

Tom Still: Federal rules on data privacy make more sense than state-by-state laws

Posted on Thursday, Jan 16, 2020

The column below reflects the views of the author, and these opinions are neither endorsed nor supported by WisOpinion.com.

MADISON, Wis. – After decades of willingly sharing their personal information online, sometimes with people, companies and groups they don't even know, most Americans think it's time to regain a measure of control.

Aside from the fact it would be impossible to jam the digital genie back into the lamp, that's an entirely justifiable reaction. Data breaches have become commonplace (billions of records were potentially exposed in 2019 alone) and people worry about losing financial, health and other personal data to hackers who are intent on harm.

It is no longer a question of whether people deserve to be assured their personal data is safe or unavailable for auction. It's a question of how the goal of achieving "data privacy" is best accomplished.

>> WisPolitics is now on the State Affairs network. Get custom keyword notifications, bill tracking and all WisPolitics content. [Get the app or access via desktop.](#)

The California Consumer Privacy Act took effect this month, creating rights to access personal data from a range of companies, such as ride-hailing services, cable television companies, mobile communications firms, retailers and more. The law also comes with a right to delete personal data and to opt out of the sale of data, which some companies with huge databases do routinely but others do not.

The law exempts companies that fall below a \$25-million annual revenue threshold or process fewer than 50,000 consumer records per year, but it has nonetheless

created compliance confusion for many companies and institutions – not to mention consumers themselves. The California attorney general has yet to publish interpretative regulations.

Multiply the California law times 49 other states and the result may well be economic bedlam as companies that collect data for any reason – including health records designed to be “portable” so that people get better care – struggle to comply with a maze of regulations.

Legislatures in at least six other states, including Wisconsin, may soon consider data privacy laws. A far better approach would be federal regulation creating a unified set of expectations that won’t inhibit interstate commerce or otherwise put U.S. companies and data sources at a competitive disadvantage.

The European Union’s General Data Protection Regulation, known by the acronym GDPR, is the best-known example of a widely applied data privacy law. Other countries such as Brazil, New Zealand and India have also taken a national approach to how personal data can be collected, stored, used and transmitted.

In an age of political gridlock, however, can Congress pass a bipartisan data privacy package? The answer is a lot closer to “yes” than one might think.

Late in 2019, two U.S. senators circulated largely similar bills on data privacy. U.S. Sen. Maria Cantwell, D-Wash., introduced the Consumer Online Privacy Act and U.S. Sen. Roger Wicker, R-Miss., put forth the U.S. Consumer Data Privacy Act. Both bills borrow provisions of the California law related to consumers’ rights over their data and the duties of companies to inform consumers of those rights. One major difference between the bills is whether the federal law would automatically pre-empt all state laws, or only in areas of direct conflict.

A federal approach would also work with regulations already in place, while a state-by-state patchwork would run the risk of contradicting them. Existing federal rules include the Health Insurance Portability and Accountability Act, known commonly as HIPAA, which protects personal health information. The federal Fair Credit Reporting Act oversees the collection and use of certain consumer information. Other existing regulations apply to data regarding students and children.

Enduring data privacy relies in part on consumers thinking through their own online habits, as well as companies adopting a culture of respect for the identifiable data

they collect. It also makes sense to have national rules that encourage continued innovation while protecting people in whatever state they call home.

— *Still is president of the Wisconsin Technology Council. He can be reached at tstill@wisconsintechcouncil.com.*