can verify children and parents' identities, the FTC, alarmingly, endorsed the use of facial recognition technology in conjunction with photo ID as one mechanism.[3]

Another major component of COPPA is age verification to limit data collection on minors. The FTC mandates that websites and online services must take steps to make sure they do not collect personal information from children under 13 without parental consent. The means by which verification occurs most commonly is expanded on in multiple sections below, though it often includes the user's self-attestation or other methods to verify their age. This verification process poses one of the most pressing threats to user privacy online.

a. California

In September, 2022, California enacted the first specific and comprehensive child privacy code going beyond COPPA's minimums. The California Age Appropriate Design Code, also known as the "Design Act," or "the Code," requires operators of online services, features, or products to actively emphasize children's best interests during the production's design stage, according to the Design Act. Notably, the legislation does not treat all children as identical, instead requiring companies to evaluate the unique needs of five different age cohorts: 0-5 years; 6-9 years; 10-12 years; 13-15 years; and 16 to 17 years.

Notably, the Design Act is limited to large internet services and California-focused data brokers, only covering firms with: (1) $25 million or more in revenues; (2) personal information of 100,000 or more California residents; or (3) mainly generating revenue through Californians' data.[4] The

[3] FTC, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, accessed September 6, 2023, https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business

[4] "Four Key Considerations for Implementing the California Age-Appropriate Design Code," Perkins Coie, accessed September 6, 2023, https://www.perkinscoie.com/en/news-insights/four-key-considerations-for-implementing-the-california-age-appropriate-design-code.html.

legislation also is limited to firms whose content is "likely to be accessed by children," measured by marketing to children or evidence of children's actual use.[5]

b. Utah

In March, 2023, Utah enacted the Utah Social Media Regulation Acts ("USMRA"), imposing sweeping age verification requirements for social media companies, banning minors from creating an account without parental consent, and banning their access to services between 10:30 PM and 6:30 AM. While the legislation does not specify how firms should verify users' ages, it grants the state Division of Consumer Protection sweeping power to specify identity requirements without creating any safeguards against the potential impacts on users' privacy or safety.[6]

Beginning on March 1, 2024, social media companies must: Verify the age of adults seeking to open/maintain a social media account, obtain the consent of parents or guardians of users under 18, allow parents full access to their child's account, create a default curfew setting that blocks overnight access to minor accounts (parents can adjust), protect minor accounts from unapproved direct messaging, and block minor accounts from search results.[7] Additionally, social media sites will be barred from collecting minors' data, targeting minors' accounts for advertising, and targeting addictive features towards minors' accounts.

The law raises potent privacy concerns for Utah teens' freedom of speech. Time Magazine cites arguments that young social media users will find workarounds to this legislation, as has been the case for the "over 13" age limitations implemented by major social media sites like Instagram and Facebook.[8] Teens can already bypass the USMRA's age verification measures through the use of a VPN, which combined with ambiguous enforcement mechanisms, means the law will do little more than broadly stifle online free speech.

c. *Louisiana*

In June, 2023, Louisiana passed legislation requiring all minors under 18 to obtain parental consent before making accounts on a majority of popular social media and online gaming sites. Louisiana has historically been an aggressive proponent of online censorship, being one of the first states to pass a law requiring age verification for adult entertainment websites. The newly enacted HB61 raises similar concerns as the USMRAs, including broad-based curtailment of free expression for minors and adults.

Concerns have also been expressed over the vague language used in drafting the law. HB61 bans "Interactive Computer Services" from accepting sign-ups from users under 18. The exact scope or

[5] "Four Key Considerations," Perkins Coie.
[6] S.B. 152, Social Media Regulation Amendments, Utah Senate, Gen. Sess. (Utah 2023).
[7] S.B. 152, Social Media Regulation Amendments, Utah Senate, Gen. Sess. (Utah 2023).
[8] Anisha Kohli, "Utah's Passes Laws Restricting Social Media Use for Minors," *Time*, March 25, 2023, https://time.com/6266100/utah_teens_social_media_laws/.

definition of what is considered an "interactive computer service" is not clearly defined, leaving major room for interpretation in terms of which sites and games are deserving of limitations.

As is also the case in Utah, it is unclear how the bill will properly be enforced considering that existing parental consent and age verification requirements are constantly being subverted by minors online.

III. Practical and equitable barriers

a. Privacy-preserving age verification is impossible

As a practical matter, the Surveillance Act's vision for online identity verification is utterly unworkable. The law would mean ruinous fines for internet entities that "should know that the product is accessible to and used by children" and fail to properly identify child users.[9] But for firms operating on a global internet, at a time when we know teenagers routinely access every type of site, firms know every website is accessible to children.

Perfect age verification is impossible, especially if entities seek to provide any meaningful privacy to users. Currently, many websites require users to self-certify that they are old enough to legally access the content provided (typically 13, 18, or 21 years old depending on the specific service or content). While it can be a crime to falsely certify one's age, doing so is commonplace. While other forms of age verification can make it incrementally more difficult for users to falsely certify their age, none of them are foolproof, and all come at the price of privacy and/or accessibility.

The Surveillance Act's sweeping penalties would put companies under extraordinary pressure to utilize far more invasive age verification methodologies than self-certification. As a result, the law's impact will be almost indistinguishable from Utah and Louisiana's, even if drafted quite differently. Where Louisiana and Utah explicitly direct internet firms to use draconian technologies to catalog their users, the Surveillance Act would raise the risk of bankruptcy for companies that let even a single child use their platform undetected. In each case, companies face financial incentives to impose the most aggressive age verification options.

But while companies may avoid liability by using more invasive technology, children will still suffer. First, lawmakers must face the humbling reality that the digital native children (those who came of age using digital technologies) are likely to prove adept at circumventing whatever new technology is put forward. For example, a generation ago, some websites started requiring credit card information to verify that a user was over 18 years old before realizing how many minors quickly learned to copy a caregiver's card. And like every other form of age verification in use today, credit card verification came at the price of privacy and anonymity.

Credit card verification is still used by some internet service providers and may be used by some entities to comply with the Surveillance Act. But not only is it ineffective at blocking younger users

[9] 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).

from certifying they are over 18, it also can pose an insurmountable barrier for countless adults.[10] Millions of unbanked Americans simply don't have a credit card to use to prove their age. Credit card verification compounds the digital divide, walling off the internet from those with fewer financial resources, creating an internet that is only free for those who can afford to have a bank account and credit card. In addition, massive, widespread use of credit card verification increases risks of financial fraud and "normalizes" expectations of providing sensitive financial information before accessing free information—opening the door to deeper financial exploitation for vulnerable New Yorkers, such as the elderly. It's easy to understand why a vast majority of New Yorkers - surveyed by the Ali Forney Center, Brooklyn Community Pride Center, and New Immigrant Community Empowerment (NICE) - do not feel comfortable using credit card information for age verification.[11] Over a quarter of NICE members surveyed – mostly undocumented immigrant Latinx laborers who depend on their phones for their livelihoods - even reported they would limit their internet usage if credit card data was required.[12]

No matter how well-intentioned age gating may be, this pattern continues to unfold across the full spectrum of age verification technologies: tech that can't keep kids out will also exclude adults. The situation is even bleaker for sites that move away from error-prone credit card verification to requiring government ID or facial recognition.

A variety of third-party age verification firms stand to profit from the move to new forms of age gating. Vendors like Yoti and ID.Me will become expensive, invasive add-ons for nearly any website. These vendors use more traditional forms of credit card verification, along with mobile phone service verification, third party database verification, government ID verification, facial recognition comparison, and even photo age comparison. All of these novel methodologies raise alarming threats to Americans' privacy and to open internet.

Facial recognition, photo age estimation, and other forms of biometric surveillance are a threat to everyone on the internet, but particularly to BIPOC users. Facial recognition has long been proven to be more error-prone for Black and Latinx faces, particularly Black women.[13] The same discrimination manifests with age verification, with algorithms less accurately able to estimate the age of BIPOC children and adults. In practice BIPOC children will be able to easily impersonate adults, and many BIPOC adults will be wrongly barred from websites, either told that their face doesn't match their own photo ID or that they appear younger than they actually are. Like credit card verification, a majority of survey respondents oppose using facial recognition for age verification online.[14]

---

[10] Amit Asaravala, "Why Online Age Checks Don't Work," *Wired*, October 10, 2002, https://www.wired.com/2002/10/why-online-age-checks-dont-work/.
[11] N.Y.I.I.C. Survey Results.
[12] I.D.
[13] Vítor Albiero et. al., "Gendered Differences in Face Recognition Accuracy Explained by Hairstyles, Makeup, and Facial Morphology," *IEEE Transactions on Information Forensics and Security* 17 (2022): 127–37. Natasha Singer and Cade Metz, "Many Facial-Recognition Systems Are Biased, Says U.S. Study," *The New York Times*, December 19, 2019.
[14] N.Y.I.I.C. Survey Results.

Mobile phone verification and third-party data verification are two other forms of age gating that will amplify the same disparities caused by credit card verification. Unbanked users are more likely to use pay-as-you-go cellphones that aren't linked to their name or age. And reliance on third party data is even worse, as many data sources contain incorrect or out of date information, wrongly blocking legitimate users as potential impersonators. Such an approach would close the internet off to undocumented immigrants, those with criminal justice involvement, and others who object to having their data tracked, including those who exercise opt-out or deletion rights under the California Consumer Privacy Act or proposed New York Digital Fairness Act. And for those immigrant internet users who still use websites despite such monitoring, every login will put them at risk of ICE surveillance.

Government ID verification, an increasingly common method that requires the full presentation of a government-backed ID card to access the internet, is perhaps the most Orwellian option available. Requiring government ID would exclude the millions of Americans without valid ID, replicating online the same exclusion seen at election polls in states that require government ID cards to vote.

b. Segregation of data sets

In complying with the Surveillance Act, an internet entity will likely be required to segregate data between sets of child users and adult users to govern their processing differently. Most companies collecting vast amounts of data keep data sets encrypted and mostly inaccessible. Even when identifying and sorting child users may be possible with flawed age gating methodologies, isolating data related to child users and governing it differently is not easy. If it does not prove technically feasible to reliably sort data into different governance systems, parts of the Surveillance Act become useless. For instance, it would be impossible to apply penalties or enforce the legislation, as any regulator attempting to do so would not be able to access the child data in a readable and succinct form.

For the vast majority of websites covered by the Surveillance Act, however, even the above methodologies would be brand-new, unfamiliar burdens – especially for entities such as community nonprofits whose mission is vastly different from social media or online commerce.

c. Ableist barriers

The Surveillance Act does not include any specific disability accommodations, putting children and anyone with a disability in harm's way. While laws like the Americans with Disabilities Act (ADA) already apply to websites and internet services, enforcing the ADA online and creating an accessible internet more broadly has been a decades long endeavor.[15] Rather than designing accessible services from the start, companies have only recently considered features to make websites usable for disabled people.[16] Similarly, it will take many years and lawsuits before age and identity verification

[15] "Why Americans With Disabilities Use The Internet Less Frequently," Bureau of Internet Accessibility, February 17, 2022, https://www.boia.org/blog/why-americans-with-disabilities-use-the-internet-less-frequently.
[16] David Moradi, "Despite Efforts, Businesses Struggle with Accessibility," *MIT Technology Review*, April 7, 2022, https://www.technologyreview.com/2022/04/07/1048543/despite-efforts-businesses-struggle-with-accessibility/.

services implemented to comply with the Surveillance Act become inclusive of disability, potentially locking disabled people out of the internet once again.

d. Corporate snooping becomes more invasive

To comply with the Surveillance Act, websites and online services will need to collect additional personal information to determine if a user is under 13.[17] This process can involve collecting more data than previously necessary, leading to greater invasiveness when websites do not collect identifying data for other purposes. Now, under the Surveillance Act, these websites would be compelled to collect identifiable data, and may reuse it for consumer surveillance. Companies also will also be incentivized to collect and retain user information to demonstrate compliance with the Surveillance Act. This could involve storing more information about user interactions, verifiable parental consent, or other records.

e. Effects on undocumented migrants

Age and identity verification requirements will harm undocumented communities—within New York and nationally—in irreversible ways. In recent years, ICE routinely drew on commercial databases and internet service providers' to track and deport undocumented families.[18] ICE has paid businesses, including Thomson Reuters and RELX, tens of millions of dollars in exchange for access to sensitive information, including the CLEAR database, which combines "data from credit agencies, cellphone registries, social-media posts, property records, utility accounts, fishing licenses, internet chat rooms and bankruptcy filings, all fused and vetted by algorithm to form an ever-evolving, 360-degree view of U.S. residents' lives."[19] ICE has also sent tens of thousands of subpoenas to digital platforms such as Google, Twitter and Meta.[20] The demands of these subpoenas have included various sensitive details of its users, including users' IP addresses, names, addresses, and billing information.[21] ICE has even weaponized the social media presence of migrants, monitoring activity on Twitter, Instagram and other platforms to obtain identifying details about migrants, such as date of birth and criminal history.[22] ICE uses this information to support a national surveillance dragnet to surveil every American and deport those who are undocumented.[23]

---

[17] Emma Roth, "Online Age Verification Is Coming, and Privacy Is on the Chopping Block," *The Verge*, May 15, 2023, https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety.

[18] Mckenzie Funk, "How Ice Picks its Targets in the Surveillance Age," *The New York Times,* October 22, 2019, https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

[19] Cora Currier, "Lawyers And Scholars To LexisNexis, Thomson Reuters: Stop Helping Ice Deport People," *The Intercept,* November 19, 2019, https://theintercept.com/2019/11/14/ice-lexisnexis-thomson-reuters-database/.

[20] Dhruv Mehrotra, "ICE Is Grabbing Data From Schools and Abortion Clinics," *Wired*, April 3, 2023, https://www.wired.com/story/ice-1509-custom-summons/.

[21] Johana Bhuiyan, "Revealed: the contentious tool US immigration uses to get your data from tech firms," *The Guardian*, May 25, 2023, https://www.theguardian.com/us-news/2023/may/25/us-immigration-surveillance-google-twitter-meta-personal-data.

[22] "How An Occupy Ice Activist and Daca Recipient Was Deported for Tweeting," *The Intercept,* November 2, 2019, https://theintercept.com/2019/11/02/deportation-occupy-ice-daca/.

[23] Cindy Carcamo, "Immigration Officials Created American Surveillance Network," *Governing*, May 11, 2022, https://www.governing.com/security/immigration-officials-created-american-surveillance-network.

This ever-widening ICE surveillance dragnet has compelled many undocumented migrants to go to great lengths to protect their anonymity. Many undocumented people in the U.S. have become increasingly wary of using any digital platform traceable to their legal name and immigration status. However, the Surveillance Act would make it impossible for members of migrant communities in the U.S. to maintain any anonymity on the internet.

Age and identity verification requirements would force undocumented migrants to avoid all internet use, or risk arrest and deportation. Indeed, if the Surveillance Act passes, many migrants would likely remove all ties to the internet to protect themselves and their families. According to one survey respondent from NICE, "Online resources are a huge part of today's society. Taking this away can destroy a person's life. Not being able to access job listings, information, and housing listings can all lead to poverty and a decrease of life quality."[24] Indeed, nearly a third of all NICE respondents – predominantly undocumented Latino/a workers – indicated that they had serious concerns with being required to use government ID to use the internet.

