An uptick in concern about digital privacy is sweeping the nation. Incidents such as injury law firm advertisements targeting emergency room patients based on location, smart home assistants recording conversations unbeknown to their owners, and Facebook’s Cambridge Analytica scandal have all contributed to concerns about digital privacy.

Federally, S.2728 or the Social Media Privacy Protection and Consumer Rights Act of 2018, was introduced on April 23. The bill addresses company transparency and outlines consequences of inappropriate data collection. The bill also increases state responsibility for enforcement by authorizing state attorneys general to pursue and investigate complaints regarding violations of the law as civil actions.

While data privacy is regulated at the federal level, states also have jurisdiction over what occurs within their boundaries regarding data collection. In California, citizens are attempting to bring The California Consumer Privacy Act to the November ballot. Listed in the bill are regulations regarding the rights of consumers and their children about the knowledge and purpose of data collected by businesses; requirements of equal pricing and non-discriminatory practices upon an inquiry regarding personal data for companies; and requirements of notification if personal data has been sold, breached or compromised.

Minnesota (325M.01 to 0.9) and Nevada (205.498) have laws regarding Internet Service Providers to keep information concerning their customer private unless otherwise agreed to by the individual. Indirectly, California (1798.83) and Utah (13-37-201 to -203) govern the types of personal information businesses share or sell to a third party for marketing purposes or for direct compensation. The laws require written notice of the data’s use to the consumer.

The issue of digital privacy extends beyond state and national borders and the European Union recently took action by revamping the General Protection Data Regulation, or GDPR, to place extended regulations on companies processing personal data. The GDPR was originally adopted in 2016 and placed regulations on corporate use of personal data to target unknowing consumers. The extended regulations require consent, breach notification, right to access personal data that has been collected, right to be forgotten or removed from the system, increased data portability, and the establishment of data protection officers for companies that collect data.

Most states already have established consumer protection and privacy laws however, they are widely considered to be out of date regarding social media, technology and new innovations. As technology continues to change, states will be working to provide additional protection for their citizens by expanding laws to include policies like the EU and the California Consumer Privacy Act.