Legislative Affairs
125 Broad Street, 19th Floor
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of the New York Civil Liberties Union
Before the Joint Legislative Budget Hearing on Economic Development/Arts

February 26, 2026

The New York Civil Liberties Union (NYCLU) is grateful for the opportunity to submit the following testimony for the Joint Legislative Budget Hearing on Economic Development/Arts. The NYCLU advances civil rights and civil liberties so that all New Yorkers can live with dignity, liberty, justice, and equality. Founded in 1951 as the state affiliate of the national ACLU, we deploy an expert mix of litigation, policy advocacy, field organizing, and strategic communications. Informed by the insights of our communities and coalitions and powered by 90,000 member-donors, we work across complex issues to create more justice and liberty for more people. As part of a nationwide network of ACLU affiliates, we offer not only our own experience working at the intersection of speech, privacy, and technology, but also the lessons learned by our sister affiliates in states that have been on the cutting edge of litigating and legislating to protect privacy in the digital age. In addition, as the legal arm of New York's reproductive rights movement, the NYCLU strives to ensure that New York remains a beacon for equality and bodily autonomy and the full range of reproductive rights, from access to abortion care to birth justice. The NYCLU also fights for LGBTQ New Yorkers by advancing access to health care, as well as protections in the workplace, education, housing, and more. We fight the criminalization of trans lives and abuse in prisons and jails. We advocate for state recognition of LGBTQ identities and help New Yorkers know their rights.

I. Introduction and Background

It is no longer possible to participate in society without providing personal information to private companies and other third parties that may, in and of itself, reveal intimate details of one's life, or that, when combined with other data and analyzed, may expose such information. The consequences can be profound. For example, personal information has been leveraged to ensure that only younger men see certain job postings and to exclude African-Americans from viewing certain housing advertisements.[1] Personal information has also been used to target advertisements to African-Americans urging them not to vote[2] and to identify and track

[1] *See* Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU SPEAK FREELY, Mar. 19, 2019, https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping.
[2] Natasha Singer, *Just Don't Call It Privacy*, NYTIMES, Sept. 23, 2018, https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.

participants in Black Lives Matter protests.[3] The U.S. military has harvested data from a Muslim prayer app and a Muslim dating app to track users' location – particularly chilling in a community that has long been subjected to intrusive government surveillance.[4] Reporting on these and other phenomena, the *New York Times* observed that exploitation of personal information enables "unequal consumer treatment, financial fraud, identity theft, manipulative marketing, and discrimination."[5]

And yet, New Yorkers – and people across the country – demonstrate time and again that they care about privacy. Ninety-two percent of Facebook users alter the social network's default privacy settings, indicating that they wish to choose with whom they share personal information.[6] Similarly, ninety-two percent of Americans believe companies should obtain individuals' permission before sharing or selling their personal information.[7] The same percentage believe that entities should be compelled to provide individuals with a list of all the data they have collected about them,[8] and more individuals in the United States use Microsoft's dashboard to access the personal information Microsoft has about them than individuals in Europe do.[9] In fact, seventy-six percent of Americans believe they do not have "enough control over how companies use their data."[10]

Unfortunately, rather than protecting individual privacy in the digital age, Parts Y and AA of the Executive Transportation, Economic Development, and Environmental Conservation (TEDE) Article VII Legislation would undermine anonymous communications on the internet, render vulnerable young people less safe, and give New Yorkers a false sense of security in and control over the personal information they share online. For these reasons, the legislature

---

[3] Jonah Engel Bromwich, Daniel Victor, & Mike Isaac, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, NYTIMES, Oct. 11, 2016, https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html; Ethan McLeod, *Police Arrested Freddie Gray Protesters Last Year by Surveilling Social Media*, BALTIMORE FISHBOWL, Oct. 12, 2016, https://baltimorefishbowl.com/stories/police-arrested-freddie-gray-protesters-last-year-surveilling-social-media/.

[4] Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE, Nov. 16, 2020, https://www.vice.com/en/article/us-military-location-data-xmode-locate-x/; Kate Ruane, *Privacy Rights Do Not Come With a Price Tag*, ACLU, Apr. 21, 2021, https://www.aclu.org/news/privacy-technology/privacy-rights-do-not-come-with-a-price-tag.

[5] *Id*.

[6] Emil Protalinksi, *13 million US Facebook users don't change privacy settings*, ZDNET, May 3, 2012, https://www.zdnet.com/article/13-million-us-facebook-users-dont-change-privacy-settings/.

[7] Christopher Boone, Vice President of Real World Data and Analytics, Pfizer, The Business of Big Data, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

[8] *Id*.

[9] Julie Brill, Corporate Vice President and Deputy General Counsel for Global Privacy and Regulatory Affairs, Microsoft, Former Enforcers Perspective: Where Do We Go From Here? What is Right, Wrong, or Indeterminate about Data Policy?, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 8, 2018).

[10] *Ipsos Consumer Tracker*, IPSOS, Oct. 24, 2025, https://www.ipsos.com/en-us/latest-us-opinion-polls#:~:text=Ipsos%20Consumer%20Tracker,-Washington%2C%20DC%2C%20October&text=The%20poll%20also%20finds%20that%20three%20in%20four%20Americans%20(76,from%20October%202024%20(53%25.

should **omit Parts Y and AA from its one-house budgets** and work through the regular legislative process to advance meaningful privacy protections for New Yorkers.

II. The Legislature Must Omit TEDE Part Y from the FY2027 Budget

TEDE Part Y requires all online platforms to conduct "age assurance" checks and to provide minors with "privacy by default," which prohibits anyone who is not currently connected with the young person to communicate privately with them, to view or respond to their online posts, to tag them in posted media, or to view their geolocation. AI companions must also be disabled for young people's accounts by default. For young people under the age of thirteen, a parent or guardian must approve all connections a young person makes on an online platform. Part Y also establishes parental controls and oversight over youth spending on online platforms.

TEDE Part Y responds to important concerns about young people's safety and wellbeing online. Unfortunately, it does so in ways that will have unintended consequences for internet users of all ages, that will render some of the most vulnerable young people less safe, and that violate federal constitution.

A. Part Y's Age Assurance Requirement is a De Facto Unconstitutional Prohibition on Anonymous Speech on Online Platforms.

TEDE Part Y requires all online platforms to engage in "age assurance" and prohibits "self-declaration" of age as a method of age assurance.

Individuals of all ages rely on online platforms for political speech, artistic expression, advocacy, access to the news, and more. Age assurance requirements burden users who may want to engage in anonymous speech, who do not have a government ID, or who are otherwise concerned about their privacy and security. Age assurance schemes "are not only an additional hassle," but "they also require that website visitors forgo the anonymity otherwise available on the internet."[11] They force users to "relinquish their anonymity to access protected speech, and . . . create a potentially permanent electronic record" of the sites users choose to visit.[12] That "constitutes an encroachment into the personal lives of those who use the internet precisely because it affords anonymity."[13] For these reasons, courts across the country have struck down age assurance laws almost everywhere they've been enacted because they burden those who wish to use online platforms anonymously;[14] deter lawful users who cannot or will

[11] *Am. Booksellers Found. v. Dean*, 342 F.3d 96, 99 (2d Cir. 2003).
[12] *ACLU v. Mukasey*, 534 F.3d 181, 197 (3d Cir. 2008).
[13] *State v. Weidner*, 235 Wis. 2d 306, 320 (2000).
[14] *See ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D.N.M. 1998) (holding that mandatory age verification "violates the First and Fourteenth Amendments of the United States Constitution because it prevents people from communicating and accessing information anonymously"), *aff'd*, 194 F.3d 1142 (10th Cir. 1999).

not verify their age;[15] and because they raise significant privacy concerns.[16] Where less restrictive alternatives exist, the government cannot impose age assurance on adults in the name of protecting young people.

The offense here is particularly grave because the Executive proposal prohibits self-declaration of age, meaning that people will effectively be required to provide identification. This concern is not mitigated by the proposal's requirement that information collected for the purpose of age assurance be deleted immediately nor by its prohibition on repurposing age assurance information. More than three-quarters of people in the U.S. broadly distrust online platforms,[17] and more than seventy percent of them are skeptical of the government's ability to hold platforms accountable for misusing their personal information.[18] These individuals are unlikely to trust online platforms to actually delete their age assurance information, even if required by law.

What is more, simply the perception of being watched changes people's behavior.[19] Requiring someone to show identification to access an online platform – even if the identity information is ultimately deleted – is likely to contribute to a perception of being watched and chill participation in digital life and utilization of online services.[20]

---

[15] *See*, *e.g.*, *PSINet, Inc. v. Chapman*, 362 F.3d 227, 236-37 (4th Cir. 2004) (age-verification using credit card numbers "creates First Amendment problems of its own" because "many adults may be unwilling to provide their credit card number online" and "[s]uch a restriction would also serve as a complete block to adults who wish to access adult material but do not own a credit card"); *Se. Booksellers Ass'n v. McMaster*, 371 F. Supp. 2d 773, 782 (D.S.C. 2005) (holding that age verification creates a "First Amendment problem" because "age verification deters lawful users from accessing speech they are entitled to receive").

[16] *See NetChoice, LLC v. Bonta*, No. 22-CV-08861-BLF, 2023 WL 6135551, at *12 (N.D. Cal. Sept. 18, 2023) (noting the California Age Appropriate Design Code's age verification provision was "actually likely to exacerbate the problem by inducing covered businesses to require consumers, including children, to divulge additional personal information.").

[17] *See generally* Colleen McClain, Michelle Faverio, Monica Anderson, & Eugene Park, *How Americans View Data Privacy*, PEW RESEARCH CENTER, Oct. 18, 2023, https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

[18] *Id*.

[19] *Cf.* Keith Dear, Kevin Dutton, & Elaine Fox, *Do 'watching eyes' influence antisocial behavior? A systemic review & meta-analysis*, 40 EVOLUTION & HUMAN BEHAVIOR 269 (May 2019).

[20] *E.g.* Avi Goldfarb, Rotman Chair in Artificial Intelligence and Healthcare, Rotman School of Management, University of Toronto, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018) (testifying that "it's much harder to get people to fill out surveys than it used to be."); Lior Strahilevitz, Sidley Austin Professor of Law, University of Chicago Law School, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018) (testifying that fewer people answer their cell phones today "if it's an unrecognized number."); Amalia Miller, Associate Professor of Economics, University of Virginia, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018) (testifying that if individuals "don't feel that their data are safe, they may not download apps on their phone . . . They may shut off Facebook or never post their child online because they don't feel that privacy is protected" and observing that the U.S. has been slower to adopt electronic medical records, leading to "greater mortality, greater infant mortality.").

Perhaps worse still, not everyone has identification, like a driver's license, or is even eligible for one. Birth certificates and other vital records are often lost to time. Government identification measures may not accurately reflect a person's gender, and obtaining an ID that does may not be possible.[21] Not everyone has a credit card, a bank account, or a utility bill, and many people rightly do not trust online platforms with their financial information. Those without an ID – or an accurate ID – are disproportionately poor, older, immigrant, transgender, or Black.[22]

Most offensively, Part Y's textual justification for prohibiting self-declaration of age is to prohibit adults from seeking privacy protections by default.[23] This is unlikely to pass muster as an important governmental interest in a First Amendment challenge should Part Y become law.

B. Part Y Will Inadvertently Trap Vulnerable Young People in Unsafe Situations

We all want young people to be healthy, affirmed, and safe and to have the support and information they need to learn, grow, and make important decisions for themselves and their futures. The majority of young people involve a parent when they encounter challenging situations or have major questions they are exploring; indeed, parent and family support is a primary predictor of a young person's well-being.[24] Unfortunately, some young people cannot involve a parent for reasons rooted in their own safety and well-being, including fear of physical or emotional abuse, loss of financial support or homelessness, or other serious family problems.[25] Even young people who feel safe in their families generally may still wish to not involve a parent in particularly sensitive aspects of their lives, and that should be their decision.

Since the advent of the internet, LGBTQ young people have turned to connections online to find community and imagine a future for themselves. Some young people make connections on the internet to seek access to abortion care or information about sexual orientation, gender identity, contraception, abortion, mental health or substance abuse treatment, STI or HIV testing or treatment, or other topics that are stigmatized.[26] And, in the most egregious of circumstances,

---

[21] *See generally Trump v. Orr*, __ U.S. __ (Nov. 6, 2025).
[22] *See generally* THE ID DIVIDE: HOW BARRIERS TO ID IMPACT DIFFERENT COMMUNITIES AND AFFECT US ALL (Movement Advancement Project, Nov. 2022), *available at* https://www.mapresearch.org/id-documents-report.
[23] The actual language reads, ". . . to ensure an adult cannot pose as a minor, an operator cannot use self-declaration of age or minor status to determine whether a user is a covered minor[.]" A.10008/S.9008 Part Y § 2, 2025-2026 Reg. Sess. (NY 2026). Given that neither minors nor adults can connect with a young person without parental consent, the only thing this provision accomplishes is preventing adults from selecting privacy by default.
[24] *See generally* L. Edwards-Leeper & N. P. Spack, *Psychological evaluation and medical treatment of transgender youth in an interdisciplinary "Gender Management Service" (GeMS) in a major pediatric center*, 59 J. OF HOMOSEXUALITY 321 (2012); J. Rafferty, *Ensuring comprehensive care and support for transgender and gender-diverse children and adolescents*, 142 PEDIATRICS (2018).
[25] LA Hasselbacher, A Dekleva, S Tristan, ML Gilliam, *Factors influencing parental involvement among minors seeking an abortion: A qualitative study*, AM J. PUBLIC HEALTH, 104, 2207-11 (2014).
[26] *See* Brendan J. Lyons & Joshua Solomon, *Big Tech enlists 'vulnerable' groups to thwart internet safety bills*, TIMES UNION, Mar. 14, 2024, https://www.timesunion.com/capitol/article/big-tech-enlists-vulnerable-

young people may make connections on the internet to escape family violence at home. It is critical for these vulnerable young people to be able to communicate privately and connect with others on the internet, even, and perhaps especially, when it may not be safe for them to involve their families.

For these reasons, we urge the legislature to **omit TEDE Part Y from the FY2027 budget.**

III. The Legislature Must Omit TEDE Part AA from the FY2027 Budget

TEDE Part AA creates a data broker registry and suggests that it might require data brokers to delete individuals' personal information and allow them to opt-out of sale and sharing of personal information upon request. However, as drafted the proposal is unlikely to require any actual deletion or limitations on sales or sharing of personal information; instead, it is likely to give New Yorkers a false sense of security. This is, perhaps, at least in part because it is based on California's Delete Act.[27] California's Delete Act builds and relies upon California's pre-existing comprehensive privacy law.[28] New York has no underlying comprehensive privacy law, and many of Part AA's provisions make little sense in the absence of such a foundation. What is more, the Part is rife with drafting choices – and errors – that undermine its intended purpose.

A. TEDE Part AA Does Not Effectively Require Data Brokers to Delete Individual Information

It is difficult, from a First Amendment perspective, to regulate data brokers directly. In *Sorrell v. IMS Health Inc.*, the Supreme Court found that many of the behaviors data brokers engage in – namely the "sale, transfer, and use of data"[29] – are First Amendment-protected speech and overturned a Vermont statute that prohibited regulated entities from "selling or disseminating prescriber-identifying information for marketing," subjecting content- and speaker-based restrictions "on the sale, disclosure, and use of" personal information to heightened scrutiny.[30] Because the activities of journalists, opposition researchers, and data brokers – collecting and disseminating information – are very similar, restrictions on data brokers are likely to be viewed as a speaker-based distinction subject to heightened scrutiny under *Sorrell*.

TEDE Part AA may successfully avoid a First Amendment challenge because as currently drafted, it does not actually require any data deletion or limitations on data collection, sharing,

---

groups-thwart-18927407.php ("[C]oncerns include that LGBTQ youth and young people seeking reproductive health information online, but who have unsupportive families, may be blocked from that access.").

[27] *See generally About DROP and the Delete Act*, CALIFORNIA PRIVACY PROTECTION AGENCY, https://privacy.ca.gov/drop/about-drop-and-the-delete-act/ (last visited Feb. 20, 2026).

[28] *See generally Rights under the California Consumer Privacy Act*, CALIFORNIA PRIVACY PROTECTION AGENCY, https://privacy.ca.gov/california-privacy-rights/rights-under-the-california-consumer-privacy-act/ (last visited Feb. 20, 206).

[29] Molly Cinnamon, *You Have the Right to Be Deleted: First Amendment Challenges to Data Broker Deletion Laws*, 9 Geo. L. Tech. Rev. 492, 510 (2025).

[30] 564 U.S. 552, 562 – 65 (2011).

and sales. TEDE Part AA requires data brokers to register and provide information indicating "**if** the data broker permits a consumer to opt-out of" its data collection, databases, or data sales (emphasis added).[31] This provision on its face appears to suggest that permitting such opt-outs is optional for data brokers.

The proposal does later purport to require data brokers to delete information upon request and where a deletion "request cannot be verified," a data broker is directed to "process such request as an opt-out of the sale or sharing of such consumer's personal information."[32] The bill, however, does not separately require data brokers to honor opt-outs of sale or sharing of personal information, and no existing New York law provides such a requirement. The only reasonable interpretation is that where the opt-out request kicks in, it will be entirely subject to whether the data broker has, of its own goodwill, decided to offer such an option in New York.

In addition, the deletion requirement itself is accompanied by so many exceptions that it is unlikely that any information will actually be deleted. Exemption (a)(iv), to "exercise free speech,"[33] alone likely permits a data broker to retain any data it wishes to. This is because the data broker itself maintains free speech rights, and, as described above, the Supreme Court has held that the "sale, transfer, and use of data" are First Amendment-protected speech.[34] Courts are also increasingly finding that everything from targeted advertising to delivering search results – along with anything done by an algorithm – is protected speech.[35] A data broker can claim that any required deletion violates its own free speech rights and continue to maintain information.

As if that loophole is not enough, Part AA also permits data brokers to refuse a deletion request if it is "reasonably necessary" to maintain a person's information "within the context of a business' ongoing relationship with such consumer,"[36] "to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on such consumer's relationship with the business and compatible with the context in which such consumer

---

[31] A.10008/S.9008 Part AA § 2, 2025-2026 Reg. Sess. (NY 2026).
[32] *Id*.
[33] *Id*.
[34] Molly Cinnamon, *You Have the Right to Be Deleted: First Amendment Challenges to Data Broker Deletion Laws*, 9 Geo. L. Tech. Rev. 492, 510 (2025).
[35] *See, e.g.*, *NetChoice, LLC v. Att'y Gen., Fla.*, 34 F.4th 1196, 1213 (11th Cir. 2022) (social media content moderation protected by the First Amendment to the same degree as the press' editorial discretion); *see also*, *e-ventures Worldwide, LLC v. Google, Inc.*, 2017 WL 2210029, at *4 (M.D. Fla. Feb. 8, 2017) (analogizing Google's search results to a newspaper editor's publishing decisions, and affording full First Amendment protection), *citing Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 258 (1974); *Langdon v. Google*, 474 F. Supp. 2d 622, 629–30 (D. Del. 2007) (same holding, same rationale); *Search King Inc. v. Google Tech., Inc.*, No. CIV-02-1457-M, 2003 WL 21464568, at *4 (W.D. Okla. May 27, 2003) (same – "Google's PageRanks are entitled to "full constitutional protection."); *Zhang v. Baidu.com, Inc.*, 10 F. Supp. 3d 433, 435 (S.D.N.Y. 2014) ("the First Amendment protects as speech the results produced by an Internet search engine."); *but see*, *Dreamstime.com, LLC v. Google, LLC*, No. C 18-01910 WHA, 2019 WL 2372280, at *2 (N.D. Cal. June 5, 2019) (acknowledging editorial control akin to *Miami Herald* but nonetheless denying Google's motion to dismiss a breach of contract case, stating that, even assuming 1A protections, Google has "no special immunity from the application of general laws.").
[36] A.10008/S.9008 Part AA § 2, 2025-2026 Reg. Sess. (NY 2026).

provided the information,"[37] or if the data broker stored the individual's information while the individual was in New York and then collected it when the individual "and stored personal information is outside of New York."[38]

Reasonably necessary is itself a liberal standard that puts far looser safeguards on companies' use of personal information than a strictly necessary standard. This means that it allows companies a freer hand to use people's personal information in ways that benefit the company to the detriment of the individual, or at best, with no benefit to the individual. In combination with the exceptions listed, it will easily result in the exemptions swallowing the rule.

The first two of these carve-outs presuppose a relationship with data brokers that individuals do not have. Most individuals do not have direct relationships with data brokers and are not directly providing their personal information to data brokers. To the extent that there is any "ongoing relationship," it consists of data brokers hoovering up people's personal information without their knowledge or consent, and this exception seems to permit that behavior to continue. What is more, nearly three quarters of Americans believe they have no control over what companies do with their data,[39] suggesting strongly that ignoring a deletion request would align with individual expectations.

The final exception invites data brokers to store New Yorkers' personal information indefinitely while they are in New York and then collect and process it when they leave the state, also circumventing the bill's purported deletion requirements.

For all of these reasons, Part AA is likely to give individuals a false sense of security – namely the impression that they have a right to delete or request limitations on sales and sharing of their data that they simply will not have.

B. TEDE Part AA is Poorly-Drafted

1. TEDE Part AA Includes a Sensitive/Non-Sensitive Distinction that Undermines Privacy

Rather than define personal information straightforwardly and in an evergreen way as any information that is reasonably linkable, directly or indirectly, to a specific individual, household, or device, TEDE Part AA's definition of personal information subject to its supposed deletion requirement is a laundry list of particular types of data and includes what the bill describes as "sensitive personal information," perhaps giving data brokers freer rein to maintain and do whatever they want with supposed "non-sensitive" information. As a threshold matter, much of the list of "sensitive personal information" is already separately included

[37] *Id*.
[38] *Id*.
[39] *See generally* Colleen McClain, Michelle Faverio, Monica Anderson, & Eugene Park, *How Americans View Data Privacy*, PEW RESEARCH CENTER, Oct. 18, 2023, https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

within the definition of "personal information,"[40] and it is not clear what drafters mean to accomplish by listing these categories twice.

More importantly, drawing lines between sensitive and non-sensitive information is increasingly illogical in the digital age. So-called non-sensitive information can be aggregated to reveal sensitive information, and, in fact, some non-sensitive information, in isolation, may reveal sensitive information. For example, while health status is frequently considered sensitive, shopping history is not. But, if an individual is shopping at TLC Direct[41] and Headcovers Unlimited,[42] two websites that specialize in hats for chemotherapy patients, their shopping history may reveal their health status. In addition, so-called non-sensitive information can be used for purposes that are quite sensitive.[43] And, sensitivity is highly subjective; different individuals are likely to perceive the sensitivity of different pieces of personal information differently. For these reasons, any line drawing around sensitivity is inherently arbitrary. Therefore, at a minimum, the sensitive/non-sensitive distinction must be removed from TEDE Part AA.

Moreover, even within its own terms, TEDE Part AA's sensitive personal information definition is particularly ill-suited to the current moment. While it recognizes "racial or ethnic origin, citizenship or immigration status, religious" beliefs, as well as "personal information concerning a consumer's sex life or sexual orientation"[44] as sensitive, it does not acknowledge anything about gender identity or transgender status as sensitive, notwithstanding that, along with immigrants, transgender people are perhaps among the most vulnerable in Donald Trump's America.[45]

---

[40] *E.g.* social security, driver's license, or passport number, geolocation, and biometric data.
[41] TLC DIRECT, https://www.tlcdirect.org (last visited Nov. 2, 2018).
[42] HEADCOVERS UNLIMITED, https://www.headcovers.com (last visited Nov. 2, 2018).
[43] *E.g. supra I.*
[44] A.10008/S.9008 Part AA § 2, 2025-2026 Reg. Sess. (NY 2026).
[45] From the first days of his administration, Trump has engaged in a concerted effort to eliminate access to gender-affirming care, culminating in the proposed rules to prohibit federal Medicaid coverage for gender-affirming care for young people, Medicaid Program; Prohibition on Federal Medicaid and Children's Health Insurance Program Funding for Sex-Rejecting Procedures Furnished to Children, 90 Fed. Reg. 242 (proposed Dec. 19, 2025) (to be codified at 42 CFR 441 and 457), and prohibit general hospitals that provide gender-affirming care to young people from receiving federal Medicare and Medicaid dollars. Medicare and Medicaid Programs; Hospital Condition of Participation: Prohibiting Sex-Rejecting Procedures for Children, 90 Fed. Reg. 242 (proposed Dec. 19, 2025) (to be codified at 42 CFR 482). In the first days of his administration, Trump issued an executive order (EO) purporting to redefine "sex" for federal purposes based on ideas that sex is only male or female, cannot be changed, and is based solely on reproductive cells at conception. Exc. Order No. 14168, 90 Fed. Reg. 8615 – 18 (Jan. 30, 2025). He then issued a second EO explicitly targeting health care for transgender young people, and, among other provisions, instructing the federal Department of Health and Human Services to change Medicare and Medicaid conditions of participation or conditions for coverage with the aim of making it impossible for participating providers to deliver gender-affirming care. Exc. Order No. 14187, 90 Fed. Reg. 8771 – 73 (Feb. 3, 2025). To be clear, these orders are, for the most part, not enforceable on their face. *See e.g.* Letter from Letitia James, N.Y. Attorney General, to Colleague (Feb. 3, 2025) (https://ag.ny.gov/sites/default/files/letters/ag-james-to-hc-providers-re-tro-letter-2025.pdf). But, the Trump administration has continued its relentless attacks on transgender people and the health care providers who take care of them: it launched a tipline, *see* Christopher Wiggins, *Doctors warn of*

Similarly, in its substantive provisions, the bill includes special safeguards from disclosure to law enforcement for reproductive health information[46] but contains no such protections for gender-affirming care information. This is at best an oversight and at worst a stigmatizing refusal to meet the current moment. It is also diametrically opposed to the effort to align New York's reproductive health care and gender-affirming care shield laws that the legislature undertook last year.

2. TEDE Part AA Undermines Itself by Including Substantive Protections Within Its Definitions Section

TEDE Part AA attempts to govern the relationship between data brokers and their service providers and contractors by providing, within the definitions section of the proposal, provisions the Part's drafters expect to see in contracts between these entities. However, if a service provider or contractor wishes not to be covered by this legislation, all it needs to do is write a contract with a data broker that is materially different from the definition's requirements. Because these requirements are included within the definitions and not within the substantive law, there is no penalty for writing a contract that does not include them, and if an entity were to do so, it would effectively write itself out of the proposal's (meager) requirements.

'terrifying' effects as Trump creates snitch line to report gender-affirming care patients, THE ADVOCATE, April 17, 2025, https://www.yahoo.com/news/doctors-warn-terrifying-consequences-trump-004626861.html, and issued whistleblower guidance, U.S. Dep't of Health & Human Services, Guidance for Whistleblowers on the Chemical and Surgical Mutilation of Children (Apr. 14, 2025), inviting health care workers, clinic staff, and others to report gender-affirming care providers and patients to the federal government. U.S. Attorney General Bondi issued a memo prohibiting the federal government from relying on the World Professional Health Association for Transgender Health's Standards of Care 8 and directing the federal Department of Justice to conduct Food, Drug, and Cosmetic Act and False Claims Act investigations of puberty blocker and hormone manufacturers and distributors and health care providers delivering gender-affirming care. Memorandum for Select Component Heads from the Attorney General (April 22, 2025) (https://www.justice.gov/ag/media/1402396/dl). In June, the Federal Trade Commission took up the mantal, hosting a workshop on "Unfair or Deceptive Trade Practices in 'Gender-Affirming Care' for Minors." Press Release, Federal Trade Commission, FTC Announces Workshop on Exploring Unfair or Deceptive Trade Practices in "Gender-Affirming Care" for Minors (June 9, 2025) (https://www.ftc.gov/news-events/news/press-releases/2025/06/ftc-announces-workshop-exploring-unfair-or-deceptive-trade-practices-gender-affirming-care-minors). And this past summer, the federal Justice Department began to issue subpoenas demanding confidential patient information from doctors and hospitals that provide gender-affirming care to young people. Azeen Ghorayshi & Glenn Thrush, *Justice Dept. Demands Patient Details From Trans Medicine Providers*, NYTIMES, July 10, 2025, https://www.nytimes.com/2025/07/10/health/transgender-medicine-minors-trump-subpoena.html. We understand that these subpoenas have been targeted to access states and that some New York providers have received subpoenas.

[46] "(4) for the purposes of this subparagraph, a consumer accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services, shall not constitute a natural person being at risk or danger of death or serious physical injury." A.10008/S.9008 Part AA § 2, 2025-2026 Reg. Sess. (NY 2026).

3. TEDE Part AA Contains Problematic HIPAA Exemptions

In addition to the proposal's exemptions from its deletion requirement, TEDE Part AA also includes seven exemptions from the full scope of the legislation. Most of these exemptions are for protected health information covered by the federal Health Insurance Portability and Accountability Act (HIPAA), HIPAA covered entities, and business associates under HIPAA. The business associate exemption, as well as the exemptions for information de-identified under HIPAA's de-identification standard, are misplaced.

HIPAA protects highly sensitive information, namely personally identifiable information generated in health care settings, as well as health care billing information.[47] However, once HIPAA-protected information is de-identified, HIPAA no longer applies,[48] and business associates may use it freely unless contractually prohibited from doing so,[49] and most do.[50]

It is trivial to re-identify data that has been de-identified using HIPAA's de-identification standard. For example, Dr. Latanya Sweeney,[51] a professor at Harvard and the preeminent researcher on re-identifying de-identified data, has conducted studies in Washington,[52] Maine, and Vermont[53] to re-identify health information that has been de-identified using HIPAA's de-identification standard by linking news stories to de-identified patient data. Her team found that 28.3 percent of names from Maine news stories and 34 percent of names from Vermont news stories uniquely matched to one hospitalization in the Maine and Vermont hospital data, meaning that when de-identified to the HIPAA Safe Harbor standard, the Maine data allowed for a 3.2 percent re-identification rate and Vermont data allowed for a 10.6 percent re-identification rate.[54] In Washington, newspaper stories about hospital visits led to identifying

---

[47] *See generally The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, Sept. 27, 2024, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
[48] *May a health information organization (HIO), acting as a business associate of a HIPAA covered entity, de-identify information and then use it for its own purposes?*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/faq/544/may-a-health-information-organization-de-identify-information/index.html.
[49] *See generally* Kenneth D. Mandl & Eric D. Perakslis, *HIPAA and the Leak of "Deidentified" EHR Data*, 384 New England J. of Med. 2171 (2021); Katharine Miller, *De-Identifying Medical Patient Data Doesn't Protect Our Privacy*, STANFORD UNIV. HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, July 19, 2021, https://hai.stanford.edu/news/de-identifying-medical-patient-data-doesnt-protect-our-privacy.
[50] *See* Katie Palmer, *'Some very noble, some less than noble': The growing health data marketplace sparks privacy concerns*, STAT, June 9, 2021, https://www.statnews.com/2021/06/09/datavant-ciox-health-data-hipaa/.
[51] *Latanya Sweeney*, HARVARD KENNEDY SCHOOL FACULTY PROFILES, https://www.hks.harvard.edu/faculty/latanya-sweeney (last visited Feb. 20, 2026).
[52] Latanya Sweeney, *Only You, Your Doctor, and Many Others May Know*, TECHNOLOGY SCIENCE, Sept. 28, 2015, https://techscience.org/a/2015092903/.
[53] Ji Su Yoo, Alex ra Thaler, Latanya Sweeney, & Jinyan Zang, *Risks to Patient Privacy: A Re-identification of Patients in Maine and Vermont Statewide Hospital Data*, TECHNOLOGY SCIENCE, Oct. 8, 2018, https://techscience.org/a/2018100901/.
[54] *Id*.

the matching health record 43% of the time.[55] In a separate study, she and her team found correct re-identifications for roughly 25% of de-identified records in a subset of a HIPAA-compliant environmental health dataset.[56]

Given that data brokers can be business associates and given the relative ease of re-identifying information de-identified according to HIPAA's de-identification standard, particularly by entities, like data brokers, with access to large data sets, exemptions for business associates and for information de-identified under HIPAA's standard are inappropriate in any consumer privacy statute, particularly one that purports to govern data brokers.

4. A Drafting Error in the Exceptions Will Lead to Confusion

TEDE Part AA's exceptions from the deletion requirement (proposed §1804(4)) dictate that a data broker is not required to delete personal information "if either of the following apply."[57] Paragraph (a) then begins "if it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to" and a laundry list of thirteen exemptions follows.[58] Paragraph (b), which appears to be the other "of the following" reads "personal information described in this subdivision shall only be used for the purposes described in this subdivision and shall not be used or disclosed for any other purpose, including, but not limited to, marketing purposes." This text is nonsensical as an independent rationale to maintain personal information in the face of a deletion request.

5. TEDE Part AA Sidelines the Agency With Privacy Expertise

Surprisingly, TEDE Part AA grants most of its regulatory and oversight authority to the Department of Financial Services rather than the Attorney General's Office when the latter has deep privacy expertise and more frequently oversees and implements privacy-protective legislation.

Because TEDE Part AA is so poorly drafted and because it will give individuals a false sense of security while doing nothing to protect privacy, **the legislature should omit TEDE Part AA from the FY2027 budget**. If the legislature feels compelled to include a section on data brokers, it can consider including a simple data broker registry – this would provide much needed transparency into an opaque industry and allow the legislature time to develop appropriate language that actually protects privacy during the regular legislative session.

*****

[55] Latanya Sweeney, *Only You, Your Doctor, and Many Others May Know*, TECHNOLOGY SCIENCE, Sept. 28, 2015, https://techscience.org/a/2015092903/.
[56] Latanya Sweeney, Ji Su Yoo, Laura Perovich, Katherine E. Boronow, Phil Brown, & Julia Green Brody, *Re-identification Risks in HIPAA Safe Harbor Data: A study of data from one environmental health study*, TECHNOLOGY SCIENCE, Aug. 27, 2017, https://techscience.org/a/2017082801/.
[57] A.10008/S.9008 Part AA § 2, 2025-2026 Reg. Sess. (NY 2026).
[58] *See supra* III(A).

The NYCLU thanks the legislature for the opportunity to provide testimony and for your work on the budget and stands ready to assist legislators to develop and advance meaningful privacy protections during the regular legislative session.