ACLU of New York

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

2019 – 2020 Legislative Memorandum

Subject: **Relates to the collection of emergency health data and personal information and use of technology to aid during COVID-19**
S. 8448-D (Thomas) / A. 10583-C (L. Rosenthal)

Position: **CONDITIONAL SUPPORT**

We all share the fervent desire to safely re-open our state, and for many, there may be a temptation to turn to invasive technologies – from temperature screening devices to contact tracing apps – that promise to stem the virus' spread while permitting us to return to our normal routines. Many of these technologies collect the intimate details of our lives: our health status and symptoms, our associations, our locations and movements, and in some cases, even the details of our faces. Unfortunately, we have no national or state law governing privacy in the digital age that might protect this personal information from abuse and misuse.[1]

S. 8448-D (Thomas)/A. 10583-C (L. Rosenthal) would bridge this gap by requiring privacy protections for COVID-19 mitigation technologies, like Bluetooth proximity tracing and other digital contact tracing applications, infrared thermometers, standoff thermal cameras, symptom-tracking apps, and applications that provide food delivery to enable individuals to self-quarantine. Unfortunately, in the last round of amendments, the bill's most effective enforceability provision – a private right of action – was removed. Because the bill's protections will be meaningless without a robust enforcement mechanism, the NYCLU will support this legislation only if the private right of action is restored.

There are myriad individuals – such as undocumented immigrants, LGBTQ youth who come from unsafe homes, people who live in apartments with more people than they have on the lease, survivors of sexual violence and domestic violence, and over-policed communities – who could be at risk if their location, associations, or health status is released. The involvement of surveillance technologies in COVID-19 mitigation ups the ante by permitting more of this information to be collected and

[1] *See generally* Privacy & Technology What's At Stake, ACLU, https://www.aclu.org/issues/privacy-technology (last visited July 14, 2020). Furthermore, the Health Information Portability and Accountability Act (HIPAA) does not apply to the vast majority of technological COVID interventions. *See* Summary of the HIPPA Security Rule, HHS, July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

pooled more rapidly, creating treasure troves for data thieves, law enforcement, or immigration enforcement.

We already know that private companies have not always been good custodians of our personal information. One need only look at the running list of data breaches[2] to get a glimpse of the problem – to say nothing of the ways in which personal information has been misused by those to whom it has been entrusted. Personal information has been leveraged to ensure that only younger men see certain job postings, to skew certain housing, employment, or credit advertisements based on the race of the viewer,[3] and to urge Black voters to sit out the 2016 election.[4] It is easy to imagine targeted advertisers using suspected or confirmed COVID status to direct housing advertisements away from particular individuals or, conversely, to target job postings to those anticipated to have antibodies. Snake oil salesman may wish to advertise fake remedies to those believed to be COVID-positive.

The risks to individuals if their information falls into law enforcement or immigration enforcement hands may be more pernicious. If individuals have any reason to believe that sharing the details of their lives will expose them or their loved ones to criminalization or deportation, they simply will not use the applications and technologies that are designed to limit COVID-19's spread.

S. 8448-D/A. 10583-C would ameliorate these problems and enable individuals' security while using technology-assisted COVID interventions. The bill requires covered entities to notify people of what information they are collecting, what they are doing with it, and who they are sharing it with so that individuals can make informed decisions about what technologies to use. It also requires individuals' informed, opt-in consent before their information is collected or in any way used, and it limits applications to collecting and using only as much information as they need to do their jobs. It includes strict data retention limits, permits individuals to access everything a covered entity has about them, requires covered entities to have robust security practices, and strictly limits them from sharing individual information with third parties, including law and immigration enforcement. Importantly, it prohibits individual information from being repurposed in ways that the person to whom it pertains did not consent to and requires covered entities to engage neutral third party auditors to evaluate the efficacy of the technology, as well as its privacy and access to health care implications and the risks it poses of inaccurate, unfair, biased, or discriminatory results.

---

[2] List of data breaches, Wikipedia, https://en.wikipedia.org/wiki/List_of_data_breaches (last visited July 14, 2020).

[3] *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.

[4] 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.

An Amendment is Needed to Ensure this Bill is Effective

Unfortunately, the bill lacks an effective enforcement mechanism. While the bill maintains the Attorney General's enforcement role, government resources are necessarily limited – particularly as Governor Cuomo threatens massive budget cuts in response to coronavirus-induced revenue declines.[5] The Attorney General will only be able to enforce in the most egregious cases, if at all.[6] A private right of action not only allows individuals to seek redress in cases where the government chooses not to intervene or lacks the resources to intervene, but the threat of private lawsuits is likely to incentivize companies to adhere to a COVID-19 tech privacy law and protect individuals' information.

S. 8448-D/A. 10583-C includes numerous protections that are vital to preserve privacy in the digital age – whether during the COVID-19 pandemic or more generally. Given the stakes as we rush to safely re-open our communities, privacy protections for COVID-19 mitigation technologies are an important place to start. The NYCLU urges that S. 8448-D/A. 10583-C be amended to include a private right of action to ensure its efficacy. The protections it includes are not just privacy necessities; they are public health imperatives, and they must be enforceable.

[5] *E.g.* Anne McCloy, *Cuomo says NYS needs $61 billion to avoid 20 percent cut to hospitals, schools, localities*, CBS 6 ALBANY, May 12, 2020, https://cbs6albany.com/news/coronavirus/cuomo-says-nys-needs-61-billion-to-avoid-20-percent-cut-to-hospitals-schools-localities.

[6] *Cf.* Letter from Xavier Becerra, Attorney General, Cal., to Assemblymember Ed Chau and Senator Robert M. Hertzberg, Cal. Legislature (Aug. 22, 2018) (https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/08/ag-becerras-letter-re-california-consumer-privacy-act.pdf) (Writing about consumer privacy legislation in California, California Attorney General Becerra lamented that the lack of a private right of action would limit enforcement: "Finally, the CCPA does not include a private right of action that would allow consumers 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 consumers with a private right of action under the CCPA.")