Feb 14, 2019

Representative Zack Hudgins
Members of the House Innovation, Technology & Economic Development Committee
205A John L. O'Brien, P.O. Box 40600
Olympia, WA 98504-0600

AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Jean Robinson
Board President

Michele Storms
Interim Executive Director

Shankar Narayan
Technology & Liberty Director

Dear Chair Hudgins and Members of the House Innovation, Technology & Economic Development Committee:

Following up on my testimony in committee earlier this week, I write on behalf of the ACLU of Washington (ACLU-WA) in opposition to the Senate version of HB 1854 shared with stakeholders ("Carlyle 5") and in support of three other bills that collectively help address issues of data privacy and surveillance—HB 2046 (Rep. Kloba's alternative data privacy policy bill), HB 1654 (Rep. Ryu's face surveillance regulation bill) and HB 1655 (Rep. Hudgins's transparency bill around automated decision systems).

I. Overview

The ACLU-WA has a long-demonstrated commitment to individual privacy and consumer privacy issues. The events of the past year have shown both that data is power in our society; and that Big Tech will not police itself in this space. Consumers wanting to live a modern life hemorrhage data everywhere they go—from doing business on the internet, to being surveilled and tracked by cameras and other devices as they move about, and much more. All this data feeds unaccountable automated decision systems (ADS) that have unfair results. It has never been more clear that **we need the Legislature to support real empowerment that will allow consumers to take control of their data and rein in technologies like face surveillance and ADS that are being rapidly adopted without rules, transparency, or fairness.**

Unfortunately, **Carlyle 5 (HB 1854) does the opposite—**while borrowing some language from Europe's strong data privacy model (the GDPR), it does not establish a remotely similar framework. And the framework it does establish is riddled with so many exceptions and loopholes that **its overall effect will be to authorize data privacy violations, cede power to large corporations, legalize profiling that would otherwise be illegal, and preempt local efforts to enact strong data privacy protections**. The bill also authorizes a permissive regime on facial recognition (or face surveillance) that allows widespread adoption of the

technology with virtually no safeguards. More specifics on both these aspects of the draft are given below—I hope this information will be useful to the Committee.

We recommend the following steps:

- **On data privacy, the Committee should reject Carlyle 5 (HB 1854) and pass Rep. Kloba's own alternative privacy bill, HB 2046,** which does not preempt local regulations and makes progress on privacy policies; and convene consumer privacy advocates (rather than large tech companies) in the legislative interim to create meaningful privacy protections that truly model Europe's strong GDPR.

- **On automated decision-making, the Committee should reject Carlyle 5 and pass Rep. Hudgins' HB 1655,** which deals with the harms of data-driven automated decision-making and clearly makes discrimination by algorithm illegal. Contrast this to Carlyle 5's approach, which removed even the previous draft's weak protections against profiling. I recently sent the Committee a separate letter signed by 17 community-based organizations in support of moving HB 1655, and hope you will strongly consider it.

- **And on face surveillance, the Committee should reject Carlyle 5 and pass Rep. Ryu's HB 1654,** which creates a mechanism to ensure Washingtonians can determine how and where face surveillance will be used in our society. I have also sent a separate letter to the Committee signed by 17 community-based organizations in support of HB 1654.

II. Data Privacy in Carlyle 5

In this section of my letter, I attempt to summarize major concerns with Carlyle 5's approach to data privacy, which places very narrow restrictions on privacy violations in favor of businesses whose significant data privacy misconduct is well-documented. This list is not comprehensive. It's worth noting that in virtually all of the categories below, Carlyle 5 has become worse than earlier drafts, suggesting that it may not be possible to salvage the bill.

Specific concerns include:

1. **Using GDPR language without clearly defining terms is an invitation to evasion.** As mentioned in testimony earlier this week, simply parachuting in language similar to GDPR cannot work—because there is no regulatory regime in Washington State that could reasonably be expected to shepherd this law. By contrast, the GDPR relies heavily on interpretations and guidance being issued by EU and individual nation data protection authorities. The bill should create a clear plan and directive for the development of a regulatory infrastructure that can support a law such as this. Without a clear path forward in that manner, the law will not provide consumers with substantive protections.

