



May 22, 2023

Speaker Steve Yeager  
Majority Floor Leader Sandra Jauregui  
Minority Floor Leader P.K. O'Neill  
Nevada Assembly  
401 S. Carson St.  
Carson City, NV 89701

Re: Nevada S.B. 370, Nevada Health Privacy Legislation — *SUPPORT IF AMENDED*

Dear Speaker Yeager, Majority Floor Leader Jauregui, and Minority Floor Leader O'Neill.

Consumer Reports sincerely thanks you for your work to advance consumer privacy in Nevada. S.B. 370 seeks to extend to Nevada consumers important new protections relating to their personal health data, including prohibitions against collecting, selling, or sharing consumer health data without affirmative opt-in consent, the right to know the personal health data companies have collected about them and the right to delete that information.

Many companies that collect especially sensitive personal information, including personal health data, are failing to safeguard it. For example, a 2021 Consumer Reports investigation into seven of the leading mental health apps showed that they had significant privacy issues: many shared user and device information with social media companies and all had confusing privacy policies that few consumers would understand.<sup>1</sup> Similarly, the Federal Trade Commission has recently enforced against several companies that improperly shared personal health information with

---

<sup>1</sup> Thomas Germain, Mental Health Apps Aren't All As Private As You May Think, Consumer Reports, (March 2, 2021), <https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/>

third-parties or broke their privacy promises to consumers, including fertility tracker apps Flo<sup>2</sup> and Premom<sup>3</sup>, online counseling service BetterHelp<sup>4</sup>, and online prescription company GoodRx.<sup>5</sup>

Even when companies do not outright lie about their privacy protections, the hazy bounds of existing privacy law further complicate consumers' ability to understand company data practices. In a 2023 study headed by University of Pennsylvania researchers, 82% of consumers didn't realize that HIPAA does not apply to many health-related data in mobile apps.<sup>6</sup> As a result, many consumers share sensitive health information with businesses under the illusion that it has preexisting legal protections, when, in many cases, none exist..

Lawmakers need to remedy this imbalance. At a minimum, businesses should be required to transparently communicate to consumers when they are collecting and sharing health data, and this data should *only* be disclosed if consumers give an affirmative opt-in consent. While Consumer Reports would prefer a framework that prevents the collection *and* secondary use of personal health data for any purposes other than providing the service requested by the consumer, we are glad to see that S.B. 370 earnestly attempts to improve consumer privacy.

In particular, we appreciate that S.B. 370 includes:

- *A reasonable definition of consumer health data.* The definition of consumer health data included in this legislation covers key categories of personal information consumers may share with businesses that deserve additional protection, including among others, health conditions and interventions, biometric or genetic data, use or acquisition of medication, and gender-affirming care. Contrary to claims made by industry representatives, this definition would not feasibly cover *all* personal information, as it is limited to only personally identifiable information that a regulated entity actively uses to identify the health status of an individual.

---

<sup>2</sup> Federal Trade Commission, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others, (June 22, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>

<sup>3</sup> Federal Trade Commission, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order, (May 17, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>

<sup>4</sup> Federal Trade Commission, FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising, (March 2, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook>

<sup>5</sup> Federal Trade Commission, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising, (February 1, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>

<sup>6</sup> Turow, J., Lelkes, Y., Draper, N. A., & Waldman, A. E, Americans Can't Consent To Companies' Use Of Their Data, (February 20, 2023), [https://repository.upenn.edu/asc\\_papers/830/](https://repository.upenn.edu/asc_papers/830/)

- *Restrictions on sharing and selling without consent.* S.B. 370 requires that regulated entities obtain separate, specific consent to share consumer health data and written authorization to sell consumer health data. Importantly, the bill requires that any consent to *sell or share* consumer health data must be obtained separately from consent to *collect* consumer health data. This is especially important, as the drafters removed a provision that would have prevented consent to collect being obtained through agreement of general terms of service (see below). However, we note that the distinction between sharing and selling is often blurry, and may be confusing to consumers. Instead of bifurcating sharing and sales into separate consent processes, we suggest prohibiting all data disclosures to third-parties unless the consumer provides written authorization.
- *Prohibitions on geofencing.* Individuals should be able to receive in-person health care services without fearing that companies are tracking their visits and/or disclosing that information to additional third-parties. Potential uses or disclosure of such information could result in consequences that range from embarrassing to outright adversarial. For example, businesses could share healthcare visit information with insurance companies who could then use it as a basis to increase monthly premiums. Some third-parties may even disclose or be forced to disclose geofenced data with law enforcement. S.B. 370 appropriately bans such activity.

