UNIVERSITY OF CALIFORNIA, LOS ANGELES **UCLA**

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

DEPARTMENT OF GENDER STUDIES
1120 Rolfe Hall , Box 951504
LOS ANGELES, CALIFORNIA 90095-1504
Phone: (310) 206-8101
Fax: (310) 206-7700
http://www.genderstudies.ucla.edu

TO: New York City Chancellor of the Department of Education,
Chief Privacy Officer of the Department of Education,
General Counsel to the Department of Education,
and members of the Panel of Educational Policy

FROM: UCLA Center on Race and Digital Justice

SUBJECT: In response to the Chancellor's revisions to the A-820 regulations on student privacy

DATE: November 22, 2024

Dear New York City Department of Education Chancellor, Chief Privacy Officer, General Counsel, and members of the Panel of Educational Policy,

I am writing to you in response to revisions to Chancellor's Regulation A-820.[1]

At the Center for Race & Digital Justice, we research and challenge how digital, internet, and AI technologies diminish human possibilities. We advocate for interventions that actualize a just society rooted in the restoration and expansion of civil, sovereign, and human rights. Issues like enforcing people's data rights and the protection of people's data bodies[2] is a major subject in our work.

Given our expertise in the subject, to us it is clear that the revisions to Chancellor's regulations A-820 are insufficient.

Protecting our data rights and data bodies is essential for protecting against harm and supporting human dignity. Research shows the harm of data collection, especially when the data collection is nonconsensual.

[1] Revisions to Chancellor's Regulations A-820 can be found in the PEP - Panel Meeting Schedule under the section entitled "PEP Meeting – November 20, 2024" in the bullet point entitled "Chancellor's Regulation A-820" (website last visited November 14, 2024).

[2] Using the term data bodies from Our Data Bodies, an organization that includes many collaborators. Our Data Bodies explains that "our data bodies are discrete parts of our whole selves that are collected, stored in databases, the cloud, and other spaces of digitally networked flows, and used to make decisions or determinations about us. They are a manifestation of our relationships with our communities and institutions, including institutions of privilege, oppression, and domination." (2018 Our Data Bodies Report, page 24).

This harm can be psychological as well as tangible and material. For example, psychological harms include the emotional toll that comes with data collection – feelings of dehumanization, extraction, alienation, frustration, anger, were key themes from the over 100 in-depth interviews conducted in Our Data Bodies' 2018 research.[3] Continuous levels of monitoring can lead to increased levels of stress and anxiety.[4] Failure to protect our data bodies when our data is sold to data brokers has led to enabling abusive individuals to stalk, harass, and harm people (disproportionately impacting women, people of color, LGBTQ+ people, and children).[5] [6] The psychological impacts of data collection and monitoring can lead to individual behavioral change, creating a chilling effect.[7] [8] These harms not only hurt our individual humanity, but our ability to live in a robust participatory democracy.

Massive data collection and its heedless use has enabled discrimination time and time again. The use of and application of massive amounts of data into algorithms, marketed artificial intelligence ("AI"), and other technological tools for decision making has shown systemic discrimination. Some of the best known examples of this discriminatory effect of data driven technological or algorithmic tools are in the policing space. For example, significant discriminatory impacts can be found in facial recognition[9] [10] [11] [12] when it is employed in policing tools like surveillance cameras, unmanned aerial vehicles, and certain smart equipment; pretrial risk assessment[13]; predictive policing[14] [15]; automated license plate readers[16] [17]; body

[3] 2018 Our Data Bodies Report by Tawana Petty, Meriella Saba, Tamika Lewis, Seeta Peña Gangadharan, Virginia Eubanks (June 15, 2018).
[4] I Spy With My Little Eye by A.J. Marsden, Ph.D., and William Nesbitt, Ph.D. in Psychology Today (November 6, 2017)
[5] 2022 Report to Congress from Office on Violence Against Women's Grant Funds Used to Address Stalking (2022)
[6] People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs by Justin Sherman in Lawfare (Oct. 30, 2023).
[7] Ethical side-effect of dataveillance in advertising: Impact of data collection, trust, privacy concerns and regulatory differences on chilling effects by Joanna Strycharz and Claire M. Segijn, published in Journal of Business Research (February 2024).
[8] How constant surveillance puts protesters at risk - Marketplace Molly Wood interviewing Simone Brown on Marketplace (September 18, 2020).
[9] Gender Shades by Joy Buolamwini, Dr. Timnit Gebru, Dr. Helen Raynham, Deborah Raji, and Ethan Zuckerman from the MIT Media Lab and Civic Media, from the paper "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification."
[10] "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match" by Kashmir Hill reported in the New York Times (December 29, 2020, Updated January 6, 2021).
[11] "Faulty Facial Recognition Led to His Arrest—Now He's Suing" by Natalie O'Neill reported in Vice (September 4, 2020).
[12] Michigan father sues Detroit Police Department for wrongful arrest based on faulty facial recognition technology" press release from American Civil Liberties Union (April 13, 2021).
[13] "Machine Bias" by Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner reported in ProPublica (May 23, 2016).
[14] "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice" by Rashia Richardson, Jason Schultz, and Kate Crawford published in NYU Law Review (February 13, 2019).
[15] "Predictive policing is still racist—whatever data it uses" by Will Douglas Heaven reported in MIT Technology Review (February 5, 2021).
[16] "NYPD Defends Tactics Over Mosque Spying; Records Reveal New Details On Muslim Surveillance" by Adam Goldman and Matt Apuzzo reported in HuffPost via the Associated Press (February 24, 2012).
[17] "San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error" by Kade Crockford in American Civil Liberties Union news and commentary (May 13, 2014).

