Data Privacy Detective Podcast – Episode 26 – How safe is the personal data you provide to state governments?

Aug 14, 2018

Categories:

Podcast
Publications

Authors:

Joseph J. Dehner
Trey Grayson

Because U.S. states employ over 16 million people and hold the data of almost all American residents, state governments are major targets for data villains seeking to obtain data about us. How safe is our personal information in the hands of state governments and what security challenges must states address to better protect personal data?

Podcast guest Trey Grayson is a veteran of these issues, having served as Kentucky's Secretary of State for eight years and later as director of Harvard's Kennedy School of Government's Institute of Politics and member of the President's Commission on Election Administration, which reviewed the 2012 election. Trey is now a principal of the public policy firm CivicPoint and an attorney with Frost Brown Todd LLC. As an attorney and public policy expert, Trey offers guidance on the state of cybersecurity and state-held data in episode 26 of the Data Privacy Detective podcast.

One alarming finding from Microsoft's July 2018 report, "From Policy to Practice: Strengthening Cybersecurity in State Governments," is that only 18 states require cybersecurity training of their personnel, despite the well-established fact that people are usually the weakest link in a data protection regimen. According to Trey Grayson, however, most states have greatly enhanced their cybersecurity practices in recent years, and while efforts to disrupt voting systems in 2016 (including by the Russian Government) are well-documented, no major breach of election data resulted. One explanation for this might be the U.S. election system's diffusion of responsibility for voting systems. No single, overriding federal system exists; states and counties have their own individual systems for elections, making it difficult for election villains to launch a coordinated attack. If this is a strength of the current

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

system, it is also a weakness in that many counties and states lack sufficient resources to achieve a high level of data security.

Still, voting information is only a fraction of the vast amounts of data state governments have on us. In addition to party affiliation, voting history, and the names and addresses of registered voters, states also receive sensitive medical and financial details for a wide variety of purposes, including Medicaid, taxes, driver license registration, business licenses, and many other functions. Given the scope of this information, states have taken steps to protect from public view certain categories of individuals who may be unfairly targeted if their election history and other personal details are made public (e.g., judges, medical professionals, officeholders). But these protections do not extend to everyone else. For individuals who want to shield their personal data for similar reasons, the onus is on them to take action to achieve this.

Trey Grayson agrees with Microsoft's recommendation that all state governments adopt comprehensive, risk-based cybersecurity frameworks modeled on the Cybersecurity Framework of the National Institute of Standards and Technology (NIST).

The Microsoft report makes recommendations for state governments, starting with a grounding in NIST standards and adding the following:

- Establish an ongoing cybersecurity advisory council with industry and academia.
- Create a culture of cybersecurity.
- Leverage new resources to enhance election integrity.
- Integrate cyber resilience into every step of strategic planning.
- Consider cyber insurance to help protect state assets.
- Strong procurement policies and compliance are essential.

Since the early days, when there was a rush to digitize and publicize information, state governments have made considerable progress in protecting personal data and today generally avoid such mistakes as posting Social Security and other data without masking sensitive details within documents that are otherwise made public. Even so,

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

additional funding and cybersecurity upgrades are essential to preserve and bolster the public's confidence in elections and in the government's ability to strike a proper balance between transparency, on the one hand, and respect for the privacy of personal data, on the other.

For more information, please contact Joe Dehner, Trey Grayson, or any attorney in Frost Brown Todd's Privacy and Information Security Law Industry Group.

To share your thoughts or questions about this or other Data Privacy Detective podcasts, send a message to info@thedataprivacydetective.com. And remember – protecting your personal information begins with you.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons