

Missouri Gov. Mike Parson's unconstitutional attack on the press

From afar, Missouri Gov. Mike Parson's attempt to prosecute a St. Louis Post-Dispatch reporter looks like the folly of a vindictive politician who doesn't understand computers or the First Amendment.

But it is more serious than that. A governor trying to prosecute a journalist for reporting publicly available information poses a serious threat to press freedom. It's unconstitutional and a sign of what happens when the press becomes fair game as the "enemy of the people."

Josh Renaud, the reporter, was aggregating Missouri state data on teachers to identify who was unlicensed. He noticed that the HTML code contained nine-digit numbers and surmised these might be Social Security numbers. HTML – Hypertext Markup Language – is simple coding language that structures web pages.

Rather than rushing to post a scoop, Renaud and the Post-Dispatch did the right thing. They alerted state education officials, giving them time to fix the problem before the Post-Dispatch disclosed the longstanding privacy vulnerability.

Documents recently obtained by the Post-Dispatch under the Sunshine Act show that Education Commissioner Margie Vandeven was about to thank Renaud. But Parson surprised her. With the head of the Highway Patrol in tow, Parson went before reporters to accuse Renaud and the Post-Dispatch of violating criminal hacking laws. The case is now before a state prosecutor.

Parson's announcement was extraordinary for several reasons.

First the First Amendment does not permit the government to jail reporters for disclosing publicly available information. The U.S. Supreme Court wrote in 2001 that "state action to punish the publication of truthful information" seldom is justified, citing a case where a Florida reporter had published the name of a rape victim even though state law prohibited publication.

Second, Parson's amped up claims showed he didn't understand computers.

Mark Sableman, a media lawyer at Thompson Coburn LLP in St. Louis, explained the nature of HTML code and why it is different from content protected from hacking.

"HTML code is not hidden in any way," Sableman wrote in an email. "By its nature, it is public. Saying that it is hacking when someone looks at a web page's HTML code is a bit like saying it is hacking when someone opens the cover of a book and begins reading the pages inside. The HTML code, like the words inside the book, have always been readily accessible for anyone to see, without any locks, keys, passwords, or other access restrictions. HTML code is always public, so no one needs special authorization."

He pointed to a 2006 case – *Field v. Google Inc.* – where a federal judge held, in Sableman's words, that "codes within the HTML serve as signals to the public, including search engines, as to how a website can be accessed, and whether or not its contents can be copied or indexed by search engines.

"In other words, courts recognized 15 years ago that HTML code is available to the public, and meant to be available to the public, and indeed that users in some circumstances are legally required to examine a website's HTML code. It is not the kind of private restricted computer or network content that is protected by hacking laws."

The key issue regarding the application of the federal hacking law – the Computer Fraud and Abuse Act – is whether computer access was “unauthorized” or “beyond the scope of authorization.”

This past spring, the U.S. Supreme Court refused to apply the federal hacking law to a Georgia police sergeant who improperly received \$5,000 for running a license plate check for a friend who was trying to determine if a woman he had met was an undercover officer.

Justice Amy Coney Barrett said that applying the law to such a case would attach criminal penalties to a “breathtaking amount of commonplace computer activity” – such as employees using work computers for personal emails.

Barrett cited an amicus brief filed by the Reporters Committee for Freedom of the Press warning that a broad interpretation of the hacking law could hinder reporting based on whistleblowers and data analysis.

This “is especially concerning in the context of the press, where selective enforcement could be motivated by a government official’s disagreement or dislike of the substance of the journalism,” the brief said.

That is exactly what appears to be the case with Parson. He didn’t like the Post-Dispatch disclosing that the state hadn’t protected teachers’ private data. He even ignored the FBI, which told the state the incident was “not an actual network intrusion.”

The Highway Patrol has finished its investigation and turned it over to Cole County Prosecuting Attorney Locke Thompson, a Republican who previously worked in the state Attorney General’s office. Parson said at a Dec. 29 press conference that he expects Thompson to pursue the case.

“If somebody picks your lock on your house...,” he said, “they

do not have the right to go into your house and take anything that belongs to you.”

A better analogy, say media lawyers, would be a good Samaritan walking past your house and noticing the door is open with valuable possessions in view who then warns you about the danger.

The danger here is a duly elected governor retaliating against a reporter for disclosing the truth.

Editor's note: A version of this column ran in the Washington Post in January before a prosecutor decided not to pursue criminal charges

William H. Freivogel is publisher of the Gateway Journalism Review, a former Post-Dispatch editor, a journalism professor at Southern Illinois University and a member of the Missouri Bar.