worn cameras[18] [19]; and electronic shackling[20] [21]; and gunshot detection systems.[22] [23] And these harms – individual and societal harms, psychological and material harms – are not limited to policing. They have crept into our systems for housing[24] [25], loans[26], employment[27], finances[28], immigrant rights[29] [30] [31] [32], healthcare access[33], and more.

Alarmingly, the harms of data collection, sale of data to third party data brokers, and the potential discriminatory impacts of algorithms and AI have also already seeped into our schools.

For example, a report by Center on Democracy and Technology on the 2021-2022 school year[34] showed that monitoring students is more often used for discipline than student safety. It leads to increased risk of student interaction with law enforcement, disproportionately targets and harms students who are LGBTQ+, low-income, Black, and/or Hispanic. The survey conducted for the report showed that 89% of teachers say that their schools monitor student activity when students are on school issued and/or personal devices. Even without third party software as an intermediary, the collection and sharing of data between schools and other government entities can lead to deep harm. For example, investigative reporting and advocacy revealed that in Pasco County, Florida, data sharing between the school district and the local

[18] "Failure to turn on body cameras flouted Minneapolis police policy" by Matt McKinney and Libor Jany reported in Star Tribune (July 18, 2017).

[19] Letter from United States Department of Justice Civil Rights Division to Albuquerque Police Department (April 10, 2014).

[20] Cages Without Bars by the Shriver Center on Poverty Law, Media Justice, and Chicago Appleseed Center for Fair Courts (September 2022).

[21] "Immigration Cyber Prisons: Ending the Use of Electronic Ankle Shackles" by Tosca Giustini, Sarah Greisman, Peter L. Markowitz, Ariel Rosen, and Zachary Ross published in Yeshiva University, Cardozo School of Law Online Publications (July 2021).

[22] "OIG finds that ShotSpotter alerts rarely lead to evidence of a gun-related crime and that presence of the technology changes police behavior" press release from the Chicago Office of Inspector General (August 24, 2021).

[23] "New MPD Point & Aim reports show disparity where officers draw their guns" by Shaun Gallagher reported in WTMJ-TV Milwaukee (November 17, 2021).

[24] "Algorithms Allegedly Penalized Black Renters. The US Government Is Watching" by Khari Johnson, Wired (January 16, 2023).

[25] "We Found That Landlords Could Be Using Algorithms to Fix Rent Prices. Now Lawmakers Want to Make the Practice Illegal" by Heather Vogell, ProPublica (January 30, 2024).

[26] How Some Algorithm Lending Programs Discriminate Against Minorities NPR's Scott Simon speaks with Washington Post columnist Michelle Singletary (November 24, 2018).

[27] Over Two Dozen Labor Unions, Civil Rights Groups, and Public Interest Advocates Endorse New York's BOT Act, press release from Center for Democracy and Technology (May 16, 2024).

[28] Protecting Older Consumers 2023-2024 (A Report of the Federal Trade Commission), Federal Trade Commission (Oct. 18, 2024).

[29] Multiple resources from Just Futures Law from their Fighting Data Brokers page (last visited November. 15, 2024)

[30] Protecting Immigrant Access to Fair Credit Opportunities | Consumer Financial Protection Bureau by Sonia Lin, (Oct. 12, 2023).

[31] The Data Broker Loophole is Being Exploited to Target Immigrant Communities by National Association of Criminal Defense Lawyers (May 22, 2024).

[32] Documents Reveal ICE Using Driver Location Data From Local Police for Deportations by Vasudha Talla of ACLU of Northern California (March 13, 2019)

[33] Data Privacy & Reproductive Freedom: How Digital Surveillance Increases the Risk of Pregnancy Criminalization Post-Dobbs, National Partnership for Women & Families by Ashley Emery of National Partnership for Women & Families (October 2024).

[34] Hidden Harms: The Misleading Promise of Monitoring Students Online by Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, and Hannah Quay-de la Vallee from Center on Democracy and Technology (August 2022).

