



MISSOURI HOUSE OF REPRESENTATIVES
WITNESS APPEARANCE FORM

BILL NUMBER: HB 1162		DATE: 3/8/2021	
COMMITTEE: General Laws			
TESTIFYING: <input checked="" type="checkbox"/> IN SUPPORT OF <input type="checkbox"/> IN OPPOSITION TO <input type="checkbox"/> FOR INFORMATIONAL PURPOSES			
WITNESS NAME			
INDIVIDUAL:			
WITNESS NAME: ARNIE C. AC "HONEST-ABE" DIENOFF-STATE PUBLIC ADVO		PHONE NUMBER:	
BUSINESS/ORGANIZATION NAME:		TITLE:	
ADDRESS:			
CITY:		STATE:	ZIP:
EMAIL: arniedienoff@yahoo.com	ATTENDANCE: Written	SUBMIT DATE: 3/8/2021 2:02 PM	
THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.			

I am in Support of this Bill.



MISSOURI HOUSE OF REPRESENTATIVES
WITNESS APPEARANCE FORM

BILL NUMBER: HB 1162		DATE: 3/8/2021
COMMITTEE: General Laws		
TESTIFYING: <input checked="" type="checkbox"/> IN SUPPORT OF <input type="checkbox"/> IN OPPOSITION TO <input type="checkbox"/> FOR INFORMATIONAL PURPOSES		
WITNESS NAME		
INDIVIDUAL:		
WITNESS NAME: BROOKE HENDERSON		PHONE NUMBER:
BUSINESS/ORGANIZATION NAME:		TITLE:
ADDRESS:		
CITY:	STATE:	ZIP:
EMAIL: mbhenderson@protonmail.com	ATTENDANCE: Written	SUBMIT DATE: 3/7/2021 6:42 PM

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.

Chairmen Trent and Esteemed Members of the House, I am testifying in Support of HB 1162 to protect Missouri's teachers and students. Protection of our education system and those in it, especially the children, must be protected to the highest standard and laws but created to ensure their protection. I want Missouri to be the leader in America for taking a strong stance on protecting teachers and students when it comes to data privacy. As more and more on-line learning is taking a forefront, our children have never been more at risk to bad actors, data-mining, data breaches, on-line creditors, and long-term harm as a result of personally identifiable information being collected. This information is being collected, in most cases, without the consent of parents. Students as young as 5 years-old are automatically being assigned Google accounts that use and collect personally identifiable information. In many schools more than 181 apps are being used in the classroom and at home. That means over 181 terms of use and policies, some are over 80 pages in length. In September 13, 2018 the FBI issued a warning to all education institutes about the dangers of Edtech and Data collection. On multiple occasions Missouri United States Senators Josh Hawley (R) partnered with Marsha Blackburn (R), Ed Markey (DI), and Richard Blumenthal (D) in a bi-partisan effort to strengthen data and on-line protections for children via COPPA. I, personally, have substantial evidence of great harm to both our students and teachers. A child's education cannot and MUST not come at the cost of our children or our teachers. According to the k-12 Cybersecurity resource, there have been more than 1,800 incidents of data breaches involving k-12 since 2016. Many districts suffered more than one breach. This is concerning and alarming. Several of these breaches have occurred in Missouri's schools putting students' education at direct risk and again creating long-term harm for America's students. Education has to the expectation and the exception. One of the ways to provide an excellent education begins with robust data privacy bills. I applaud Representative Trent's deep understanding of this critical situation and I fully support HB 1162. Thank you for your time and dedication to Missouri! Brooke Henderson



MISSOURI HOUSE OF REPRESENTATIVES
WITNESS APPEARANCE FORM

BILL NUMBER: HB 1162		DATE: 3/8/2021
COMMITTEE: General Laws		
TESTIFYING: <input checked="" type="checkbox"/> IN SUPPORT OF <input type="checkbox"/> IN OPPOSITION TO <input type="checkbox"/> FOR INFORMATIONAL PURPOSES		
WITNESS NAME		
INDIVIDUAL:		
WITNESS NAME: MARY BYRNE, ED.D.		PHONE NUMBER:
BUSINESS/ORGANIZATION NAME:		TITLE:
ADDRESS:		
CITY:		STATE: ZIP:
EMAIL: mary.byrne53@att.net	ATTENDANCE: Written	SUBMIT DATE: 3/7/2021 8:25 PM

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.