Given the enormous role that the internet plays in modern life, this would mean that up to tens of millions of migrants across the U.S. would be cut off from major services that are key to their everyday lives. Without access to the online world, migrants would lose crucial tools that both help them maintain ties to their native countries and allow them to resettle more easily. Many rely on online services to connect with family members and other loved ones abroad, to access information and resources that help them adjust to life in the United States, or to earn remuneration by performing work for online companies such as UberEats or DoorDash. Forcing migrants to self-censor and abandon the internet would create emotional and practical labor for people who may have already fled traumatic experiences or are merely dealing with the everyday trauma of undocumented life in the United States.

f. Effects on LGBTQIA+ youth

The Surveillance Act doesn't only leave undocumented communities vulnerable, it also threatens LGBTQIA+ youth. The legislation requires anyone under 18, including those who are in college or foster care and those who are legally emancipated, to obtain parental consent and submit to tracking for access to internet services.[25] Invoking one-size-fits-all parental access neglects the queer and trans young people who have homophobic or transphobic parents, or who are simply not yet comfortable revealing their sexualities to their parents.

Children and teenagers have relied on online communities as safe spaces and supportive lifelines for decades. The internet, while flawed, has been a lifeline for queer and trans youth. Digital spaces allowed for inclusive remote communities even when they physically reside in unaccepting places. Online platforms such as TrevorSpace, It Gets Better Project, and less formal chat forums in spaces like video games, allow queer and trans youth who live in intolerant households to interact with

[24] N.Y.I.I.C. Survey Results.
[25] S. 3281, N.Y. State Senate, 2023-2024 Reg. Sess. (N.Y. 2023).

other young LGBTQIA+ people.[26] While touting child safety, surveillance bills threaten to cut off queer youth from online communities and isolate those who need connection most.

Additionally, internet services and malicious lawmakers can use the Surveillance Act to justify online censorship. For example, websites could censor the discussion of sexuality during Pride month (e.g., "I am bi," or "support trans rights") under the justification of removing content that is not age appropriate. In fact, homophobic and transphobic groups have pointed to child privacy legislation similar to the Surveillance Act as a tool to force internet entities to remove content shared by sexual and gender queer users.[27] Indeed, the Surveillance Act's implications are similar to Florida's "Don't Say Gay" law. The "Don't Say Gay" law, which restricts any classroom instruction regarding sexual orientation or gender identity for students grade three and below, institutionalizes the erasure of LGBTQ youth—as well as LGBTQIA+ history, culture, and identity.[28] The New York Surveillance Act could similarly facilitate a similar erasure—a digital erasure of access to information for and about LGBTQIA+ youth.

At a moment in which the LGBTQIA+ community is facing constant threats to their safety and livelihood, safe online spaces are more important than ever, but bills like the New York Surveillance Act would eliminate them. The LGBTQIA+ community has faced centuries of abuse and oppression and increasing violence and precarity in the past few years. And the U.S. has seen a rise in violent and deadly hate crimes against trans and gender non-conforming people and an increase in discriminatory legislation in many U.S. states.[29] If teens are required to register their internet usage with parents, digital lifelines will become a potential threat that outs users to the very parents many are hiding from.[30]

And while the New York Surveillance Act poses many risks to LGBTQIA+ youth, similar surveillance bills in more conservative states, such as Utah, Louisiana, and Arkansas, are even worse. In those states, LGBTQIA+ youth are far more likely to live with homophobic or transphobic parents, whose monitoring of their internet and social media could be life-threatening.[31] Moreover, in such states, queer and trans folks are already facing legislative attacks on their humanity in bills that ban gender-affirming care for minors.[32] Surveillance bills only serve to compound the

---

[26] Claire Cain Miller, "For One Group of Teenagers, Social Media Seems a Clear Net Benefit," *The New York Times*, May 24, 2023 www.nytimes.com/2023/05/24/upshot/social-media-lgbtq-benefits.html.

[27] Mike Masnick, "Heritage Foundation Says That Of Course GOP Will Use KOSA To Censor LGBTQ Content," *Tech Dirt*, May 24, 2023, https://www.techdirt.com/2023/05/24/heritage-foundation-says-that-of-course-gop-will-use-kosa-to-censor-lgbtq-content/.

[28] Solcyre Burga, "Florida's New 'Don't Say Gay' Laws: What They Mean for Kids," *Time*, April 20, 2023.