2. **The bill does not place any requirements on businesses to have a legitimate reason for processing or sharing data.** In testimony this

week, Microsoft suggested that under Carlyle 5, a business had to declare a business purpose for collecting data, and would have to delete it if the business purpose no longer existed. This is emphatically not the case. In fact, the bill excludes the most important concept under the GDPR—the idea that entities should not be allowed to process the personal data of data subjects without some lawful basis for doing so. While the bill includes references to some concepts that orbit the concept of lawful basis (e.g., the bill contemplates "unlawful" processing and "legitimate" grounds for processing), it does not actually require controllers to establish a legal basis for processing personal data. It instead assumes that a business may process any data it wants about an individual, allows businesses to fail to document their justifications, and allows them to shift over time without notice to the consumer.

To address this, the bill should incorporate, wholesale, the requirement that exists under the GDPR that controllers establish (and document in any data privacy impact assessment) the grounds for processing data. Where consent is not relied upon (e.g., legitimate interest is the basis relied upon by the controller), then the bill should allow for the applicable regulatory bodies under WA state law (e.g., the Attorney General) to provide guidance akin to what EU law allows. Without a mandate of this sort, the law effectively legitimizes a vast amount of data processing currently carried out to the detriment of consumers, without providing consumers meaningful protections or remedies.

3. **The scope of application of the law is far too narrow.** The bill only applies to a limited subset of companies of a certain size or that are engaged in certain business practices. But consumer privacy should be protected from all companies, not just those that meet the narrow criteria set forth in the bill, and this is particularly true when we live in an era where countless small, fledgling companies are competing for consumer data. Their consideration for consumer privacy should begin on day one, not just at the point where they cross some arbitrary threshold.

4. **The bill heavily narrows or guts original GDPR definitions, allowing widespread evasion**:

    a. The **definition of consent has been heavily limited**. It is no longer required to be "freely given", meaning that burying terms in legalese or terms of services hundreds of pages long will be the norm—and as we all know, such check-the-box consent is not meaningful. This definition provides a large exemption to the processing restrictions in the bill.

    b. The **definition of personal data is heavily narrowed** well beyond what the drafters of the GDPR intended and is modeled after bad state data breach notification laws and the misunderstanding that the only data people should have to worry about are data sets that identify people on their face. This inures to the benefit of some of the worst privacy violators, such as advertisers. If the law doesn't apply to abstract persistent identifiers, it cannot protect consumer

privacy. Instead, a more robust definition of personal data should be included in a manner that does not include gaping loopholes.

c. **De-identified data should not be excluded** from the definition of personal data. This is a stark departure from the GDPR, which was developed with the understanding that data about a person can be extraordinarily sensitive even when trivially separated from key identifiers. It is for this reason that only truly anonymous data escapes the key regulations under the GDPR by not being considered "personal data" (data that could not possibly linked to another person, without regard for the data sets that might exist in the world). The scope of the current definition will allow data brokers, third party advertisers, and other parties unknown to consumers to exchange invasive and detailed datasets all because it is slightly abstracted from a "known natural person," even if it can be readily re-identified—something that is becoming increasingly easy when dealing with technological innovations and abstracted data sets.

d. **The definition of sale, which already only provided limited protection to consumers, has been further narrowed** by expanding exemptions even further. For example, an acquisition of one company by another doesn't qualify as a sale. So if Facebook purchases a data broker and ingests all their data, even that wouldn't receive the limited protections afforded to sales under the law. In a world where data is often exchanged, rather than bought or sold for money, monetary consideration should not be the limiting factor.

e. **The definition of process is heavily narrowed to a short list of specific actions on data**. Compare this to the GDPR's definition, which effectively encompasses any operation performed upon data.

f. **The definition of sensitive data has been narrowed to exclude political beliefs**, which are the exact kind that should receive heightened protection. Following the last election and various advertisers' roles in exploiting people's political beliefs, this is a particularly unfortunate omission.

5. **In multiple places consumer rights apply only to data that is maintained in "identifiable form."** This is an attempt to sidestep accountability by simply slightly abstracting data or splitting up data sets. Companies should not be able to shirk the very limited consumer rights offered in the bill by simply separating two databases.

