

Collin R. Walke, JD, CIPP-US, CIPM
cwalke@hallestill.com
(405) 553-2322

March 9, 2025

VIA EMAIL

Senator Wendy Harrison
wharrison@leg.state.vt.us

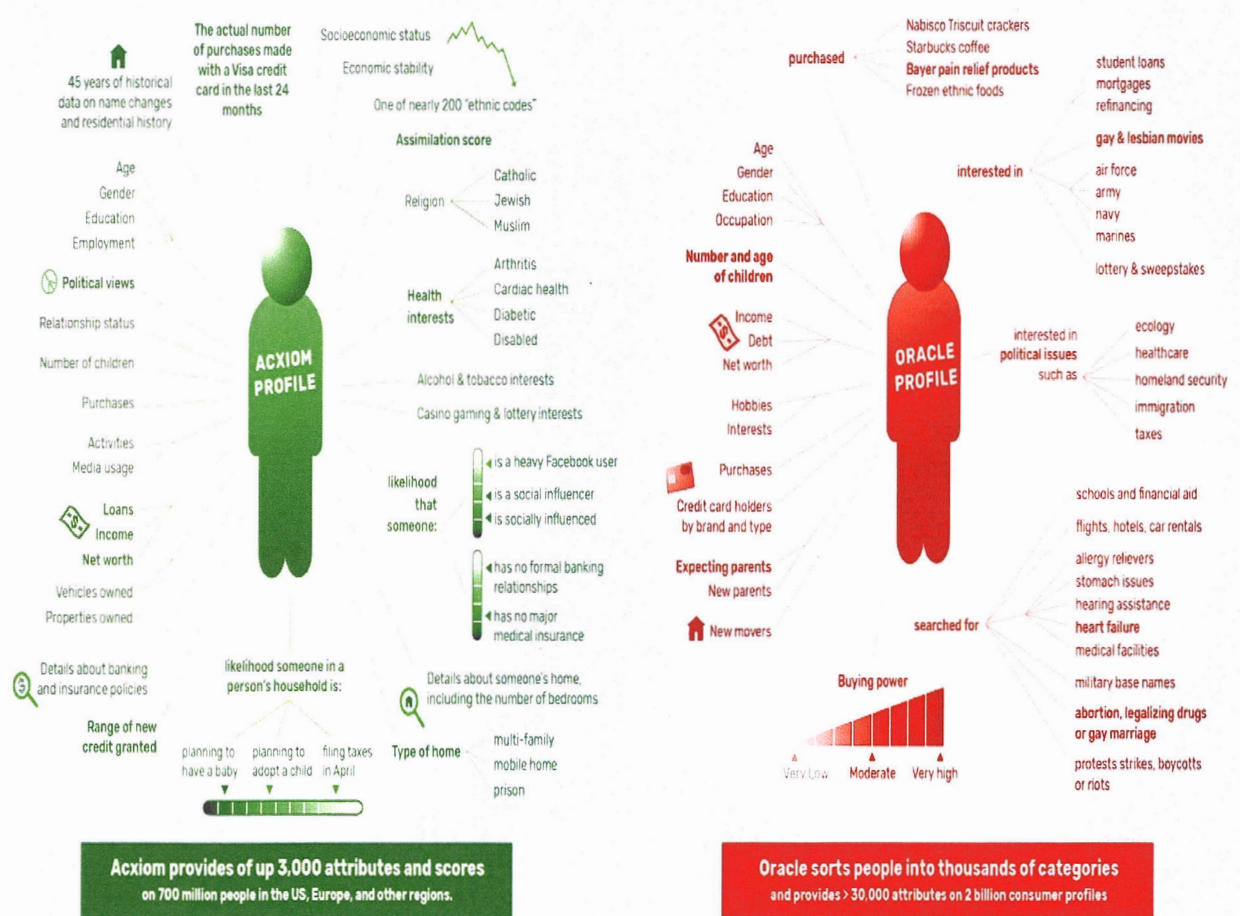
Re: S. 71 - An Act Relating to Consumer Data Privacy and Online Surveillance

