

Cybersecurity

An ALM Publication

WWW.NYLJ.COM

VOLUME 263—NO. 40

MONDAY, MARCH 2, 2020

Implications of the ‘Data Fiduciary’ Provision in the Proposed New York Privacy Act

BY JOSEPH V. DEMARCO

The proposed New York Privacy Act (NYPA), currently pending before the state legislature, could significantly contribute to the trend of stronger state data privacy laws appearing nationwide. While it has many core elements of other recent state data privacy legislation, such as California’s Consumer Privacy Act (CCPA), New York’s proposed law, however, goes substantially further—and it does so in several novel respects. In particular, the NYPA has a provision creating the “data fiduciary,” by which entities collecting and controlling data would owe fiduciary duties to the individuals from which the data was collected (commonly referred to as data subjects). Under §1102 of the NYPA, these obligations would include “the duty of care, loyalty and confidentiality,” as well as

JOSEPH V. DEMARCO is a partner in the law firm of DeVore & DeMarco and a mediator and arbitrator with FedArb, resolving complex commercial and data privacy and security disputes between businesses.



SHUTTERSTOCK

the requirement to “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.” These provisions would establish standards of care that would shift the burden of protecting consumer information to business entities and other data collectors.

The NYPA’s provisions relating to data fiduciaries provide that fiduciary duties should be exercised to secure consumers against

“privacy risks.” This term is, however, defined quite broadly to include direct or indirect financial loss, physical harm, psychological harm, significant inconvenience or time expenditure, adverse employment outcomes, stigmatization or reputational harm, disruption and intrusion from unwanted commercial communication, price discrimination and others. This long list of privacy risks suggests that the proposed fiduciary duties would be meant to protect consumers in a wide variety of scenarios.

While the precise contours of NYPA's "data fiduciary" concept remain to be developed, the way traditional fiduciary duties have applied in New York might theoretically provide insight on how these obligations would play out in practice. Typically, fiduciary duties arise out of a relationship of trust and confidence between an agent and principal, or rather when one person is under a duty to act for or to give advice for the benefit of another regarding matters that are within the scope of the relation. While a finding of such a relationship is very fact-specific, it is grounded in a much higher level of trust than is normally present between persons involved in arm's length commercial transaction. Nonetheless, it is well-established under New York law that fiduciary duties can arise even in commercial transactions where one party reposed trust and confidence in another party who exercises discretionary functions for the party's benefit or possesses superior expertise on which the party relied. Indeed, this common law principle goes back centuries, underpinned by notions of equity and often arising between parties of unequal bargaining power. In New York, common examples of relationships with fiduciary duties include (1) an employee to the employer, (2) an attorney to the client, (3) a corporate officer or director to the corporation, (4) a member of a joint

venture to the rest of the members, and (5) co-authors of musical works to pick a few common examples.

Nor is the existence of a fiduciary duty an academic question. Fiduciary duties regularly require the person with the duty (the agent) to scrupulously act in a manner that benefits the other (the principal) and not themselves. Not surprisingly, these obligations are reflected in the NYPA's provisions that consumers should be protected above a business's own financial interests. The duty of confidentiality is essentially a duty to maintain in confidence all private information and knowledge entrusted to the agent, prohibiting disclosure without permission.

These provisions would establish **standards of care that would shift the burden** of protecting consumer information to business entities and other data collectors.

Traditionally, these duties govern many different practical situations. For example, fiduciary duties require an attorney to operate competently, avoid conflicts of interests, safeguard a client's property and honor the client's interests over their own. They would require a corporate director to exercise good faith and honest judgment to lawfully and legitimately further the corporation's interests—obligations which could be violated by paying oneself

excessive compensation, or misappropriating confidential and proprietary ideas, technology and business plans and providing the information to competitors. They could be violated by a shareholder withholding financial and other information from a fellow shareholder and forcing her out of the company, or by a health care provider disclosing personal patient information to others, even potentially a patient's spouse. Similarly, they would require an insurer to protect a consumer's confidential personal information, all provided in an application for life insurance.

Applying these common law principles, under the NYPA, data collectors and controllers would owe similar obligations to consumers from direct contractual relationships established through online interactions and transactions, even through routine online commercial transactions and standard website terms-of-service agreements. Yet the differences between traditional fiduciary relationships and the relationships between data collectors and data subjects—for example, an e-commerce merchant selling shoelaces—would undoubtedly raise numerous questions on how fiduciary obligations could be practically applied in that online context. Nor should this come as a surprise since there is an inherent tension between a company's interests in processing consumer data and a consumer's own privacy and financial

interests. This tension automatically arises from the inherent nature of the relationship since routine data collection practices allow companies to construct profiles on data subjects by capturing their online behaviors and preferences as part of the selling process. From this process, the more that companies seek to monetize these profiles, the more a consumer could be subjected to financial loss or other consequences derived from exploiting these consumer profiles.

Questions abound if a routine e-commerce transaction directly implicates fiduciary duties. Applying those duties in the context of online marketplaces, would a large online retailer, which tracks a user's purchases and shopping preferences have an obligation to ensure that the consumer is in fact getting the best price on a product? Under the duty of loyalty, which would require prioritizing the consumer's financial interests over the company's own interests, the company would theoretically need to inform the consumer if it was aware of the same product being sold at a more competitive price. Would a cloud service provider be obligated to inform a consumer of another service that provided faster processing speeds or more secure data storage if it was aware of even marginal deficiencies in its own service? Moving beyond these commercial contexts, the fiduciary obligations of a social media network would similarly raise interesting and

substantial questions. For example, if processing data from an individual's Facebook account gave a company information on the individual's personality traits or physical and mental well-being, how far would the data collector have to go in order to protect the individual from physical or psychological harm? Would it create any obligation on the part of the platform or provider to protect the individual from manipulation, fear, or psychological distress generated by targeted advertising on sensitive political or social issues? These duties would admittedly lead to some extreme obligations that would conflict with numerous other obligations, and even fundamental rights, of companies controlling data.

The vast implications of the NYPA, in applying fiduciary duties to data controllers, are further amplified by the provision that these fiduciary duties would "supersede any duty owed to [affiliated] owners or shareholders" of the legal entity. This would presumably require data controllers to prioritize the fiduciary duties owed to the data subjects over the traditional fiduciary duties owed to their own company and its shareholders and investors. The implications of the data fiduciary provision are extended even further as the NYPA creates a private right of action, so that private individuals could bring civil lawsuits alleging violations potentially over all the previously mentioned circumstances.

Moreover, the reach of the NYPA is extremely broad, covering most companies that conduct business in New York or with New York residents, making the extraordinary effect that the NYPA would have on the technological marketplace undeniable.

As traditional fiduciary duties impose very substantial obligations on the part of an agent to protect and further the interests of the principal, it is unclear how courts would practically apply the data fiduciary provision of the NYPA to relationships on cyberspace—already commonly viewed as less personal and more arms-length than interactions in other contexts. One solution might be to create alternative dispute resolution mechanisms to mediate and, if needed, arbitrate these disputes in a speedy and cost-effective manner. In sum, before the New York legislature takes this monumental step in fundamentally altering data privacy and the very nature of online business models in cyberspace, it should carefully consider the extent of the proposal's implications and guide its application through sufficiently specific language and provisions.

