

The blame game began even before Parson's press conference, as Wednesday's *Post-Dispatch* report said:

In the letter to teachers, Education Commissioner Margie Vandeven said "an individual took the records of at least three educators, unencrypted the source code from the webpage, and viewed the social security number (SSN) of those specific educators."

In reality, the Post-Dispatch discovered the vulnerability and confirmed that the nine-digit numbers were indeed Social Security numbers. The paper then told the department that it had confirmed the vulnerability with three educators and a cybersecurity expert.

The *Post-Dispatch* story included the paper's attorney's response to the state's accusations.

"The reporter did the responsible thing by reporting his findings to DESE so that the state could act to prevent disclosure and misuse," *Post-Dispatch* attorney Joseph Martineau wrote in the statement. "A hacker is someone who subverts computer security with malicious or criminal intent. Here, there was no breach of any firewall or security and certainly no malicious intent. For DESE to deflect its failures by referring to this as 'hacking' is unfounded. Thankfully, these failures were discovered."

Parson's definition of "hacker" is quite broad, as he claimed that "a hacker is someone who gains unauthorized access to information or content."

"Under Missouri law, a person commits the offense of tampering with computer data if he or she knowingly and without authorization accesses, takes, and examines personal information without permission," Parson said. "This data was not freely available and had to be converted and decoded in order to be revealed."

A 'Mind-Boggling' Flaw

The *Post-Dispatch* also spoke with Professor Khan for its initial story on the vulnerability. "We have known about this type of flaw for at least 10-12 years, if not more," Khan told the newspaper in an email. "The fact that this type of vulnerability is still present in the DESE web application is mind-boggling!"

"Unfortunately, these types of flaws and poor design choices are more common than we'd like," Khan also wrote. "Local and state governments across the country are often still using applications developed many years ago and potentially containing serious security flaws."

While the *Post-Dispatch* apparently confirmed the flaw by looking at just a few employees' records, the article said that "state pay records and other data" indicate that "more than 100,000 Social Security numbers were vulnerable."

Local teacher's union spokesperson Byron Clemens told the *Post-Dispatch*, "We're pretty shocked to

hear” about the vulnerability exposing teachers’ personal data. Clemens “praised DESE for taking quick action to remove the affected website, but cautioned, ‘We don’t know if anybody’s been harmed yet.’”

Thursday’s [follow-up story](#) in the *Post-Dispatch* pointed out that Parson “has often tangled with the state’s media outlets over coverage he dislikes” and that, after this morning’s press conference, he “didn’t respond to questions that were yelled at him as he retreated into his office.”

Missouri Press Association attorney Jean Maneke was quoted as saying, “There is not a solid basis to suggest the *Post-Dispatch* did anything wrong. The story simply points out that government dropped the ball. It is to the public’s benefit that this information be out there to protect sensitive information.” Maneke also said that Parson’s tactic of “threaten[ing] legal action even when there is no basis for it... was often used by the Trump administration to intimidate reporters.” She added, “I am not aware of any time a public official has sued a member of the media for something like this and had a successful lawsuit.”

Source: [Missouri Threatens to Sue a Reporter Over a Security Flaw](#)