Dear Chairwoman Harrison,

The below are but two (2) examples of the volume and sensitivity of data collected and inferred by companies about us:

DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle



© Checkmate LLC 01/14/10. April/May 2017. © 2017. All rights reserved. This information is provided for informational purposes only. This information is based on publicly available information and Oracle's best effort to accurately interpret and represent the companies' activities. Oracle cannot accept any liability in the case of omissions, errors, or omissions. Oracle's annual reports, developer website (API tools), Oracle press releases, Oracle website, and Oracle's website, last updated for January, 2017. Except as otherwise indicated, all other trademarks are the property of their respective owners. For more information on the sources see the report "Corporate Surveillance in the US" by the Center for Democracy and Technology.

This data is on top of data that is bundled and sold without effective regulation of any kind, *including children’s location data from popular apps like Life360.*¹ One would think that in the day and age of AI, where anyone’s data can be hijacked for deepfake or nefarious purposes, legislators would be eager to protect the public from the pilfering of their privacy for profit and exploitation.

However, a mountain of misinformation exists with regard to the function and costs relating to data privacy regulations. As a former legislator who personally battled oppositional lobbyists and their propaganda on my own opt-in data privacy legislation, an International Association of Privacy Professionals Certified Information Privacy Professional – US, Certified Information Privacy Manager, and attorney who works in the data privacy and cybersecurity field, I can speak with first-hand knowledge and provide logical proof that data privacy regulations actually *save everyone money.*

A. PRIVACY REGULATIONS SAVE MONEY AND SOLVE THE FREE RIDER PROBLEM.

Almost every cyber security insurance policy I have ever reviewed asked if the applicant implemented a privacy policy and certain other technical controls related to privacy concepts such as data minimization.² “Data minimization” is a decades-old concept that means companies should only retain data that is necessary for specific operations. If the data is not needed, then it should be deleted. Standard privacy policies mandate data minimization. The reason insurance companies want to ensure data minimization is implemented is because of the costs associated with remediating a data breach. The larger the amount of data retained by a company, the more likely the costs for remediation will be higher.

For example, if a company only does one-time transactions and retains no data relating to a particular consumer or client, then (1) the company is a low-value target for hackers and (2) even if the company is hacked, the costs of indemnification/remediation would likely be low. If, on the other hand, a company has poor privacy controls and retains data dating back to 2001, then in the event of a hack, the insurance company will likely have greater notification and/or indemnification obligations, depending on the data accessed. In other words, insurance companies want to make sure companies minimize data so that they minimize the value of claims.

And this begs the question: If companies are opposing S.71, do they not have cyber insurance? If they do, do they have privacy policies implemented that are actually meaningful (*i.e.*, in keeping with S.71)? If not, then those companies are free riders in the cyber insurance

¹ <https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user>

² See *e.g.*, https://www.in.gov/cybersecurity/education/cyber-law-and-insurance/cyber-insurance-toolkit/underwriting-security-controls-questions-resources/#Policies_and_Procedures

market whose vulnerabilities increase the risk pool for everyone else; and therefore, the costs for everyone else.

Moreover, businesses should already be complying with privacy industry standards. Even in Oklahoma, where we grow it, feed it, or pump it out of the ground – data isn't our thing - when I presented my opt-in data privacy legislation in 2020 to a group of developers, they all asked the question: “**What’s the problem with your legislation? We’re already telling our clients to do this.**” In other words, unless a business is too antiquated to understand its vulnerabilities by not abiding by data privacy standards (and thereby existing as a free rider) or they profit off the sale of our data (which should be illegal in any event), there is absolutely no reason why data privacy regulations should inherently increase costs.

