CYSE406 Cyber Law

21 March 2023

PRIVACY POLICY GUIDANCE MEMORANDUM

By

Alan Schneider

Memorandum Number: 2023-1

MEMORANDUM FOR: DISTRIBUTION

FROM: Alan Schneider Chief Privacy Officer

SUBJECT: Mongo State Privacy Policy Recommendations Regarding Collection, Use, Retention, and Dissemination of Information on Mongo State Citizens by federal and commercial entities.

I. PURPOSE

This memorandum provides information on current federal and state regulations regarding privacy protections afforded to U.S. persons for information collected, used, retained, and/or disseminated by federal or commercial entities. Further it will provide privacy policy recommendations to the office of the governor for consideration and introduction into state law.

II. BACKGROUND

Informational privacy or more specifically Data privacy is the the ability of a person to decide to what extent, when and how personal information about them is collected and disseminated to others. It can consist of an individual’s name, location, contact information, online or real-world behavior. When used individually or combined with other information that is linked or is linkable to an individual, personal Information can be used to distinguish or trace an individual's identity. Coupled with increasingly sophisticated data collection and aggregation tools utilized by government, commercial and criminal entities. This can effectively limit individual ability to control the degree and amount of private information that is readily accessible to these entities.

With that in mind, consideration must also be paid to issues of consumer data protection, where government and commercial entities data protection and notification safeguards may be inadequate to shield the data collected. Resulting in an increased number of data breaches and cyberattacks by entities who realize the value of this information. These types of compromises contribute to third order order effects like criminal fraud and harassment of users, personal data being sold to outside parties without user consent and potential limiting effects on constitutionally protected speech considering intrusive tracking and monitoring of social media and other forms of digital communication.

III. Definitions and Examples of personal data

1. Personally Identifiable Information (PII)
   This is information that, when used alone or with other relevant data, can identify an individual. PII may contains stand-alone data (passport information) that can identify a person uniquely, or partial data (race) that can be combined with other partial data (date of birth) to successfully recognize an individual. PII is further broken down into two categories. Sensitive and non-sensitive.

   a. Sensitive PII (SPII) contains information "which if lost, compromised or disclosed without authorization could result in substantial harm, embarrassment, inconvenience or unfairness to an individual." (1)
      Examples of SPII: Full name, social security number, driver's license, mailing address, credit card information, passport information, financial and medical records
   b. Non-Sensitive PII. Contains information readily accessible from public sources, like phonebooks, the internet. While not able to directly identify an individual, it might be aggregated with other information to identify an individual.
      Examples of non-sensitive PII: zip code, race, gender, date of birth, place of birth, religion.

2. Biometric data.
   This is data that describes and classifies measurable physical properties inherent in the human body to identify individuals.
   Examples of Biometric data: fingerprints, hand geometry, facial recognition, voice, iris, retina, ear shape, walking gait, DNA, palm print or finger vein patterns

3. Protected/ Personal Health Information (PHI)
   Contains data related to any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

III Federal privacy protections

1. The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. From which information is retrieved by the name of the individual or by some identifier assigned to the individual.

2. Health Insurance Portability and Accountability Act (HIPAA) establishes a national standard to protect individuals' medical records and other personal health information. Safeguarding protected health information (PHI). The HIPAA Privacy Rule protects individual's rights to their health information, copies of their records and their right to have medical information corrected. This act applies to, health plans, health care clearinghouses, and health care providers.

3. Gramm-Leach-Bliley Act (GLBA)
   The Gramm-Leach-Bliley Act: “Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.” (2)

4. Fair Credit reporting Act protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services. Information in a consumer report cannot be provided to anyone who does not have a purpose specified in the Act. Companies that provide information to consumer reporting agencies also have specific legal obligations, including the duty to investigate disputed information. (3)

5. Childrens Online Privacy Protection Act (15 U.S.C. 6501, et seq.,) prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children under the age of 13 on the Internet. (4)

6. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) Protects the privacy of student education records. It applies to any school that receive funds under U.S. Department of Education programs. (5)

7. Genetic Information Nondiscrimination Act (GINA) Prohibits discrimination against individuals based on their personal genetic information, as it applies to health insurance and employment. (6)

IV State privacy laws not covered by federal statutes.

1. Illinois Biometric Information Privacy Act. (BIPA) Establishes standards for companies’ collection, processing and dissemination of Illinois consumers biometric data. Requires written consent for collection of biometric data. Directs companies to notify individuals what biometric data is being stored or collected, the length of time and specific purposes for which the data is being collected and used.

V. Foreign privacy protections relevant to following policy recommendations.

1. The General Data Protection Regulation is a European Union law that requires any organization that collects, processes or disseminates personal data to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. It also regulates the exportation of personal data outside the EU. The regulation enumerates seven principles of data protection and eight privacy rights that must implemented by any organization operating within the EU, as well as any outside of the EU which offer goods or services to customers or businesses in the EU. It also empowers member state data protection authorities to enforce the GDPR with sanctions and fines up to €20 million or 4% of global revenue, whichever is higher. Authorities can also issue sanctions, such as bans on data processing or public reprimands.

V. Policy recommendations

Exploration of elements of the EU's General Data Protection regulation as implemented into state law, may fill privacy protection gaps left by overly narrow or ambiguous federal legislation. The scope of the regulations should apply to any organization within mongo state or outside mongo state that offers goods or services to customers within mongo. With direction on collection, processing and storage and protection of personal data under seven key guidelines and enumerating eight individual privacy rights.

A. Guidelines

1. The data was collected lawfully, with the express consent of the individual.
2. Limited in purpose. The data is collected for specified, explicit and legitimate purposes. Clearly communicated to individuals through notification.
3. Limited in scope. Only the smallest amount of data may be collected to comply with the collection purpose.
4. It must be accurate. With checks and balances to update, correct or erase incorrect or incomplete data, with regular audits to ensure data integrity.
5. Limited data retention. Limit the length of time data is stored and required anonymization of data not actively used.
6. Maintain integrity and confidentiality of the data collected, safeguarding it from internal and external threats and exposure.
7. Accountability. Maintain appropriate measure and records as proof of compliance, that can be produced at any time for regulatory authorities.

B. Privacy rights

1. Individual right to be informed about the collection and use of personal data.
2. Right to access personal data: confirmation that your data is being processed.
3. Right to have inaccurate personal data corrected or complected if it is not complete.
4. Right to erasure of personal data (to be forgotten.)
5. Right to restrict or object to processing in certain circumstances
6. Data portability, allowing the data subject to secure and reuse personal data for their own purposes on different services.
7. Rights where electronic systems use personal information to make decisions without human intervention.
8. Right to withdraw consent to have personal data collected at any time.

VI. Additional Comments.

Specific language must be added to any potential legislation prohibiting organizations from using Terms of service to make consent for data collection a requirement for use of their goods or services. As well ensuring that biometric information as detailed in Illinois Biometric Information Privacy Act is specifically enumerated in the policy guidelines above or adopted as a separated and distinct regulation. Further it is recognized that the reach of enforcement for EU privacy authorities vs potential state privacy regulation is greater and the state will likely encounter difficulty with the transnational nature of potential violations, it is then suggested that within applicable federal guidelines that partnership agreements to share information and provide support as it relates to privacy violations should be developed.

Works Cited

1. Sensitive personally identifiable information (SPII). Virginia Information Technologies Agency. (n.d.). Retrieved March 23, 2023, from https://www.vita.virginia.gov/policy--governance/glossary/cov-itrm-glossary/s/sensitive-personally-identifiable-information-spii.html

2. Staff, the Premerger Notification Office, and The FTC Office of Technology. "Gramm-Leach-Bliley Act." Federal Trade Commission, 16 Feb. 2023, www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

3. "Fair Credit Reporting Act", www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

4. Children's Online Privacy Protection Rule (COPPA), www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

5. "Family Educational Rights and Privacy Act (FERPA)." Home, US Department of Education (ED), 25 Aug. 2021, www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

6. Genetic Information Nondiscrimination Act (GINA) GovInfo, www.govinfo.gov/app/details/PLAW-110publ233.

7. Biometric Information Privacy Act., www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.