[29] Madeleine Carlisle, "Anti-Trans Violence Reaches Record Highs across U.S. in 2021," *Time*, December 31, 2021, time.com/6131444/2021-anti-trans-violence/.

[30] Evan Enzer, "POV: We Need to Give Kids Their Space Online," *Fast Company*, November 21, 2022, https://www.fastcompany.com/90812915/pov-we-need-to-give-their-kids-space-online.

[31] Anna Brown, "Deep Partisan Divide on Whether Greater Acceptance of Transgender People Is Good for Society," *Pew Research Center*, February 11, 2022, www.pewresearch.org/short-reads/2022/02/11/deep-partisan-divide-on-whether-greater-acceptance-of-transgender-people-is-good-for-society/.

[32] "Attacks on Gender Affirming Care by State Map," *Human Rights Campaign*, accessed July 26, 2023, www.hrc.org/resources/attacks-on-gender-affirming-care-by-state-map.

restrictions that LGBTQIA+ youth are already facing by cutting off one of the only remaining lifelines they have to gender-affirming care: the internet.

According to original research by LGBTQIA+ service providers, who surveyed LGBTQIA+ young people, 80% of survey respondents oppose forcing minors to obtain parental consent before using the internet.[33] Over 90% think ID verification and parental monitoring would be disastrous for LGBTQIA+ people, chilling their access to resources.[34]

Online freedom in New York is more important than ever after attacks on trans rights elsewhere. As a result of the recent bans on gender-affirming care across the country, New York has become a refuge state for people seeking healthcare illegal in their home states.[35] If the New York Surveillance Act is passed, young people who have travelled to New York seeking access to care will once again be cut off from it.

g. Effects on reproductive rights

There is immense danger in allowing police, prosecutors, and private anti-choice groups to surveil abortion seekers. While New York's abortion protections are strong, other states have draconian laws against reproductive care, and they could utilize data collected through the New York Surveillance Act to prosecute people traveling for reproductive healthcare. Children who move to New York to escape dangerous family situations or attend school could be subject to prosecution for seeking reproductive health care, even if they temporarily live away from their home-state. Additionally, online telehealth, is a primary source for abortion inducing prescriptions, but attaching an identity verification requirement to online reproductive health services puts nationwide abortion seekers at risk when they access a New York doctor's website.[36]

The Surveillance Act's parental consent mandate is also a dangerous threat to abortion access in New York. Parental consent makes it impossible for minors seeking reproductive healthcare to do so confidentially, compromising their security and ability to access care if parents object. The Surveillance Act's simplistic age cut off of 18 includes a wide range of young adults who may not even live under the care of their guardians—youth at college, in foster care, or those who have been legally emancipated would all be cut off from reproductive care.

The end result could be a significant chilling effect that denies reproductive healthcare to both New Yorkers and those fleeing their home state for potentially lifesaving care. According to another

[33] N.Y.I.I.C. Survey Results.
[34] N.Y.I.I.C. Survey Results.
[35] "New York City Welcomes Growing Number of Out-of-State Abortion Patients," *The New York Times*, April 12, 2023, https://www.nytimes.com/2023/04/12/nyregion/abortions-out-of-state-nyc.html.
[36] "Roadblock to Care" (Surveillance Technology Oversight Project 2023), https://www.stopspying.org/roadblock-to-care. "Pregnancy Panopticon: Abortion Surveillance After Roe," (Surveillance Technology Oversight Project 2022), https://www.stopspying.org/pregnancy-panopticon.
[36] S. 3281, N.Y. State Senate, 2023-2024 Reg. Sess. (N.Y. 2023). To be codified at N.Y. Gen. Bus. Law § 899 CC (7)(B).

survey respondent, "Access to information for vulnerable people is crucial. So, any barrier to lifesaving information, such as health care, could have grave consequences."[37]

b. Effects on victims of domestic violence and abuse

Like LGBTQ+ youth, the Surveillance Act cuts minors facing domestic violence and abuse off social media and other important platforms. Many abused people turn to the internet for help, whether seeking out social services, self-help resources, or examples of others who have escaped similar situations. Under the Surveillance Act, abusive parents can block all access to these resources by withholding consent. The Surveillance Act, and like bills, seriously hamper the ability of children to find anonymous help, restricting their ability to find support and putting them as risk of additional violence.[38]

IV. Courts will likely strike down the Surveillance Act

Laws like the Surveillance Act have already faced constitutional challenges in other states. A number of social media companies sued California to challenge the Code on multiple fronts.[39] Additionally, Utah's strict limitations on underage users has drawn national criticism for infringing on free speech.[40] The Surveillance Act will inevitably face similar lawsuits on overbreadth and First Amendment grounds.

