To: Governor Tar-Míriel

From: Jessica Ali

Subject: Overview of Privacy & Data Protection with Recommendations

Date: 13 MAR 2023

Data privacy is often called information privacy and is one "area of data protection that concerns the proper handling of sensitive data," such as PII. When considering the definition of data privacy, it is essential to note that "data privacy is not data security" are two different conversations (*What Is Data Privacy? | SNIA*, n.d.). Data security protects against hackers, whereas data privacy "governs how the data is collected, shared, and used" (*What Is Data Privacy? | SNIA*, n.d.). To further the conversation, we will discuss data privacy and the growing concerns of misuse of PII for profit in the private sector. An increasing number of American citizens are concerned with the "sale of personal data" and the readability of the terms and conditions clauses (*Bill Resource*, n.d.). One example we can draw when creating our bill is the state of Connecticut's Public Act N. 22-15, AN Act Concerning Personal Data Privacy and Online Monitoring. The principal value in introducing such a bill at a state level focuses not only on the American citizen as part of the collective but also on an individualized level. Where data concerns range from a faith-based collection of data to the economic value our state puts forth for the collective in future projects. In sum, our form needs to trust that we have their best interest in mind in an increasingly competing digital age where ads are being tailored more from person to person versus the collective. A key area in tailoring a more personal digital age is using biometric data and PII as identifiers in the private sector.

The California Consumer Privacy Act of 2018 provides “consumers [to] request that a business delete personal information that the business collected” (*State Laws Related to Digital Privacy*, 2022) as a great starting point for our draft and the U.S Department of Labor outlines PII as “any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means ."A typical PII example is a social security number. However, more importantly, in our current Digital Age, in 2016 Breyer v. Germany, the Court of Justice of the European Union ruled IP addresses "can be considered PII- in certain circumstances" the important takeaway is the circumstances where consumer data is tailored for ads and revenue of a company, an IP then becomes PII (2022). Another example of essential data to persons is biometric data for personalized advertising. The GDPR defines them as "personal data resulting from specific technical processing relating to the physical, physiological or [behavioral] characteristics of a natural person, which allow or confirm the unique identification of that natural person” (ICO, n.d.). One example found more often than not in the private advertising sector is facial recognition and the use of facial identifiers to collect emotions. For example, if a person views their phone and reacts to an ad, the company then stores the reaction for future use to tailor ads to increase a positive response amongst said, person or future groups.

Amongst these groups is a growing concern about the readability of permissions for the above collection of facial recognition and PII. Therefore suggestions for our foundation include a push to create TOCs at a general reader level language, shortened TOCs, more accountability in the private business sector for biometric data collection, and more regulation of third-party sales

of such data. Such examples of practical solutions are outlined in the GDPR or the General Data Protection under the European Union, which is seen as one of the "toughest privacy…law in the world" and applies to all persons, even those not in the European Union (Wolford, 2022). A logical and insightful foundation for us moving forward is to focus on the data production principles outlined in the GDPR as follows: "lawfulness, fairness and transparency" when processing data such as explicit permissions in the TOS concerning the "data minimization, accuracy, storage limitation, integrity and confidently" all while being accountable as a "data controller" regarding the above principles (Wolford, 2022). One example in the state of Virginia has similar parallels with the GDPR's regulations, such as the deletion of data by the data controller.

To close, we should push for data privacy protection at a state level to ensure trust between ourselves and our citizens in a growing private digital age concerning the GDPR and state laws already enacted, such as in Connecticut, California, and Virginia. The consequences of not entering the conversation with reliable solutions for our citizens may economically impact our state and leave room for privatized entities to take advantage of our citizens.

References

B. (2022, May 12). *Is an IP address PII? The answer is nuanced.* BlueCat Networks. Retrieved From https://bluecatnetworks.com/blog/is-an-ip-address-pii-the-answer-is-nuanced/.

Bill Resource. (n.d.). Retrieved From https://custom.statenet.com/public/resources.cgi?id=ID:bill:CT2022000S6.

Guidance on the Protection of Personal Identifiable Information. (n.d.). Retrieved From DOL. https://www.dol.gov/general/ppii

ICO. (n.d.). *What is special category data?* Retrieved From https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/.

State Laws Related to Digital Privacy. (n.d.). Retrieved From https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy.

What is Data Privacy? | SNIA. (n.d.). Retrieved From https://www.snia.org/education/what-is-data-privacy.

Wolford, B. (2022, May 26). *What is GDPR, the EU's new data protection law?* GDPR.eu. Retrieved From https://gdpr.eu/what-is-gdpr/.