February 12, 2021

The Honorable Andrew M. Cuomo
Governor of New York State
633 3rd Ave, 38th Floor
New York, NY 10017

Re: Opposition to Parts II and JJ of the FY22 Public Protection and General Government Budget Legislation

Dear Governor Cuomo,

The undersigned privacy, consumer protection, civil rights, and civil liberties groups write in strong opposition to Parts II and JJ of the FY22 Public Protection and General Government (PPGG) Article VII bill. We urge you to remove these sections from the final budget legislation. These provisions purport to protect individual privacy, but in effect would put a legal imprimatur on companies' current practices of collecting, using, and monetizing individuals' personal information in ways that New Yorkers do not understand and would be unlikely to agree to if they did understand. This letter offers our understanding of the problems any comprehensive privacy legislation must tackle and outlines how this budget proposal falls well short of addressing these concerns.

Background

It is no longer possible to participate in society without providing personal information to private companies and other third parties that may itself, or when combined with other data, reveal the intimate details of our lives. This was true even before the pandemic, but, as COVID-19 has forced much of life – from school to work to doctor's visits to grocery shopping to time with loved ones – online, private companies have been able to amass even more information about each of us. The consequences for our privacy – and our civil rights – can be profound. For example, personal information has been leveraged to ensure that only younger men see certain job postings and to exclude Black people from viewing certain housing advertisements. During the 2016 election, personal information was used to target advertisements to Black Americans urging them not to vote.[1] As the *New York Times* observed, exploitation of personal information enables "unequal consumer treatment, financial fraud, identity theft, manipulative marketing, and discrimination."[2]

Privacy legislation is complex, and it is too important to get wrong. It should not be rushed through in the context of the budget, but rather, it should be carefully crafted over time to ensure that it actually addresses the most pernicious harms associated with use and abuse of personal information in the digital age.

To start, any comprehensive legislation must account for the extreme power disparity between the companies operating in the digital ecosystem and individuals as well as the discriminatory impacts of this opaque system. Legislation must actually protect individuals by regulating the real-world ways in which our privacy and equality are undermined. That means 1) covering of all the ways that companies

[1] 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.
[2] *Id*.

process and monetize our personal information, even when that information does not change hands, 2) empowering individuals to choose how their personal information is used, and 3) ensuring that covered entities cannot use amassed personal information to circumvent our civil rights laws. The sections that follow will describe the ways in which Parts II and JJ of the FY22 PPGG bill are wholly inadequate to these tasks.

Part II of PPGG applies too narrowly

The proposed legislation purports to protect "consumers," which it defines as "identified or identifiable natural person[s]."[3] "Identified or identifiable natural person," in turn, is defined "by reference to specific information," like a name, identification number, geolocation data, or an online identifier.[4] This is true despite the fact that an entity need not know an individual's name, identification number, online handle, or location to very effectively leverage that person's personal information against them or to discriminate against them. For example, if the entity – or its advertising algorithm – knows that a cluster of characteristics pertaining to an individual indicate that that individual is more likely to be female, it may not show that individual a senior management job posting or an advertisement for an engineering position.[5] Whether or not the entity knows the individual's name, identification number, or similar piece of information is irrelevant for the individual's experience, but if the entity does not have that information, the individual is completely unprotected by this legislation.

In addition, although it can be easy to re-identify de-identified information,[6] the proposal includes a definition of "de-identified" that would not protect against re-identification.[7] It then exempts "de-identified" information from the bill's obligations, permitting unfettered use and abuse of information that could easily be connected to a specific individual and used to ascertain the intimate details of that person's life.

Furthermore, the proposal broadly carves out every aspect of personal information collection in the employment context.[8]

---

[3] FY 2022 New York State Executive Budget Public Protection & General Government Article VII Legislation, Part II § 2, 2021-2022 Reg. Sess. (N.Y. 2021).

[4] *Id*.

[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; Leigh Freund, President and CEO, Network Advertising Initiative, Competition and Consumer Protection Issues in Online Advertising, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018) (testifying that "women are less likely to see employment ads for careers in the science/technology/engineering/math field . . . simply because they have higher value to other advertisers because women do more shopping.").

[6] *See generally* BEN GREEN, GABE CUNNINGHAM, ARIEL EKBLAW, PAUL KOMINERS, ANDREW LINZER, & SUSAN CRAWFORD, OPEN DATA PRIVACY: A RISK-BENEFIT, PROCESS-ORIENTED APPROACH TO SHARING AND PROTECTING MUNICIPAL DATA (Berkman Klein Center 2017) ("Traditional privacy and anonymization frameworks focus on identifying and removing personally identifiable information (PII). Recent research, however, has revealed that this framework is unsustainable and ineffective. Because so much data is now available from a wide variety of sources, and because databases can be manipulated and combined in complex and unpredictable ways, information that might not be deemed PII can lead to the identification of a specific individual and enable inferences to be made about that individual").

[7] FY 2022 New York State Executive Budget Public Protection & General Government Article VII Legislation, Part II § 2, 2021-2022 Reg. Sess. (N.Y. 2021).

[8] *Id*.

Part II is drafted to undermine the protections it purports to provide

Although the proposal purports to limit covered entities from using or disclosing "personal information for purposes other than those specified" in required disclosures,[9] the legislation then immediately effectively nullifies this purpose limitation by explaining that as long as the entity merely offers individuals the option to opt-out of sale or sharing of personal information and to "limit the use and collection of their personal information," it need not comply with the purpose limitation and can use and collect individuals' personal information for whatever it desires without informing the individual.[10]

While the bill does require covered entities to comply with opt-out requests,[11] it places no limits on coercive site designs that manipulate individuals out of opting out. Moreover, it includes four separate provisions permitting pay-for-privacy or financial incentives for sharing information and/or declining to opt-out. These pay-for-privacy provisions risk making privacy a luxury good, available only to those who can afford to pay for it, further marginalizing the most marginalized, and exacerbating the existing digital divide.[12] Individuals enduring socioeconomic or regional economic disadvantages – including, disproportionately, people of color – already have less privacy; they rely on cheaper, unencrypted cell phones, free email, and other more affordable, but less secure, technology. The digital divide is a privacy divide, and pay-for-privacy would only worsen it.

In fact, an opt-out regime, in and of itself, fails to adequately protect individual privacy, because default is too often destiny. This is particularly true for individuals who do not have the time or knowledge to navigate opt-out options – disproportionately, the elderly, the disabled, and those for whom English is not a first language, as well as economically disadvantaged individuals. Because many individuals never change a site's default settings, significantly more personal information will be processed under an opt-out regime than under an opt-in regime.[13]

Moreover, the opt-out option applies primarily to "sale of personal information."[14] While it is marginally helpful that the budget proposal appears to define "sale" to include sharing of personal information,[15] the focus on sale is woefully too narrow. This is because sale, or even direct sharing of personal information, is not the most frequent way personal information is monetized or used to discriminate against the person to whom it pertains. Many entities guard their troves of personal information and leverage them to sell advertisements: an advertiser approaches the entity with an audience it would like to reach (say, suburban women with children who drive minivans and like the color blue), and the entity uses the personal information it maintains to match the advertisement to the desired audience.[16] The fact that the personal information does not change hands is immaterial for individuals' experiences.

---

[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] Gry Hasselbach & Pernille Tranberg, *Privacy is creating a new digital divide between the rich and poor*, THE DAILY DOT, Oct. 23, 2016, https://www.dailydot.com/layer8/online-privacy-data-ethics/.
[13] 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.
[14] FY 2022 New York State Executive Budget Public Protection & General Government Article VII Legislation, Part II § 2, 2021-2022 Reg. Sess. (N.Y. 2021).
[15] *Id*.
[16] *Id*. Some entities are also set up to find look-alike audiences with similar traits to a pre-populated list an advertiser provides. Some also permit an advertiser to target particular individuals. UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).

They are aware that companies monetize their personal information even if that information is not literally sold. Moreover, this sort of targeting enables the many harms described above.

