# NYCLU
## ACLU of New York

## 2023 – 2024 Legislative Memorandum

**Subject:**    **Digital Fairness Act**
          **A.3308 (Cruz) / S.2277 (Kavanagh)**

**Position:**  **SUPPORT**

---

It is no longer possible to participate meaningfully in society without providing personal information to private companies that may reveal the intimate details of our lives, whether by itself or when combined with other data. And, as other states move to ban abortion[1] and gender-affirming care[2] – and to use personal information private companies harvest to prosecute people for seeking, providing, or helping others to obtain such care[3] – the stakes have gotten higher.

The consequences of the use and abuse of personal information can be profound. As long ago as 2012, Target was using shoppers' purchasing habits to identify when they were pregnant – often before they themselves knew.[4] Precisely-targeted pricing, advertising, and other automated decision tools are used to exclude people of color, women, and older individuals from housing, credit, and employment opportunities in ways that would be unthinkable in the offline world.[5] During the 2016 election, personal information was used to target advertisements to Black Americans urging them not to vote.[6] Indeed, privacy violations can

---

[1] *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)

[2] *See generally* Mapping Attacks on LGBTQ Rights in U.S. State Legislatures, ACLU, June 23, 2023, https://www.aclu.org/legislative-attacks-on-lgbtq-rights.

[3] *E.g.* Josh Funk, *Nebraska woman charged with helping teenage daughter have abortion*, AP, Aug. 9, 2022, https://www.pbs.org/newshour/health/nebraska-woman-charged-with-helping-daughter-have-abortion#:~:text=OMAHA%20(AP)%20%E2%80%94%20A%20Nebraska,to%20burn%20the%20fetus%20afterward.

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

[5] *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.

[6] 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.

lead to a range of harms, from monetary losses to harassment to public exposure of our intimate lives to reputational damage. Misuse and abuse of personal information in the digital age can limit awareness of and access to opportunities, exacerbate information disparities, erode public trust and free expression, and disincentivize individuals from participating fully in digital life.[7]

In government hands, automated decision systems increasingly determine everything from teacher evaluations and child custody to sentencing, probation, and parole – and more. Computer-generated decisions have the veneer of objectivity, but these systems are built on human inputs, and they produce biased results. Automated decision systems all too often replicate and amplify harm towards people who already face bias and discrimination.

The Digital Fairness Act, A.3308 (Cruz)/S.2277 (Kavanagh), will tackle the worst harms of the digital age by protecting privacy and addressing the civil rights abuses associated with misuse and abuse of personal information holistically in the same bill. **The NYCLU strongly supports this legislation and urges its immediate passage.**

People often do not know or consent to the ways companies collect, use, retain, share, and monetize our personal information – in fact, Carnegie Mellon researchers found that it would take 76 workdays to read all of the privacy policies one encounters in a year.[8] And, yet privacy remains popular in New York and across the country. Ninety-two percent of Facebook users alter the social network's default privacy settings,[9] demonstrating that they wish to choose with whom they share personal information. Similarly, ninety-two percent of people in the United States believe companies should obtain their permission before sharing or selling their personal information.[10]

The Digital Fairness Act will put control back in peoples' hands by requiring meaningful notice and affirmative, opt-in consent from people before their personal information is captured or used, as well as heightened protections for biometric information like fingerprints and face data – because such information is impossible to change. The bill also prohibits surreptitious surveillance by consumer products and provides people with the ability to access and delete their personal information and to transfer their personal information to another company.

Importantly, the Digital Fairness Act operates on an opt-in model, which means that companies must have individuals' affirmative consent before they collect or use their personal information. This puts the incentives in the right place. Companies want people to share their personal information, which means they are incentivized to make opting in easy and opting

---

[7] *Id.*

[8] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[9] 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/.

[10] 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).

out hard. Instead of burying individuals' options in legal jargon and complex terms and conditions, an opt-in regime will condition companies to appeal to and earn the trust of the people whose information they want to collect and use. An opt-in – or privacy-by-default – model is particularly important for people who do not have the time or knowledge to navigate opt-out options. This disproportionately includes the elderly, the disabled, and those for whom English is not a first language, as well as economically disadvantaged individuals.

In addition, recognizing the fundamental information asymmetry between companies and individuals, the Digital Fairness Act will require companies collecting intimate information and benefiting from specialized knowledge to undertake obligations similar to those required of banks, lawyers, and medical providers.

Importantly, the bill includes an enforcement mechanism that will incentivize companies to comply – individuals can sue when their rights are violated, and the state Attorney General and district attorneys or city attorneys in cities with more than 750,000 residents may also enforce.

Moreover, the Digital Fairness Act will address many of the tangible harms that arise from the abuse and misuse of personal information in the digital age by making clear that it is both unlawful discrimination and an unfair trade practice to use personal information to circumvent our civil and human rights laws.

In addition, it provides guardrails for government use of automated decision systems. It bans discriminatory tools and requires that any governmental automated decision system undergo and pass a civil rights audit conducted by a neutral third party before it is deployed. It also requires that individuals subjected to government automated decisions receive notice of the decision made, the involvement of an automated system, and an opportunity to contest the decision and seek human review. And, the bill requires government entities that use automated decision-making systems to have appropriate governing policies in place, adhere to transparency requirements, and have the approval of the relevant governing body, following a public hearing, before acquiring any new systems.

Finally, the Digital Fairness Act requires digital literacy and digital privacy education in K-12 public and charter schools to help young New Yorkers identify online fraud, as well as reliable sources and information, and to enable them to better understand how online activities are tracked and recorded, where personal information posted online may go, with whom it may be shared, how it may be used, and how best to protect digital security and digital privacy. This education will help students learn how to protect their privacy and how to identify, assess, and evaluate information they see online – including the misinformation and "fake news" that proliferate in digital spaces.

The Digital Fairness Act is not only crafted to address the actual harms that arise from abuse and misuse of personal information in the digital age, but it is carefully designed to withstand First Amendment scrutiny[11] – a pitfall that too many other privacy bills fall into.

The NYCLU urges legislators to pass the Digital Fairness Act, A.3308/S.2277, immediately – for the good of civil liberties and civil rights. The stakes are critically high. The use and misuse of our personal information online shapes the world we live in, the opportunities we get, the information we see, and the choices we can make. The Digital Fairness Act will ensure that cutting edge technology can no longer be used to circumvent our civil and human rights laws.

---

[11] *See generally Sorrell v. IMS Health*, 564 U.S. 552, 562 – 65 (2011); Allie Bohm, Policy Counsel, NYCLU, Protecting Consumer Data and Privacy on Online Platforms, Testimony before the New York State Senate Committee on Consumer Protection and the New York State Senate Committee on Internet and Technology (Nov. 22, 2019); Allie Bohm, Policy Counsel, NYCLU, A Joint Public Hearing to Conduct Discussion on Online Privacy and What Role the State Legislature Should Play in Overseeing It, Testimony before the New York State Senate Committee on Consumer Protection and the New York State Senate Committee on Internet and Technology (June 4, 2019).