Sheriff's Office led to the creation of a secret list of over 400 students that the Sheriff's department constantly harassed, surveilled, and treated as criminals.[35]

We know that there is a limit to how much technology can help students. New York state has led the way by creating regulations that block high risk, data extractive, discriminatory technologies in our schools – in 2023, New York State Department of Education put a moratorium on the use of facial recognition in schools because of its high risk of harm.[36] We don't fully know what the next high risk, data extractive, discriminatory technology is. And we don't fully know the potential risk and harm of technologies that already exist. We cannot sacrifice our students in the age of increased automation, over-reliance on algorithmic decision making, and rapid unregulated expansion of AI. When we fail to sufficiently protect student data we are unwittingly enabling the development of the next high risk, data extractive, discriminatory technology against New York City's children.

As such, the current revisions for Chancellor's Regulation A-820 are far too weak to protect our students and their families from current and future harms. They are a great starting point, but insufficient for the risks of this moment. Additional revisions must be made. Some examples of changes that can be made include:

- Include in Section II a definition of consent that follows the baseline definition of consent used in the Consentful Tech[37] framework. Include in the definition consent that consent must be affirmative and must be freely given, informed, specific, and enthusiastic, and an pathway for reversal of consent must always be provided to students and parents. Opting out is not consent. Throughout the regulations the text must be very clear when a loophole for opting out is allowed, as that is different from consent.
- Amend VII.A "A. Parents and Eligible Students generally have the right to consent to the Disclosure of Education Records and Student PII" to instead say "Parents and Eligible students must provide affirmative consent for the disclosure of education records and student PII." To say "Parents and Eligible Students generally have the right to consent" is vague and reads as being a gift of right rather than a mandatory and unalienable one that DOE and any other entities must honor.
- Add to VIII.A.2 that contracts and subcontractors are by default **not** DOE employees.
- Limit or get rid of entirely the types of student personal identifiable information (PII) that may be designated as Directory Information in Section VIII.F.3. The current list of PII that may be designated as Directory Information is far too expansive and puts students at risk. Having such an expansive list also goes beyond data minimization principles and creates a loophole to undermine affirmative consent that is far too large.
    - If limitations to types of student PII that can be designated as Directory Information is not changed, then at least require affirmative consent from the parent or eligible student for the sharing of student PII, even when designated as directory information. Do not allow for opt-out false consent as VIII.F.4.a.2 suggests.
- Add to Section IX.C that written agreements with authorized third parties accessing PII must include explanation of why student PII is necessary in order to fulfill their obligations and what benefit the access to PII will directly provide students.
- Add to Section IX.C that written agreements with authorized third parties accessing PII will include penalties for accidentally or intentionally sharing student data beyond the scope of the

[35] Pasco's sheriff uses grades and abuse histories to label schoolchildren potential criminals. The kids and their families don't know by Neil Bedi and Kathleen McGrory, published in Tampa Bay Times (November 19, 2020).
[36] New York bans facial recognition in schools after report finds risks outweigh potential benefits by Carolyn Thompson, published in the AP (September 27, 2023).
[37] Consentful Tech Framework (site last visited November 14, 2024).

project or to accidentally or intentionally sharing student data to additional parties beyond the parties named in the written agreement. This will help ensure that organizations commit to preventing data breaches and prevent unscrupulous organizations from selling student data for profit. Penalties should be proportional to the revenue and/or investment into the third party organization so that penalties do not disproportionately harm small businesses.

- More explicitly state that schools will not collect biometric data from students or families. Schools must avoid collecting biometric data from students and families at all costs. Biometric data is highly sensitive in terms of the exposure risk it creates if there is a data breach; how it could be used to criminalize protestors, abortion seekers, immigrants, and more; and the inherently discriminatory results when biometric data is used. There are other ways to improve student experience without schools collecting biometric data.

Additionally, with these changes, we must ensure that the DOE is sufficiently enforcing these regulations. Returning to the example of the ban on high risk, data extractive, discriminatory technologies like facial recognition in our schools, advocates found that schools have not been following the order from the state.[38] We cannot let the same failing happen with Chancellor's Regulations A-820. Unfortunately the current revisions to Chancellor's Regulations A-820 do not include any information on penalties for failure to comply with regulations and no information about the enforcement of these regulations. Unenforced regulations can be as bad as having no regulations at all.

We look forward to hearing about the continued revisions to Chancellor's Regulations A-820 and the plans for regulatory enforcement. Without a sufficient baseline of regulatory text and without proper enforcement, tech companies, data brokers, and fascists in government will work to profit off of our students' data without any regard for the humanity of the people who that data represents. We know that the DOE would not want to play any part in the dehumanization, extraction, or repression of any New Yorker. Improvements to Chancellor's Regulations A-820 and its enforcement is a necessary step towards that aim.

Please feel free to contact me with any follow up questions at aki@raceanddigitaljustice.org.

Sincerely,
Akina Younge

[38] NY is Ignoring the Ban on Facial Recognition in Schools by Juan Miguel and Daniel Schwarz from NYCLU (June 28, 2022)