B. THE TECHNOLOGY IS DIFFERENT, THE CRIMES AND EXPLOITATION ARE NOT.

As far back as 1792³, it was illegal to open another person’s mail in the United States, which would have been seen as an improvement from Cicero’s perspective, since he warned others to be careful what they wrote to him – lest spying eyes read it first.⁴ In 1968, Congress passed the Wiretap Act⁵ “in response to congressional investigations and published studies that found extensive wiretapping had been conducted by government agencies *and private individuals without the consent of the parties or legal sanction.*” (Emphasis supplied.)⁶ *Do tell the difference between a telecommunications company eavesdropping on an intimate conversation between you and your spouse and thousands of employees from Amazon doing the same?*⁷

Not a single member of the committee would desire any of their health information be shared publicly; and yet, many of our apps and IOTs share our health care data with companies and their employees without any meaningful regulation. Perhaps most terrifying is the fact that with AI, even innocuous data, such as grocery store purchases, can be used to predict sensitive health care conditions, such as whether a woman is pregnant. The continued bartering of our data is truly a privacy nightmare.

C. “PATCH-WORK LEGISLATION” IS NOT A JUSTIFICATION TO DO NOTHING.

In 2020, the opposition to my opt-in data privacy legislation (which passed the House with overwhelming veto-proof bipartisan support) warned of “patch-work” legislation and the costs of compliance with the same. Which is ironic because back then, the only data privacy law on the books was California’s. Now there are about 20 states with data privacy laws on the books. So, the “quilt” has gotten bigger, but I know of no business in Oklahoma doing business in other states

³ [https://scholarship.law.gwu.edu/cgi_viewcontent.cgi?article=2076&context=faculty_publications](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications)

⁴ <https://www.jstor.org/stable/3297818>

⁵ https://bja.ojp.gov/program/it/privacy-civil-liberties_authorities/statutes/1284

⁶ *Id.*

⁷ <https://www.vox.com/2018/5/24/17391480/amazon-alexa-woman-secret-recording-echo-explanation>; *see also*, <https://time.com/5568815/amazon-workers-listen-to-alexa/>

with privacy laws that went bankrupt complying with privacy regulations. There are several reasons for this.

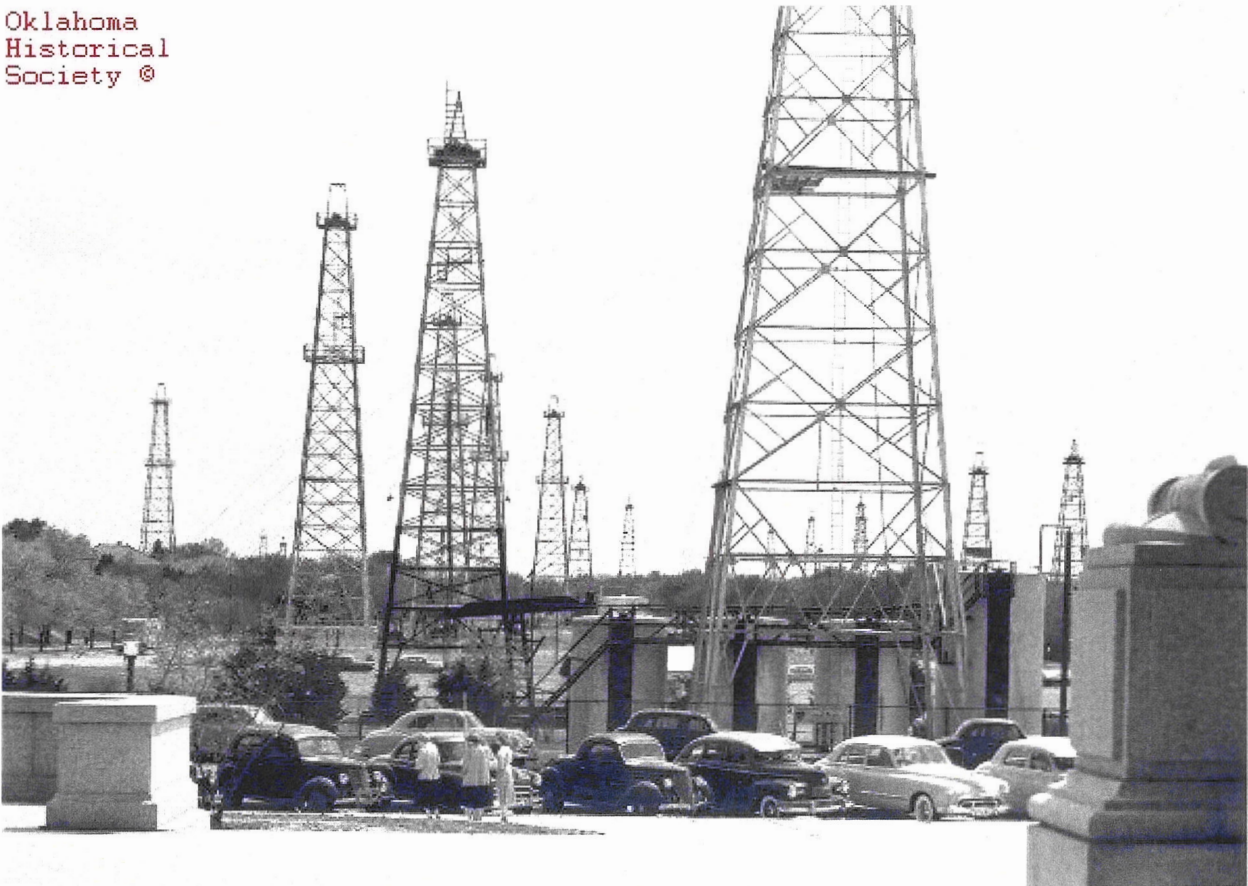
First, aside from thresholds for applicability and definitional nuances, data privacy laws are fairly uniform in concept (*i.e.*, data minimization, data portability, consent, the right to access, the right to delete, the right to correct, etc.). Therefore, compliance discrepancy costs are minimal. If you have to comply with one, you can fairly easily comply with all.

