

## Consumer Data Protection Laws in the State of Mongo

Data protection and privacy as well as user privacy has become an increasingly vital concern in today's digital age, especially considering that almost every single website and service has you signing up for an account to store your legal name, home address, phone number, email address, and even credit card information. It is imperative to users rights for companies that collect this data to protect it from unauthorized or malicious access that could be used to harm said users, and to only collect what data is necessary in order to reduce the magnitude of breaches. Now that cell phones have progressed to such a state that the companies that provide them store biometric data such a facial scans and fingerprints, the range of personally identifiable information, or PII, has increased in both severity to the user and in the protections needed to properly safeguard said data from bad actors.

There are a litany of laws around the world that govern how companies collect and use your data. In the United States, we have several landmark federal laws that control the usage of PII. The first example is the Privacy Act of 1974, which dictates a baseline for how federal agencies store, transfer, disseminate, and access personal information – this act also applies to some companies such as federal contractors, that expressly work with or on behalf of federal agencies in the United States<sup>[2]</sup>. Another example is the Federal Trade Commission Act, or FTCA, which attempts to control the use of deceptive marketing practices intending to obtain PII. Examples of this are phishing emails, where bad actors pose as companies that do not represent them while requesting consumer information ranging from email addresses and passwords to social security numbers and credit card info. The FTCA punishes said actors by applying fines and, in more extreme cases, jail time for those who maliciously and deceptively seek to acquire PII. This act can also be used in cases of consumer unfairness, such as coercing customers to buy defective products on credit without the information and ability necessary for them to assert creditor claims and properly defend themselves as creditors<sup>[3]</sup>. Lastly, and arguably the most important of the examples written here, is the Health Insurance Portability and Accountability Act of 1996, also known as HIPAA. This piece of legislature was created with the express purpose to create a guideline of standards for the privacy, security, and exchange of citizens' medical and health information. HIPAA dictates that any Protected Health Information, or PHI, whether in electronic, paper, or oral form, is to be limited in the scope of its disclosure only to covered entities. Said entities cannot disclose this information without express permission from the subject of said information, typically in the form of a Release of Information, or ROI<sup>[4]</sup>. An ROI allows an individuals healthcare provider to share their PHI with a specific person or organization, and said individual can also specify how long the data is to be released and under what circumstances it can be used and shared at will. PHI ranges anywhere from mental health status or conditions to the provisions of an individuals healthcare to payment information relating to any medical care. The specific inclusion of the individual in both the awareness of what's happening with their information and who has access to it at any given time is crucial to respecting citizens right to privacy.

I think that the state of Mongo should pursue legislature that prevents the unauthorized sale and distribution of any given website or services' PII that it collects on a user. Since federal law already dictates that a citizen is entitled to the privacy and transparency of PII collected and used by federal agencies and healthcare providers, it's only fair that some standard should be applied to those who collect everyday data on their customers, such as news websites that sell data to advertisers. A model to base such a law off of would be Virginia's Personal Information Privacy Act, which instates the limitations I talked about earlier plus some others, including HIPAA-like limits regarding the digitization of other personally identifiable documents such as drivers licenses – exceptions to that rule would be information that's necessary for purchase or transactions with third parties<sup>[5]</sup>. While the benefits to the citizens of the state of Mongo would be immense, and it would increase our citizens trust in our institutions and their mission statement of keeping our citizens safe, laws that limit corporate freedoms in this way make businesses harder to monetize. In an ever-evolving digital landscape, advertisers are the key to making any given platform or website financially viable – without the sale of personalized user data, smaller businesses in particular would face many issues when it comes to serving users advertisements that they would click on and therefore earn money for the company through. By enforcing these types of laws properly, the state would also have to hire on designated Cybersecurity literate staff to handle these cases before they're passed off to the judiciary, increasing the amount of money our citizens would have to spend on taxes. Despite these trade-offs, I think that more consumer protections are better for our state – our citizens have inalienable rights to privacy, and creating state laws similar to Virginia's PIPA only serve to strengthen the electorate's faith in our institutions and our willingness to protect and provide full transparency into how their data is being treated.

Works Cited

1. <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279>
2. [https://www.ftc.gov/system/files/documents/public\\_statements/410531/831014deceptionstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf)
3. <https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness>
4. <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
5. <https://law.lis.virginia.gov/vacodepopularnames/personal-information-privacy-act/#:~:text=A.,the%20merchant's%20place%20of%20business.>