**Annotated Bibliography**

Mariska Suparman. (2023). The Constitution: A Blueprint for American Data Privacy Law. *Widener Law Review*, *29*(1), 71–96.

Mariska reports on the growing concern of data privacy and protection, commenting on the current state of affairs, who is affected, and giving a possible roadmap of how things could be improved using precedence set in different jurisdictions own legislation such as the EU’s GDPR. Mariska explores the consequences of poor data management regarding privacy, its use cases for discrimination and identity theft, and consent of being tracked and collected data being disposed of.

MCNERNEY, B. (2022). Keep Your Fingerprints to Yourself: New York Needs a Biometric Privacy Law. St. John’s Law Review, 96(4), 1039–1070.

Mcnerney reports on the rise of biometric identification technology and its wide amount of use cases that have been popping up in recent years. He comments on the consequences of not properly managing peoples biometric data stating the failures of current biometric technologies in correctly identifying individuals, the risk to individuals who trust these companies to store their biometric data when there is a breach, and the current legislation around data privacy and protection and biometric privacy that individual states have put into action, their effectiveness, and where they could be improved and areas that still need to be addressed.

**Annotated Bibliography**

Pinto, G. P., Donta, P. K., Dustdar, S., & Prazeres, C. (2024). A Systematic Review on Privacy- Aware IoT Personal Data Stores. *Sensors (14248220)*, *24*(7), 2197. https://doi- org.proxy.lib.odu.edu/10.3390/s24072197

Pinto reports on rapid digitalization of lives in every sector globally and the massive amount of wealth large corporations such as Google and Facebook have been able to acquire thanks to data farming even without consent. Pinto then goes on to explain that this has allowed for a more rapid growth of the IoT and gave the data to make technologies more convenient but argues it should not be at the price of privacy. Pinto then conducts research on current state of privacy protection solutions for IoT enabled devices and their ecosystems and their effectiveness. Pinto explores possible security monitoring solutions that can be implemented within IoT or have already been implemented and what their proven effectiveness is so far. Pinto finishes with critiques of each security device and current threats and failings within the industry.

Simons, E. (2021). Putting a Finger on Biometric Privacy Laws: HOW CONGRESS CAN STITCH TOGETHER THE PATCHWORK OF BIOMETRIC PRIVACY LAWS IN THE UNITED STATES. *Brooklyn Law Review*, *86*(3), 1097–1134.

Simons reports on biometric identification technology’s market growth and shortcuts that have been taken to achieve such widespread use. Simons talks about the different ways biometric technologies have been defeated and how easily people can misplace their trust in biometric identification to keep their data safe. Simons then goes to break down the 4 areas of biometric privacy laws being federal privacy, state privacy, state biometric privacy, and federal biometric privacy. Simons concludes that there is precedence for a biometric privacy legislation roadmap in other sectors such as HIPAA and some states and legislative unions outside the US have also already implemented privacy laws that could inspire a federal biometric privacy law.