Second, neither S.71 nor any other existing law is anywhere near as stringent or harsh as the EU's GDPR (arguably, the most stringent data privacy law in effect in the West). Thus, imposing minimal regulations on an entirely unregulated area that poses substantial risks and harms is not unreasonable, especially in comparison to other possible regulations.

And third, the age-old political question must be asked: "Qui bono?" Who benefits? Who benefits from a lack of regulation? Not you or me. We and our loved ones are put at personal and financial risk by a lack of regulation. The only entities that benefit are those who are willing to place profits over privacy. Our data has subsidized the development of the internet and internet platforms. It is time to end that taxpayer subsidy.

A LESSON ON REGULATION FROM THE REDDEST OF RED STATES

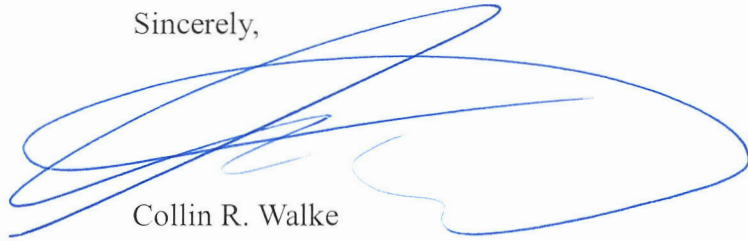
Oklahoma
Historical
Society ©



This is a historical photo of the south lawn of the Oklahoma Capitol. If you know anything about oil and gas, you know drilling wells that close together is not a good thing for the environment *or business* (because it reduces pressure and creates waste). As a result, Oklahoma eventually adopted spacing units, which specify how close wells can be drilled next to one another. There were winners and losers when spacing units were implemented, but regulation was necessary for both the consumers and the companies. Ultimately, everyone benefited from spacing unit regulation.

Data is the new oil. It's time to put in some spacing units.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Collin R. Walke', is written over the printed name. The signature is stylized and somewhat illegible due to overlapping loops.

Collin R. Walke

cc: K. Morse
KMorse@leg.state.vt.us