6. **Section 4 of the bill should be revised to mandate particular data protection requirements for contracts between controllers and processors.** This important component of the GDPR is completely absent from the bill and renders the contractual requirement ineffective at providing substantive protections for consumers.

7. **The "business purpose" exception is hugely overbroad.** Consumer rights offered under the bill have had exceptions expanded to allow businesses to ignore consumer requests where they want to use the data for "business purposes", a broad concept that all but eliminates the value of the right in the first place. Astonishingly, this applies even in some contexts where a consumer has *revoked* their consent.

8. **The rights afforded to consumers have been weakened in a variety of ways in comparison to the GDPR**. Each provision analogous to one in GDPR has been narrowed so far beyond its scope as to be unrecognizable. For example, the right to deletion now contains massive exceptions that allow companies to avoid complying with requests entirely. The already weak risk assessment provisions have been further weakened, providing wiggle room for companies to argue that they don't need to acquire consent for risky processing activities. And the bill's carte blanche exemptions under Section 10 have even been further expanded to allow companies to escape the limited restrictions on processing (for example, in cases where the processing is carried out in furtherance of a contract)—that section contains nine exemptions, each of which is very broad in itself. (For example, the bill does not apply when the company is protecting "the vital interests of the consumer *or another natural person*" (emphasis added—"vital interests" are undefined.) These rights should be strengthened to match the more robust rights that have proven effective for protecting EU data privacy.

9. **The bill eliminates the previous restrictions on profiling consumers in ways that create legal effects for consumers.** This was already a weak restriction, but it's been removed entirely, and as I mentioned in Committee, this should be alarming to all of us. It makes clear that tech companies want to be able to engage in data-based profiling unhindered by *any* consumer protection whatsoever. This is exactly the kind of profiling that HB 1655 addresses, and adds urgency to our call for the Committee to pass that bill.

10. **The bill should not create a new exemption under the Public Records Act.** The law purports to provide transparency, but undermines this effort by completely excluding the applicable records from public viewing. The existing exemptions under the PRA are appropriate to protect business and trade secret interests, while preserving the right of the public to view this important oversight documentation. In an already uneven playing field where corporations hold most of the cards, this provision undermines what little power consumers have to enforce any privacy protections.

11. **The privacy protections afforded in the bill should not have a carveout for fraud detection or providing assistance to law enforcement.** There should not be a broad carveout for fraud detection, as this creates a massive loophole where companies may retain and process data in violation of the law under the pretense of fraud or identity verification—a phenomenon already widespread. In addition, the law enforcement use is a particular protection the GDPR was specifically implemented to facilitate. Like the GDPR, Washington law should only exclude compliance with actual legal process from the bill's requirements.

12. **The bill preempts all ability of local governments to enact meaningful privacy protections.** This preemption clause demonstrates that this bill is an effort to protect technology companies, not consumers. Local government will now be unable to protect consumer data privacy, and will be limited to the weak protections provided in Carlyle 5. The preemption clause should be removed.

III. Face Surveillance in Carlyle 5

ACLU-WA's broad concerns about face surveillance have been well-documented in our separate letters to this Committee in support of HB 1654, so I will only address issues specific to Carlyle 5 in this letter. Whereas HB 1654 places a moratorium on face surveillance acquisition and sets up a task force to consider appropriate uses of face surveillance, Carlyle 5 takes the opposite approach. While it purports to limit the use of facial recognition technologies, it instead legitimizes many oft-criticized and dangerous uses, and does not create meaningful oversight over misuse, bias, inaccuracy, or accountability. It's no wonder that the technology vendors selling this technology are pushing so hard for this provision—it effectively allows this technology the legitimacy to spread unchecked, while failing to give Washingtonians a meaningful choice to determine whether widespread face surveillance is even compatible with our constitutional freedoms.

Specific concerns include:

1. **The bill places no check on the worst uses of face surveillance.** The current draft only places a restriction on tracking "specified individuals in public spaces." This provision would allow public use of face surveillance, without warrant or suspicion, including, for example, at protests or places of worship, as long as it was not for purposes of surveilling "specified individuals" on an "ongoing" basis.

   If use of previous technologies such as automated license plate readers are any gauge, generalized, non-targeted surveillance is exactly how face surveillance will be deployed by law enforcement and other agencies—for example, the entire Muslim community in New York City was surveilled by the NYPD in exactly this manner. To believe this kind of generalized usage is not a threat is to be oblivious to the history of the use of surveillance technologies, particularly against vulnerable communities. And generalized, warrantless, suspicionless use of face surveillance technology has *already* been rolled out in jurisdictions such as Orlando, Florida.

2. **Even the individualized surveillance restriction is limited by broad loopholes.** For example, even "ongoing surveillance" of an individual by a state actor is allowed with a court order—and it is unclear whether the court order requirement included in the bill establishes a threshold of probable cause. In emergencies involving danger to a person, even the court order requirement does not apply—opening the door to the kinds of sweeping surveillance conducted by the NSA after 9/11, which were justified by terrorism-related concerns. Law enforcement should not be the sole arbiter of what constitutes such emergencies—which is even more

important given that face surveillance cannot be detected or challenged by the public after its deployment.

3. **The bill allows face surveillance technology to be used even if biased, and explicitly allows profiling based on face surveillance.** The bill allows third party testing of a face surveillance tool under limited conditions, but contains no requirement that the technology not be used if found to be biased. Given the many studies showing that face surveillance is less accurate both for recognizing and determining the affect of people of color and others, this omission is concerning. The Legislature should act to take biased technology off the table only if and until it can be deployed fairly. In addition, the bill explicitly allows face surveillance-based profiling, with only the requirement for "human review." Yet human review in other automated systems has still resulted in significant unfairness and bias—human review does not meaningfully address those issues.

4. **The bill allows affect recognition to be used unchecked.** Carlyle 5 uses an extremely narrow definition of facial recognition that is limited to "unique personal identification." This ignores some of the most dangerous uses of face surveillance—those that purport to determine if an individual is happy, sad, or dangerous, simply based on an analysis of their face. Microsoft, Google, and Amazon all have face surveillance products that incorporate this kind of "affect recognition" feature.

5. **The bill legitimizes face surveillance by private actors, requiring only undefined signage.** Even the very weak notice requirements in earlier drafts of this bill have, amazingly, been further weakened. Now, simply hanging signage will allow an entity the protection of the law—and the bill explicitly states that such signage will be considered consent. Placement of a notice should not qualify as consent, particularly if a consumer has no meaningful opportunity to patronize a different business. Such signage will not help a consumer, for example, if the only grocery store in their town uses face surveillance. Finally, there are no actual requirements for what this notice needs to include (e.g. that data collected might be used for purposes other than identity verification, to profile the user, or shared with completely unrelated third parties), nor any restriction on sharing the underlying biometric data with other parties and government agencies.

6. **The bill legitimizes broad collection and dissemination of biometric data.** If the criteria under Section 15 is met, there are no restrictions on downstream use of the facial recognition data collected by state actors, and that data could be shared or used for myriad other unrelated purposes.

7. **The bill requires reporting by September 30, 2023—an eternity in the technology space.** By the time the contemplated report is made, face surveillance will be commonly used, with a patchwork of rules written by the very agencies acquiring the technology. And the bill requires only reporting in that timeframe, not meaningful regulation. Four-and-a-half years is far too long to wait to regulate the spread of a technology that has the potential to change our democracy permanently by giving government agencies unprecedented power to surveil Washingtonians in public places.

IV. Conclusion

It should be surprising to no one that companies from the technology industry have come out in support of Carlyle 5. As currently written, it is drafted to give the illusion of privacy and regulation around face surveillance, while actually achieving neither. By virtue of controlling massive amounts of consumer data with little or no restriction on how they can use it, large tech vendors enjoy a significant power imbalance with respect to individual Washingtonians. Rather than legitimize such companies' unrestricted dominion in this space, the Legislature should insist on meaningful protections that empower Washingtonians, not the tech companies that traffic in their data and facilitate unaccountable surveillance. Please reject Carlyle 5 (HB 1854), and instead pass HB 1654, HB 1655, and HB 2046 as meaningful alternatives. Thank you for your consideration.

Sincerely,

Shankar Narayan
Technology and Liberty Project Director
ACLU of Washington