The other purported individual protections included in the bill are similarly anemic. For example, the bill requires covered entities, upon receipt of a verifiable request, to provide individuals with twelve months of their personally identifiable information "in a form that is readily intelligible to the consumer"[17] free of charge. This may sound generous, but when many individuals have multi-year relationships with covered entities, this would only require the return of a fraction of their personal information. Moreover, while a format that is "readily intelligible to the consumer" may sound good, this is unlikely to be a format that is readily portable to another platform. Allowing individuals to transfer their own information ("portability") is critical to provide individuals with actual choices online and with the power to shift their digital information to another company or service. A lack of portability will entrench the current dominant players in the internet ecosystem and inhibit the rise of new platforms that might be more privacy protective.

Part JJ's confers liability protections on manufacturers without providing any additional protections to individuals

Part JJ requires certain disclosures about the use of voice recognition in consumer products both before the time of sale and during initial set-up.[18] First, it is perplexing that the bill is limited to voice recognition and does not apply to other forms of surreptitious or biometric surveillance, which are equally invasive. Moreover, the bill breaks no new ground in requiring disclosure from companies given that a company that neglects to inform consumers of surreptitious audio recording would run afoul of the Section 5 of the Federal Trade Commission Act's prohibition on deceptive trade practices.[19] But, although it imposes no new requirements on companies, Part JJ confers liability protection on manufacturers of voice recognition devices,[20] which is simply a gift to industry – without giving individuals any more rights or power.

Both Part II and Part JJ lack a meaningful enforcement mechanism

Finally, neither Part II nor Part JJ includes an effective enforcement mechanism. Both sections are enforced by the Secretary of State and neither includes a private right of action. While the state actors should certainly have a role in enforcing any privacy law, government resources are necessarily limited – particularly as the state faces a pandemic-induced budget crunch – and government actors will only be able to enforce in the most egregious cases. A private right of action not only allows individuals to seek redress in cases where the government chooses not to intervene, but the threat of private lawsuits is likely to incentivize companies to adhere to any privacy law and protect individuals' personal information.

---

[17] FY 2022 New York State Executive Budget Public Protection & General Government Article VII Legislation, Part II § 2, 2021-2022 Reg. Sess. (N.Y. 2021).

[18] FY 2022 New York State Executive Budget Public Protection & General Government Article VII Legislation, Part JJ § 1, 2021-2022 Reg. Sess. (N.Y. 2021).

[19] *See* John Riberiro, *Samsung faces complaint in US FTC over Smart TV 'surveillance'*, NETWORK WORLD, Feb. 25, 2015, https://www.networkworld.com/article/2889474/samsung-faces-complaint-in-us-ftc-over-smart-tv-surveillance.html.

[20] FY 2022 New York State Executive Budget Public Protection & General Government Article VII Legislation, Part JJ § 1, 2021-2022 Reg. Sess. (N.Y. 2021).

In addition, the civil penalties available are so low – $7,500 per violation in the case of Part II[21] and $2,500 per violation in the case of JJ[22] – as to be a rounding error for companies. There is no reason to believe they would incentivize companies' compliance with the bill's meager protections.

Conclusion

Each of the signatories to this letter urges you to remove Parts II and JJ from the budget legislation and stands ready to assist in developing thoughtful comprehensive privacy legislation.

Sincerely,

AI Now
BetaNYC
Defending Rights & Dissent
Dutchess County Progressive Action Alliance
Electronic Frontier Foundation
Fight for the Future
Immigrant Defense Project
National Action Network
New York Civil Liberties Union
NYC-DSA Tech Action Working Group
Privacy Rights Clearinghouse
Surveillance Technology Oversight Project
WESPAC Foundation, Inc.

CC. Majority Leader Andrea Stewart Cousins
Speaker Carl Heastie
Senator Liz Krueger, Chair, Senate Committee on Finance
Assembly Member Helene E. Weinstein, Chair, Assembly Committee on Ways and Means

[21] FY 2022 New York State Executive Budget Public Protection & General Government Article VII Legislation, Part II § 2, 2021-2022 Reg. Sess. (N.Y. 2021).
[22] FY 2022 New York State Executive Budget Public Protection & General Government Article VII Legislation, Part JJ § 1, 2021-2022 Reg. Sess. (N.Y. 2021).