

## Will this Utah proposal quash lawsuits from victims of data breaches?

A brief look at Utah legislative activity on tech-related proposals over the past week

By [Art Raymond@DNTechHive](mailto:Art.Raymond@DNTechHive) Feb 14, 2021, 4:03pm MST

<https://www.deseret.com/utah/2021/2/14/22279124/utah-legislature-data-breach-hacking-personal-privacy-porn-filtering-mobile-devices>

SALT LAKE CITY — Should consumers have the right to sue a company that allows their personal information to be stolen by data thieves?

Under a proposal moving quietly through the 2021 Utah legislative session, the bar for filing such a lawsuit would be raised considerably in the event that a company has taken at least some measures to keep your data protected.

Rep. Walt Brooks, R-St. George, said his bill, [HB80](#), uses a carrot in lieu of a stick to incentivize companies to build and maintain robust cyber protections for sensitive personal information they collect from customers. So long as they do, those companies can reside in a so-called legal “safe harbor” created by Brooks’ bill in which they would find some protections from tort claims following any data breach or hacking incidents.

The business-friendly proposal is drawing support from industry groups as well as the Salt Lake Chamber.

Jacey Skinner, the chamber’s vice president for public policy and general counsel, said the new protections were “a very positive way to help with the goal of protecting customer information” as opposed to rules that only mete out punishment, usually in the form of fines, if and when computer hacks or other actions lead to the loss of customers’ personal information.

The American Bar Association weighed in on [a similar proposal passed by Ohio lawmakers in 2018](#), calling the new rule “a unique incentive for voluntary compliance with cybersecurity measures that contrasts to laws in other states, like [New York](#) and [Massachusetts](#), that punish noncompliance with cybersecurity provisions.”

However, the national lawyers group also warned that the creation of an affirmative defense against tort claims, as the Utah proposal seeks to do, does not result in an impenetrable liability wall. The group’s legal analysis notes there are other avenues by which consumers who have lost data seek damages and that the safe harbor does not let companies off the hook in having to present a defense of their cybersecurity systems.

“Eliminating tort claims likely will not significantly reduce a defendant’s exposure because other common data breach claims, like statutory violations or contract theories, would likely still be available,” the bar association report reads. “Additionally, in typical data breach cases involving multiple states, plaintiffs can avoid the safe harbor entirely by electing a different state as the forum.

“Additionally, proving eligibility for the safe harbor will present significant challenges. To prove the defense, an entity must show that it created, maintained, and complied with a written cybersecurity program ... (and) it must comply with designated industry or government cybersecurity frameworks.” HB80 earned unanimous support from the Utah House Friday and now heads to the Senate for that body’s consideration.



Rep. Susan Pulsipher, R-South Jordan, discusses HB72 with members of the House Public Utilities, Energy and Technology Standing Committee at the State Office Building in Salt Lake City on Wednesday, Feb. 3, 2021. The bill would establish filter requirements and enforcement mechanisms for tablets and smartphones activated in the state on or after Jan. 1, 2022. *Steve Griffin, Deseret News*

### **Default porn filtering on mobile devices advances**

Rep. Susan Pulsipher's bill aiming to require makers of cellphones and tablets to have pornography filtering software installed and switched on for all device sales to Utah customers found support after two previous committee reviews ended without advancing the proposal.

HB72 has been revised along the way on a journey that started last October at an interim legislative hearing. The current version, in addition to calling for compulsory, switched on content filtering software on internet-connected mobile devices, also includes an enacting clause that requires five other states to adopt similar measures before the rule becomes law in Utah.

And Pulsipher dropped potential per incident fines from \$2,500 to \$10 with a cap of \$500.

While some members of the House Public Utilities, Energy and Technology Committee wanted to see the proposal pushed to the legislative interim session for further discussion, a 6-5 vote on Thursday advanced the bill to the full House for that body's consideration.

Thursday's public comments included Dr. Jacob Gibson, a South Jordan family therapist, who said he regularly sees patients and their families who are dealing with the consequences of too-early exposure to explicit, adult material.

“One of the most difficult challenges I work with are the effects from pornography,” Gibson said. “Average age of first exposure, which is often accidental, is 10 to 11 years old. Anything we can do to help prevent that puts us in a proactive rather than a defensive position.

“Because (children) are not developmentally ready to handle that type of material, it leads to the problems of depression, anxiety and all the problems that go with that including and up to its most extreme form, suicide ideation and attempts,” Gibson said.

Opponents of the bill, which include representatives of retailer and manufacturer groups, roundly agreed about the harms inherent in children being exposed to adult internet content, but argue Pulsipher’s legislation is the wrong way to address the issue.

Carl Szabo, vice president and general counsel of tech industry-supported public policy advocacy group NetChoice, said the new rule would give parents a “false sense of security” with filtering software that could be easily defeated by tech-savvy youth.

“Utah will be sending out a message to parents, ‘Don’t worry the protections are on,’” Szabo said.

And, the American Civil Liberties Union of Utah raised flags of concern over the potential for the proposal to also compel device manufacturers to implement “always on” location tracking to comply with new mandates as well as stipulations in the bill potentially creating civil rights infringements.

“This bill imposes restrictions on free speech that are too broad to achieve this goal without encouraging companies to block protected content,” one ACLU tweet on Thursday read.

### **New porn filtering requirements for school contractees**

Companies that provide digital services to K-12 Utah public schools could see new porn filtering contract clauses under a proposal that earned committee approval on Friday.

HB38 would require the providers of digital services and products used by Utah public schools to have mechanisms in place to block all “obscene or pornographic material,” according to bill language. And failure to successfully block such content, or quickly address any issues of explicit material making it past filtering mechanisms, could lead to loss of payment or contract termination.

The proposal’s sponsor, Rep. Travis Seegmiller, R-St. George, said his bill was crafted to help keep companies from inadvertently blocking appropriate content and avoiding practices that could be characterized as censorship or “book burning.”

One public commenter that spoke to members of the House Judiciary Committee Friday recounted an incident that raised her awareness of, and concern about, student access to explicit material on public school computers.

Michelle Boulter said her son was exposed, accidentally at first, to pornographic images while in a third grade computer lab class.

“He sort of just stumbled on it but continued to return to it each week,” Boulter said. “The effects of that followed him all the way until he got the help he needed in his late teens.

“Our son’s story ended happily but that’s not the case for all students.”

Committee members voted unanimously to advance HB38 to the full House for that body’s consideration.