Per the First Amendment's overbreadth doctrine, a law is unconstitutionally overbroad if it prevents a sizable portion of protected speech. The Surveillance Act utilized broad and unclear definitions and restrictions to drastically curtail legal speech, and it is clear this legislation is a minefield for lawsuits from the likes of internet companies and advocates. For instance, the Surveillance Act's broad bans on personalized advertising for products "intended primarily for educational purposes" could apply to everything from community blogs and Reddit forums to respected legacy newspapers like the New York Times. Without narrowing, these provisions very likely violate the First Amendment.

Additionally, section 4(c) of the Surveillance Act transforms the state attorney general into the Editor-in-Chief of the internet and would 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 would enable the Attorney General's Office to unilaterally redesign any aspect of the internet it calls unfit for children. Such a provision allows the attorney general unfettered discretion to target any internet

[37] N.Y.I.I.C. Survey Results.
[38] Enzer, "Give Kids Their Space."
[39] Queenie Wong, "California Lawmakers Want to Make Social Media Safer for Young People. Can They Finally Succeed?," *Los Angeles Times*, August 9, 2023, https://www.latimes.com/politics/story/2023-08-09/meta-instagram-twitter-tiktok-social-media-onlinesafety.
[40] Christopher Hutton, "Utah Teenage Social Media Law Threatens Privacy and Speech Rights, Industry Says," *Washington Examiner*, March 24, 2023, https://www.washingtonexaminer.com/policy/technology/utah-social-media-bill-industry-groups. Kevin Goldberg, "Utah Social Media Laws: Why New Bills Are Unconstitutional," *Freedom Forum* (blog), April 12, 2023, https://www.freedomforum.org/utah-social-media-laws/.

feature that enables speech they disagree with, even protected political or religious speech. Section 4(c) is an unwieldy grant of power that runs contrary to the New York State and Federal Constitutions and antithetical to democracy itself.

V. We have an alternative

To acknowledge that the Surveillance Act is unconstitutional and harmful to already vulnerable communities does not dismiss the goal of protecting young people online. But there is a way to protect New York youth without this legislation: protect *everyone's* privacy and civil rights.

Generally applicable limits on targeted advertising, addictive product design, and data collection are long overdue protections for all New Yorkers. The beauty of this approach, one that does not exclude adults, is that lawmakers can secure even broader benefits than the Surveillance Act with fewer risks. For example, 19 and 20-year-olds would benefit from many of the same protections from predatory data use that the Surveillance Act envisions for those under 18. Every New Yorker should be safe from invasive data collection, by focusing on safeguards that apply to both teenagers and adults, lawmakers can protect more users and avoid the harms of age gating and identity verification.

VI. Conclusion

While surveillance bills, such as the New York Surveillance Act, claim to protect children and teens, they fail to truly consider the needs of the diverse and vast group of people they cover. Young people are not a monolith, and many youth communities—including LGBTQIA+ people, undocumented migrants, and abortion seekers—would be hurt by the Surveillance Act rather than protected. Moreover, the bill is impractical from a technical or enforcement perspective, and the high likelihood that court will strike it down, render the Surveillance Act a useless endeavor. Lawmakers should enact legislation that recognizes digital safety as a universal right, rather than a privilege that is irresponsibly doled out to a select few and that harms large swaths of the U.S. population.

SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT, INC.
40 RECTOR STREET
9TH FLOOR
NEW YORK, NY 10006
WWW.STOPSPYING.ORG

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT