ACLU of New York

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

2023 – 2024 Legislative Memorandum

Subject: **S.365-A (Thomas) / A.7423 (Rozic) – The "New York Privacy Act"**

Position: **OPPOSE**

The ACLU of New York **OPPOSES S.365 / A.7423**, misleadingly titled the "New York Privacy Act" (NYPA). The NYPA is a gift, pure and simple, to the surveillance capitalism industry. It will do little to curb current data collection and monetization practices, less to deter future privacy abuses, and almost nothing to protect the rights of the *actual people* whose intimate details and personal autonomy are commoditized in growingly invasive and inscrutable ways in the largely unregulated data economy.

To our knowledge, **no** consumer protection, civil rights, or privacy organization supports this bill, and with good reason. We review in the following pages the NYPA's worst features, with particular focus on the bill's eleventh-hour, industry-friendly amendments, including the removal of the private right of action, but our review is by no means a *complete* assessment of the bill's flaws. That in mind, we urge legislators and staff to contact the ACLU of New York for additional—including technical—details about our concerns, and, ultimately, to reject this bill.

The NYPA's Opt-Out Consent Model

The New York Privacy Act incorporates an "opt-out" consent model for most data processing, meaning that by default, a person's consent to private data collection and sale is *assumed* unless they affirmatively "opt out." This default consent status matters a great deal, as it dictates much of what companies can do next, and it usually doesn't change, as most people take their accounts, devices, and apps as they come—never bothering to fiddle with privacy settings. This is especially true for busy professionals, poor people working multiple jobs, multitasking parents, minors and seniors who might not be digitally savvy, non-English speakers, people who access the internet solely via phone, and, frankly, anybody with better things to do than worry about whether they've correctly configured their privacy settings.

Companies that monetize our data know this, so they *prefer* opt-out consent and strive to make opting out more difficult than it should be. That strategy shows in everything from incomprehensible privacy policies that make it impossible to

understand one's rights, to websites and apps that are designed to make opting out so complicated and frustrating that users simply give up. And the payoff is real: significantly more data are collected and processed under "opt-out" regimes than "opt-in" models,[1] which—by contrast—allow people to affirmatively share their data with only the companies they choose. But that doesn't mean that an opt-in model doesn't work for companies. On the contrary, because companies want access to our data, just as they are incentivized to make opting-out hard, they would be equally incentivized to make opting-in easy.

Categorizing Data as "Sensitive" or "Non-Sensitive" is Unworkable and Actually *Hurts* Privacy

The NYPA would categorize personal data as either "sensitive" or "non-sensitive" and adjust its protections accordingly. Sensitive data—defined as data that can ***reveal*** information like race, ethnicity, sexual orientation, immigration status, biometric information, precise geolocation data, or certain identification or account numbers[2]— would, at least at first glance, receive greater protection than their "non-sensitive" counterpart.

However, "sensitive" / "non-sensitive" is a distinction without a difference, and protecting one category of data to a greater degree than the other offers consumers only a false sense of security. This is because seemingly innocuous "non-sensitive" data like shopping trends or browser history can, with only minimal processing, reveal medical conditions, ethnicity, religious beliefs, sexual orientation, immigration status, and other data deemed "sensitive". But, it is unclear whether the bill's definition is meant to cover this sort of processing or whether the bill is only interested in protecting data that directly reveals the requisite information on its face.

Moreover, enshrining into law *some* categories of "sensitive" data forecloses—or at least complicates—adding new ones when developing technology, economic trends, or cultural conditions require. It also discounts the subjective nature of the word "sensitive." Some people might consider their sexual orientation sensitive, while others may not care who knows about their romantic tendencies. Some people might proudly wear the scars of a cancer battle as a sign of resilience and survival; others might not be so comfortable revealing such a traumatic piece of medical history to every website they ever visit. And, critically, some people might change their minds about what they consider "sensitive" as politics change. A person who previously didn't care about revealing their reproductive history or location data might reconsider such openness if the two combined might land that person in prison.

---

[1] Lena V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PRO PUBLICA, July 27, 2016, https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world.

[2] The NYPA's full list of sensitive data: (a) racial or ethnic origin, religious beliefs, mental or physical health conditions or diagnoses, sexual activities or orientation, or citizenship or immigration status; (b) genetic or biometric information for the purpose of uniquely identifying a natural person; (c) precise geolocation data; or (d) social security numbers, financial account numbers, passport numbers, or driver's license numbers.

Including a sensitive/non-sensitive distinction also introduces unnecessary legal infirmities into the bill, because such a distinction is definitionally content-based.[3]

The NYPA is Riddled with Loopholes and Exceptions that Render it Toothless

Compliance with Other Laws and Government Requests

None of the NYPA's data processing—including sharing—obligations apply if data processing: (a) is required by law; (b) is "made pursuant to a request by a federal, state, or local government or government entity"; or (c) "significantly advances protection against criminal or tortious activity."[4] But several critical terms from that section are undefined. Taking them one at a time:

(a) "Required by law" – What laws? Laws that criminalize abortion or prohibit gender-affirming care? Laws from jurisdictions that lack suitable privacy protections? The stakes are too high for this to be left to interpretation.

(b) "Made pursuant to a request by federal, state, or local government or government entity" – Again, which governments? Which states? States that will combine protected health information and precise geolocation data in order to imprison people who travel to New York to obtain abortion care? **Would this clause require entities covered by the NYPA to turn information over to any government that asks, without a warrant or any sort of legal protections?**

(c) "Significantly advance[] protection against criminal or tortious activity." – *Once again*, could a company bound by NYPA claim an exception from the law's processing requirements on the basis that processing "significantly protects" them, the person to whom the data pertains, or some third party—the wording isn't clear—from criminal or tortious activity?

If the NYPA's protections collapse like a house of cards under the weight of a simple request from any government anywhere, or that of a company's own subjective determination that disregarding the law "advances protection against criminal or tortious activity," NYPA is completely, utterly useless.

A "Free Speech" Exception

The NYPA would exempt a company from most processing requirements if doing so would impair the "rights of another to exercise free speech."[5] However, courts are increasingly finding that both targeted advertising and delivering search results—

---

3 *See Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011).

4 §1103(4)(b)-(c)

5 §1105(4)(c)

along with anything done by algorithm—*are* protected speech.[6] Thus, the NYPA would seem to exempt from many of its requirements any company who can convincingly argue the bill's obligations impair its own speech, or the data collection and processing activities of other companies with whom it shares data.

Publicly Available

NYPA's recent amendments changed the definition of "personal data" to *exclude* "information that is lawfully made publicly available from federal, state or local government records, or information that a controller has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media."[7] This ambiguous, sprawling carveout will allow companies to scrape and monetize information from all kinds of repositories, including government databases, subscription-based or paywalled research services, and other sources that—even if technically "public"—would take an ordinary person years to scan and lifetimes to process.

The NYPA Does Not Have an Effective Enforcement Mechanism

Rights exist only in their enforcement. And with no private suits allowed, enforcing NYPA would fall exclusively to the Attorney General, whose office lacks the resources to investigate all but the most egregious violations and outrageous practices. If those practical limitations constrain the AG to target only larger companies whose actions hurt more people, smaller entities who violate the privacy of just a few individuals or just one particular community—perhaps an event space that spies on concertgoers' cellphones or a landlord who uses biased tenant-screening software to discriminate against potential renters—will too often fly under the radar, leaving their victims without a remedy. Allowing victims of data abuse to sue in civil court would fill this enforcement gap, and, when coupled with mandatory attorney's fees, statutory damages, and the ability to proceed as a class, would elevate New Yorkers to near-equal footing with Big Data and give them a powerful tool to bring both transparency and accountability to the data economy.

Indeed, the Attorney General of California stated as much in a 2018 letter to California legislative leaders when the state was considering the CA Consumer

---

[6] *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").

[7] §1100(17)

Privacy Act. Entreating lawmakers to consider his office's limited resources, Attorney General Becerra wrote,

> [T]he CCPA does not include a private right of action that would allow consumer to seek legal remedies for themselves to protect their privacy. . . . **The lack of a private right of action**, which would provide a critical adjunct to governmental enforcement, **will substantially increase the AGO's need for new enforcement resources**. I urge you to provide consumer with a private right of action under the CCPA. [Emphasis added.][8]

Notably, this session's first iteration of the NYPA included a limited private right of action, but in a sublime act of generosity to the surveillance capitalism industry, the private right was removed from the bill at the eleventh hour.

Indeed, the NYPA seems designed to permit companies to avoid any *public* accountability for their data practices. While the bill does require companies, at least in some circumstances, to undertake data protection assessments, these assessments are explicitly kept secret and only made available to the Attorney General upon request in the context of an investigation – and when they are turned over to the Attorney General, they are explicitly exempt the Freedom of Information Act.[9] As explained above, because investigations are resource-intensive, they will rarely occur. Moreover, the bill's provisions make it impossible for watchdog groups, security researchers, individuals, or advocates to ever know what is included in a data protection assessment or to ring alarm bells if the assessments demonstrate that personal data are being misused or abused.

