King & Spalding
Client Alert

MAY 30, 2019

For more information, contact:

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

William Johnson
+1 212 556 2125
wjohnson@kslaw.com

Michael Hollander
+1 212 556 2377
mhollander@kslaw.com

King & Spalding

New York
1185 Avenue of the Americas
New York, New York 10036-4003
Tel: +1 212 556 2100

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Broad Consumer Privacy Bill Introduced In New York State Senate

New York's State Senate is considering a bill that would impose sweeping new requirements upon companies that collect and process consumer data, including a fiduciary-like duty to protect such data. On May 9, 2019, New York State Senator Kevin Thomas introduced S. 5642, the New York Privacy Act ("NYPA"), which has been referred to the New York State Senate Consumer Protection Committee.[1] If enacted, the NYPA will roll out strict rules for the collection, use, control, processing, and transfer of data by entities that conduct business in New York or produce products or services intentionally targeted at New York residents.[2]

Of particular interest is the NYPA's proposed definition of "personal data," which references a whole host of data points including mother's maiden name, records of personal property, biometric information, internet search history, certain education records, and even thermal and olfactory data.[3] Similar to the sweeping definition of personal data provided by the California Consumer Privacy Act of 2018 ("CCPA"),[4] the NYPA's definition of "personal data" also includes a catch-all for "inference[s] drawn from any of the information described in [the NYPA's definition of personal data] to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, preferences [sic], predispositions, behavior, attitudes, intelligence, abilities, or aptitudes."[5] The bill also contains a provision that would create a private right of action for consumers to sue companies for violations of the law and seek injunctive and compensatory relief.

If the bill becomes law, in order for an entity to collect, use, process, or transfer a consumer's personal data, the entity would first need to obtain affirmative, express and documented consent.[6] The entity would also need to "exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk" and "act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances."[7] The

imposition of this fiduciary-like duty is a significant change in the level of care required by companies that collect, process, use and transfer consumer data, as it effectively requires companies to place the privacy of consumer data over the company's own livelihood, and attempts to supersede a company's fiduciary duties to owners or shareholders.

SUMMARY OF THE PROPOSED NYPA

The proposed NYPA has eleven provisions.[8]

- **§ 1100 – Definitions**
    - This section contains several notable definitions of "personal data," "consent," "consumer," "process or processing," "profiling," and "opt-in."
- **§ 1101 – Jurisdictional Scope**
    - The NYPA would only apply to entities that conduct business in New York or produce products or services intentionally targeted at New York residents. The NYPA does not address what constitutes "intentional targeting" nor does it apply to state or local governments, data regulated by HIPAA or HITECH, or employment record data.
- **§ 1102 – Data Fiduciary**
    - In order to use, process, or transfer personal data, an entity will need to obtain express and documented consent of the consumer. The entity will also need to "exercise the duty of care, loyalty, and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller, or data broker, in a manner expected by a reasonable consumer under the circumstances."
    - The bill defines "privacy risk" as "potential adverse consequences to consumers and society" including monetary loss, physical harm, psychological harm, anxiety, embarrassment, fear, significant inconvenience or time, reputational harm, and even consequences affecting private family matters.
- **§ 1103 – Consumer Rights**
    - Entities subject to the proposed law would be required to provide notice to consumers of their rights under the law, along with an opportunity to opt-in or opt-out that clearly indicates the consumer's consent or lack thereof.
    - The entity must also be capable of processing consumer requests relating to their personal data, including whether personal data is being processed, who is processing personal data (i.e., data sold to data brokers), correction of inaccurate or incomplete personal data, deletion of personal data under certain circumstances, restriction of processing of personal data, and copies of personal data.
- **§ 1104 – Transparency**
    - Data controllers must make a privacy notice freely available, which includes the categories of personal data collected, the categories of personal data shared with any third-parties, the purposes for use and disclosure to any third-parties, the names and categories of third-parties with whom personal data is shared, and any consumer rights.

  - Further, data controllers that engage in any profiling and direct marketing activities involving consumers' personal data must provide notice to consumers of such activities at or before the time the data is obtained.

- **§ 1105 – Responsibility According to Role**
  - Processors must adhere to contractually-defined instructions set by controllers.
- **§ 1106 – De-Identified Data**
  - Controllers and processors who use de-identified data need to ensure this type of data is not being used inappropriately or illegally.
- **§ 1107 – Exemptions**
  - Obligations imposed on controllers and processors may not apply in certain circumstances, such as legal and regulatory compliance, cooperation with law enforcement agencies, and prevention or detection of identity theft.
- **§ 1108 – Liability**
  - If more than one controller and/or processor violate the NYPA, liability will be allocated based on comparative fault, unless otherwise agreed to by contract.
- **§ 1109 – Government Enforcement and Private Right of Action**
  - Violations of the NYPA are considered unfair or deceptive acts in trade or commerce and unfair methods of competition with respect to Article 22-A (Consumer Protection from Deceptive Acts and Practices) of the New York General Business Laws.
  - Of particular importance, in addition to authorizing the New York State Attorney General to bring an action on behalf of the state or its residents, the bill also establishes a private right of action for consumers to sue companies and seek injunctive relief and compensatory damages, in addition to reasonable attorney's fees. Entities are also subject to a civil penalty. "When calculating damages and civil penalties, the court shall consider the number of affected individuals, the severity of the violation, and the size and revenues of the covered entity." Under the proposed bill, each victim is a separate violation, as is each provision violated.
- **§ 1110 – Preemption**
  - The NYPA will preempt any local law pertaining to processing of personal data by controllers or processors.

TAKEAWAYS

If enacted, the NYPA would challenge most businesses, especially those with modest IT budgets. The bill, in its current form, will require businesses to track and correlate nearly every data point that can be mapped to a known consumer, including inferences drawn by the business based on those data points. Although not insurmountable, it is certainly a heavy lift and businesses will need to develop an action plan in advance to remain compliant in a cost-effective manner. In addition, the new fiduciary-like duty would require companies to take a hard look at their information security and privacy programs to ensure that reasonable measures are in place to protect data that the companies collect, use, process, and transfer.

As this bill moves forward, companies that conduct business in New York or produce products or services intentionally targeted at New York residents would be wise to take the following actions:

- **Map out data flows** to identify (i) all data points retained by the organization that are considered "personal data" by the NYPA, (ii) where the data originates, (iii) why the data exists, (iv) whether the data is being shared with anyone and for what purposes, and (v) whether the reason the data continues to be maintained is due to a legitimate business purpose or a legal reason.
- **Conduct an enterprise-wide risk assessment** to identify any vulnerabilities associated with data flows (including points of ingress and egress). Identify vulnerabilities to assess risk management and implement remedial safeguards, which will need to be addressed to fulfill the company's § 1102 fiduciary-like duty to secure personal data of a consumer against a privacy risk.
- **Re-assess communications with consumers** to address the potential new requirements under §§ 1103 and 1104, including protection of certain data points regarded as "personal data" under the NYPA, but not under current law; explicit opt-in and opt-out tracking; and requests to restrict processing of personal data.

Although the NYPA has only been introduced in one chamber of the New York legislature and has just been referred to the New York State Senate Consumer Protection Committee, the proposed legislation, if enacted in its current form, would impose significant new requirements on companies that collect, use, process, and transfer New York consumers' data. Particularly, if the fiduciary-like duties envisioned by the NYPA become law, companies will need to carefully evaluate their compliance. Only time will tell whether the stringent requirements of the NYPA are enacted or whether changes are made to the bill as it moves through New York's legislative process. Covered companies should follow those developments closely.

[1] S. 5642, 2019–20 Reg. Sess. (N.Y. 2019) ("NYPA") (available at https://legislation.nysenate.gov/pdf/bills/2019/S5642).
[2] *Id.* §§ 1101–02.
[3] *Id.* § 1100(10)(a).
[4] *See* Cal. Civ. Code § 1798.140(o)(1).
[5] NYPA § 1100(10)(a)(xii).
[6] *Id.* §§ 1100(17), 1103 (entities "shall provide consumers the opportunity to opt in or opt out of processing their personal data in such a manner that the consumer must select and clearly indicate their consent or denial of consent").
[7] *Id.* § 1102(1).
[8] There is a bit of overlap with the EU General Data Protection Regulation ("GDPR") and the CCPA. For example, all three regimes have rather broad definitions of personal data (*see* NYPA § 1100(10); GDPR Art. 4(1), 9; Cal. Civ. Code §§ 1798.140(o), 1798.145(c)–(f)); require technical safeguards to protect de-identified data from being re-identified (the NYPA contemplates use of legal, administrative, or contractual safeguards, as well) (*see* NYPA § 1100(6)(b)(iii); GDPR Art. 4(5) (GDPR refers to de-identification as pseudonymisation); Cal. Civ. Code §§ 1798.140(a), 1798.140(h), 1798.140(o), 1798.140(r), 1798.145(a)(5)); provide for a right to access personal data (*see* NYPA §§ 1103(1), (5); GDPR Art. 15; Cal. Civ. Code §§ 1798.100(d), 1798.110, 1798.115); provide for a right to delete personal data (*see* NYPA § 1103(3); GDPR Art. 17; Cal. Civ. Code § 1798.105); require privacy notices to be communicated to consumers (*see* NYPA § 1104(1); GDPR Art. 13–14; Cal. Civ. Code §§ 1798.100(a)–(b), 1798.105(b), 1798.110, 1798.115, 1798.120(b), 1798.130, 1798.135); and provide for both state/administrative actions and a private right of action for violations (*see* NYPA §§ 1109(2), (3); GDPR Art. 82–84; Cal. Civ. Code §§ 1798.150, 1798.155).