June 27, 2016

The Honorable Hannah-Beth Jackson
Chair, Senate Judiciary Committee
State Capitol, Room 2171
Sacramento, California 95814

Re: AB 2688 (Gordon) Privacy: commercial health monitoring programs – As Proposed to be Amended June 21, 2016 - Oppose

Dear Senator Jackson:

We must oppose AB 2688 (Gordon), both in its current April 28, 2016 version, and as proposed to be amended on June 21, 2016. At the Assembly Privacy and Consumer Protections Committee hearing on May 3, 2016, Assemblymember Gordon committed to work to improve the privacy protections that a coalition of labor, senior and consumer rights groups stated were entirely deficient. Instead, the draft of the June 21, 2016 amendments would make AB 2688 an industry-driven proposal that licenses the worst privacy invasions.

We have already written about our reasons for opposing the previous version of AB 2688. In brief, as technology rapidly advances and more devices, apps and online platforms have access to individually identifiable medical information, California's strong Confidentiality of Medical Information Act (CMIA) should be modernized to acknowledge the proliferation of commercial access to this data. Instead of building on CMIA, with its strong consumer controls and significant sanctions for unauthorized willful or negligent data sharing of individually identifiable medical information, AB 2688 walls off CMIA and establishes a parallel and weak privacy regime for this data, which it redefines as "individually identifiable health information" merely because a business under AB 2688's scope is not currently a covered entity under CMIA. In a striking departure from CMIA, AB 2688 establishes modest and poorly crafted consumer controls, but only over willful unauthorized information sharing, and it contains no effective sanctions for violations of willful or negligent unauthorized information sharing.

Our comments on the proposed June 21, 2016 amendments that make a bad bill much worse follow:

- The latest draft amendments would eliminate an opt-in for information sharing, replacing it with an opt-out that the commercial health monitoring program "shall make available".

- It eliminates language requiring that an information sharing authorization be "clear and conspicuous", which means the "consent" now can be hidden in a lengthy legal notice that consumers don't read and cannot understand.

- It eliminates the requirement for a commercial health monitoring program to inform consumers of a right to revoke an information sharing consent, enabling it to bury the revocation request process in some obscure place on a website, or omit any mention of it at all.

- It eliminates language protecting a consumer from a cost or penalty for revoking information sharing consent, allowing a fee or penalty price for privacy.

- While the amendment refers to some undefined "request for authorization" a careful reading of the entire set of amendments leads us to conclude that this alleged "request" is in practice a no-opt information sharing requirement for any consumer that wants to use the fitness or health app, device or commercial health monitoring program.

- The draft enables a fitness app or commercial health monitoring program to deny the use of the product or service to a consumer who does not agree to the information sharing, by striking language that would have allowed a dissenting consumer to use the commercial health monitoring program. A court reviewing the legislative history of this bill would likely conclude that this non-discrimination language was struck to permit disparate treatment of consumers who assert privacy rights.

- The draft eliminates language that would have informed a consumer of the name and nature of a third party with which the personally identifiable information is shared, instead allowing a commercial health monitoring program to limit a disclosure to a vague "reason" for sharing with unlimited third parties. This disclosure could be satisfied with a generic statement such as to "enhance the user experience," which leaves the consumer in the dark about a business' plan to share confidential consumer information with data brokers and resellers.

- The draft eliminates most commercial health monitoring programs from any coverage at all, by limiting it to those whose "primary purpose" is to collect health monitoring information "when that information is stored over time". This language would exempt devices such as the Apple Watch, and a Google watch which is under development, since these devices have several purposes in addition to health information collection. It likely eliminates Fitbit, Jawbone and other devises that collect that information but may not "store" it over some ill-defined "time", which could be months, years, or decades.

- The draft allows an app developer or commercial health monitoring program to share personally identifiable health information that is "relevant" to a grievance, lawsuit, arbitration or other "claim or challenge" without consumer consent, subpoena, warrant or other due process. This language could be used to harm a worker, insured person, or consumer by allowing unrestricted handing over of confidential health information to a boss, insurer or business in a non-judicial proceeding.

- The draft permits virtually unlimited personal information sharing between a commercial health monitoring program and a co-branded entity (e.g. Apple Watch and Apple iTunes

or Apple Mac) with no further restriction on the sale, use, or sharing of the of the personally identifiable health information by the co-branded recipient.

- The draft exempts from the definition of "individually identifiable" health information any identification of a device, cell phone, computer or tablet device, allowing confidential data aggregation based on the device's identifier.
- It reduces the duty of a commercial health monitoring program to protect the security of individually identifiable health information, instead only requiring that records be "reasonably" secured.
- It further dilutes already weak liability language against an employer who releases individually identifiable health information without a worker's consent, by immunizing an employer who has "attempted in good faith to substantially comply" with this bill.

We do not believe that the ersatz privacy protection of AB 2688 is the best that consumers using commercial health monitoring programs can attain. In its current form, and as proposed to be amended, AB 2688 is a big step backwards for privacy. We urge you to vote "no" on AB 2688.

Sincerely,

Richard Holober
Consumer Federation of California

Hene Kelly
California Alliance for Retired Americans

John Simpson
Consumer Watchdog

Joe Ridout
Consumer Action

Emily Rusch
California Public Interest Research Group

Sam Rodriguez
UFCW Western States Council

CC: Members and staff, Senate Judiciary Committee
Assemblymember Gordon