By contrast, while the NYPA takes pains to shield companies from oversight, it gives the Attorney General unfettered ability to receive information from consumer protection and privacy advocates and researchers, internet-standards setting bodies, and other relevant sources upon request and without legal process to inform its rulemaking.[10]

The NYPA Will Undermine Healthcare Privacy, Including that of Reproductive and Gender-Affirming Care

Consumer privacy takes on new salience in a post-*Roe v. Wade* world where abortion is health care in New York and a crime in other states and as states rush to criminalize gender-affirming care.[11] It is impossible to have an abortion—or seek

---

[8] https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/08/ag-becerras-letter-re-california-consumer-privacy-act.pdf. Document also on file with NYCLU.

[9] §1103(1)

[10] §1107

[11] In the wake of the *Dobbs* decision, nearly half the states are poised to completely ban abortion – and many already have. *See generally Interactive Map: US Abortion Policies and Access After Roe*, GUTTMACHER INSTITUTE, May 22, 2023, https://states.guttmacher.org/policies/; *After Roe Fell: Abortion Laws by State*, CENTER FOR REPRODUCTIVE RIGHTS, https://reproductiverights.org/maps/abortion-laws-by-state/ (last visited May 24, 2023).

many other types of health care—without leaving a digital trail. New York took important first steps toward protecting New Yorkers' electronic health data in Part U of the FY2024 Health and Mental Hygiene (HMH) Article VII legislation.[12] But New York cannot bind other states' law enforcement, nor can it prevent a hostile state from obtaining New Yorkers' health data from a company's offices in that hostile state without ever setting foot in New York or going before a New York court.

The NYPA will do nothing to mitigate these risks. While it does require opt-in consent for processing of health information, once that consent is obtained, it lasts forever, and even if a person deletes their account—probably the last thing on someone's mind during a health crisis—NYPA requires companies to delete only that information "directly related"[13] to the account; the company can maintain any inferences made or information derived from that health data. This matters because once a person opts-in, companies will be able to sell that health data to out-of-state entities, ***including out-of-state law enforcement***, and companies will turn the data over to law enforcement in hostile states pursuant to legal process there.

Lastly, and as discussed above, while the definition of sensitive information subject to opt-in protections includes information that "reveals" health status, it is not clear how tight a nexus is required here—i.e., what is meant by "*reveal*." For example, as long ago as 2012, retail giant Target was using shoppers' purchasing habits to identify when they were pregnant—often before shoppers themselves knew.[14] Is shopping history in this context "sensitive information" or is the revelation of pregnancy status too attenuated?[15] If it is not sensitive information—or if health information can be ascertained through the bill's other gaping exceptions and loopholes—then companies will be able to pool and share individuals' electronic health data without even the minimal protection opt-in consent offers.

The NYPA's Eleventh-Hour Amendments *Removed* Automated Decisionmaking Protections

Both the government and private enterprise increasingly rely on automated decision-making systems that use complicated software algorithms to determine New Yorkers' eligibility for certain programs or benefits, like loans, credit, and housing.

Similarly, seventeen bills to ban gender affirming care have become law in states across the country. *See generally Mapping Attacks on LGBTQ Rights in U.S. State Legislatures*, ACLU, May 19, 2023, https://www.aclu.org/legislative-attacks-on-lgbtq-rights.

[12] HMH Part U limits when electronic service providers headquartered or incorporated in New York can respond to out-of-state warrants for reproductive health information; prohibits New York law enforcement from buying any electronic health data; and requires New York law enforcement to get a warrant if they want to obtain electronic health data. A.3007-C/S.4007-C Part U, 2023-2024 Reg. Sess. (N.Y. 2023).

[13] To make matters worse, NYPA does not define "directly related."

[14] Charles Duhigg, *How Companies Learn Your Secrets*, NY TIMES, Feb. 16, 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[15] And how is a company Target's size supposed to determine, while processing the data of tens of thousands of New Yorkers in real time, what non-sensitive data will, when processed, lead to "sensitive" conclusions that need to be treated differently or walled off altogether? The answer to this question is critically important, as mistakes here ***will*** land people in prison in other states.

These systems are notoriously prone to racial bias and other flaws that lead to inaccurate and potentially discriminatory results, and the underlying code is usually a closely guarded secret. The previous version of the NYPA included protections against discriminatory automated decisionmaking systems, but those protections were removed from the current print.

No Government Guardrails

The New York Privacy Act would not apply to the government *at all*, even though government institutions process New Yorkers' personal data and use complicated algorithms to make automated decisions about our rights and freedoms on a growing basis.

What's more, many of NYPA provisions we've discussed above allow the government to demand data from entities who process it, but remain silent on what happens to the data afterward. May the government keep it indefinitely and share it as it pleases? This, too, is a glaring omission that renders NYPA's privacy protections weak at best, and harmful at worst.

***

The New York Privacy Act is a boon to industry that would allow the most voracious members of the data economy to continue current practices undeterred and shrouded in secrecy, without meaningful safeguards to protect the very real people whose privacy and personal autonomy will suffer as a result. The ACLU of New York urges legislators to reject it.