At the same time, there are several loopholes in the current draft that should be closed in order to provide Nevada consumers with the protections they deserve. We make the following recommendations to improve S.B. 370:

- *Clarify that businesses cannot condition provision of the service based on consent to collect unnecessary data.* The current version of the bill does not include prohibitions on consent to collect consumers' health data being obtained through acceptance of general terms of use. As a result, companies could simply bury important information about their collection and use of consumer health information in a dense terms of service or privacy policy filled with legalese, unlikely to be noticed by the vast majority of consumers. This interacts ambiguously with the anti-discrimination provisions of the bill, which state that businesses cannot discriminate against consumers (presumably by denying service, see below for suggested clarifications) for "taking any action" authorized by the bill. The drafters should clarify that businesses cannot condition provision of the service upon the collection or processing of consumer health data not reasonably necessary to provide the service. Without this protection, the right to opt-in will mostly be illusory, since consumers will be forced to either accede to the business' terms of service (and the collection of their consumer health data) or forgo using the service altogether. The drafters should restore Section 23 of the legislation so that businesses must obtain

consumers' consent to collect through a separate notice, and also add a provision to ensure that consumers can use the service without agreeing to superfluous data collection.

- *Clarify that the non-discrimination provision means price or service discrimination.* While we appreciate that the bill prohibits regulated entities from discriminating against consumers that exercise their rights under this act, the term “discriminate” is not defined or otherwise explained, which could lead regulated entities from construing the term narrowly. For that reason, we urge the drafters to specifically include prohibitions against price and service discrimination. We suggest the following language:

*(a) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, or did not agree to information processing for a separate product or service, including, but not limited to, by:*

*(1) Denying goods or services to the consumer.*

*(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.*

*(3) Providing a different level or quality of goods or services to the consumer.*

*(4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.*

*(5) This title shall not be construed to prohibit a business from offering discounted or free goods or services to a consumer if the offering is in connection with a consumer's voluntary participation in a program that rewards consumers for repeated patronage, if personal information is used only to track purchases for loyalty rewards, and the business does not share the consumer's data with third parties pursuant to that program*

- *Remove verification requirements from biometric identifier consent provision.* S.B. 370 seeks to create additional protections relating to the collection, sharing, and selling of individuals' biometric identifiers. However, the bill currently provides that in order to consent to the collection of such information, individuals must allow businesses to verify their identity using standards developed by NIST. In some cases, this may require the business to collect even more invasive information than the biometric identifier itself. This runs contrary to the spirit of the rest of the legislation; privacy law should seek to limit the amount of personal information people must provide just to live their lives, not mandate additional collection. Additionally, the bill should clarify that consumers can deny consent to collect biometric identifiers not reasonably necessary to provide a service and still use the service.

- *Add a private right of action for both sections.* Given the AG’s limited resources, a private right of action is key to incentivizing companies to comply. If businesses recognize that the AG is only capable of bringing a handful of enforcement actions each year, some might simply ignore the law and take their chances in evading detection. Further, it’s appropriate that consumers are able to hold companies accountable in some way for violating their rights.
- *Remove entity level carveouts.* The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act, as well as covered entities and business associates under the Health Insurance Portability and Accountability Act. These carveouts arguably make it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire bill if one arm of their business receives enough financial information from banks or crosses the threshold into providing HIPAA-covered healthcare services, a line many of them are already currently skirting.<sup>7</sup> At most, the bill should exempt *data* that is already protected by those sectoral laws, while extending coverage to consumer health data collected by such entities that is not currently regulated.

We look forward to working with you to ensure that Nevada consumers have the strongest possible privacy protections.

Sincerely,

Matt Schwartz  
Policy Analyst

cc: Senator Cannizzaro  
Members, Nevada Assembly

---

<sup>7</sup> See e.g., The Economist, “Big Tech Pushes Further into Finance,” (Dec. 15, 2022), <https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance>; Richard Waters, “Big Tech searches for a way back into healthcare,” Financial Times, (May 17, 2020), <https://www.ft.com/content/74be707e-6848-11ea-a6ac-9122541af204>