State legislators are getting more serious about data privacy, with legislation in at least 10 states besides Missouri. Over the last decade there has been a reckoning over how digital companies collect personal data, what they do with it, and whether or not they're capable of protecting it. Online data collection is still not regulated at the federal level in the U.S. But states are slowly embracing policies to ensure that digital companies protect their users—or at least introduce more transparency. Illinois led the way in 2008 with the Biometric Information Privacy Act, a law that lets Illinois residents sue companies that collect their biometric data (face scans, fingerprints, etc.) without their consent. After Europe passed the General Data Protection Regulation in 2016, which entitles people to obtain any data collected on them and have their records deleted, California decided to use it as a framework for its own law. Two years later it introduced its version of the GDPR, called the California Consumer Privacy Act. California passed an amendment, called the California Privacy Rights Act, that clarifies the original law and adds a governing body called the California Privacy Protection Agency that can bring action against violators. The original CCPA has now inspired several look-alike laws in other states, as momentum builds for state-level privacy legislation. 2021 could be the year that privacy laws become more pervasive across the country, helping Americans wrest back some of the aspects of their digital lives. Here's a rundown of other state-level privacy laws beyond those in Illinois and California, plus the bills that could be passed into law this year. Nevada adopted the Privacy of Information Collected on the Internet from Consumers Act in 2019, which allows consumers in the state to opt out of personal data collection. Vermont In 2020, Vermont passed a law that requires data brokers to inform consumers when their personal information has been leaked or breached. Maine Maine's new privacy law went into effect in August 2020, after a short one-month delay. Unlike other privacy laws in the U.S., this one is aimed squarely at Internet Service Providers. It prevents them from sharing or selling personal customer data without explicit consent. Virginia This year, Virginia's House and Senate both approved the Consumer Data Protection Act. The governor is expected to sign it into law in March. The new rule would give Virginians many of the same data protection rights as California's law. This includes the ability to "access, correct, delete, and obtain a copy of personal data and to opt out of the processing of personal data for the purposes of targeted advertising." The law will go into effect in January 2023. New York In January, New York legislators introduced several privacy bills. The New York Privacy Act replicates much of the EU's GDPR but adds a private right of action. This will allow individuals to bring lawsuits based on violations rather than relying on a governing body to do it. Another law, Assembly Bill 27, would amend New York's general business law to include a new biometric privacy act that guards against the nonconsensual collection of a person's physical identifiers. This law also gives individuals the opportunity to seek legal action if they can make a case for how their rights have been violated. Washington After several attempts to pass a data privacy law, Washington may be in the home

stretch. The State Senate just introduced a new version of the Washington Data Privacy Act. The bill allows consumers to find out what data has been collected about them, ask for a copy of it, correct or delete that data, and have that data transferred to another platform. Critics have called the law, which was created in collaboration with Amazon and Microsoft, “toothless.” They prefer another bill, recently introduced in the House, called the People’s Privacy Act, which is more explicit about biometric data rights and requires companies to obtain explicit consent before processing or sharing personal data. It’s not yet clear how this will play out, but the state is likely to embrace one of these rules (if not an amalgamation of both) this year.

Utah passed the Electronic Information or Data Privacy Act in 2019, which required law enforcement to obtain a warrant before requesting personal data from companies. It now has another consumer privacy law currently in committee. The Consumer Privacy Act was introduced in February and allows consumers to access, copy, and delete any personal information that a company collects about them. It also empowers the attorney general to investigate a company’s data practices. The law would require companies to provide transparency around what kind of personal data they collect, who they share it with, and how customers can exercise their rights to obtain their own data.

OklahomaThe Oklahoma Data Privacy Act was introduced in January. It’s similar in scope to several other data privacy laws that aim to provide consumers access to data that’s been accumulated about them and giving them the opportunity to have it deleted. Oklahoma’s law limits the kind of companies that are subject to these rules to those that earn 25% of their revenue through personal data sales, data brokers with more than 50,000 users, or companies that make more than \$10 million annually. Those that fall into this category must have a web page on their website that tells consumers that their data may be sold and how to opt out of that sale.

There are several other bills currently on the docket in Alabama, Arizona, Florida, Connecticut, and Kentucky, all of which follow a similar format to California’s CCPA. These laws rely on consumers to opt out of data collection, rather than pushing companies to obtain consent before collecting data—a win for tech companies. Still, the more states embrace these laws, the more consumers will have a right to know what information has been collected on them and an opportunity to stop it.

Children and teachers of Missouri deserve to live in a state that protects their persons and personal data from being used without their knowledge or permission. We cannot wait for Congress to act on behalf of the American people. It’s up to the Missouri legislature to act on behalf of the people of Missouri.

The content of this article is extracted from a 2021 article by Ruth Reader published in FastCompany.com