WRITTEN TESTIMONY OF PAUL E. PARAY

Member, Paray Law Group, LLC

Provided at

The New York State Senate Public Hearing:

"Protecting Consumer Data and Privacy on Online Platforms"

Conducted by the

Senate Standing Committee on Consumer Protection
(Chair, Senator Kevin Thomas) and
Senate Standing Committee on Internet and Technology
(Chair, Senator Diane Savino)

November 22, 2019

Introduction

My name is Paul E. Paray and I am a privacy and intellectual property attorney practicing in New York and New Jersey who provides small and middle market companies with data breach assistance and help in privacy regulatory compliance. I thank Chair Senator Kevin Thomas and the Senate Standing Committee on Consumer Protection and Chair Senator Diane Savino and the Senate Standing Committee on Internet and Technology for holding this hearing and allowing me to provide this written testimony regarding the need for a bold new comprehensive privacy law in New York.

Consumer Data as a New Asset Class

Before describing what requirements should or should not be placed in a proposed New York privacy statute, it is obviously necessary to first recognize what will be protected by this prospective law. According to the World Economic Forum, "personal data represents an emerging asset class, potentially every bit as valuable as other assets such as traded goods, gold or oil." Rethinking Personal Data: Strengthening Trust, at 7, World Economic Forum Report (May 2012). Currently, there are various rights that underlie this "emerging asset class" given it is only with the trading away of such rights can anyone build on the value of any new personal data asset class. *See c.f.*, Ruth Gavison, Privacy and the Limits of Law, 89 The Yale Law Journal 421, 428-429 (1980) ("A loss of privacy occurs as others obtain information about an individual, pay attention to him, or gain access to him. These three elements of secrecy, anonymity, and solitude are distinct and independent, but interrelated, and the complex concept of privacy is richer than any definition centered around only one of them.").

Surveillance advertising has deliberately made it so these underlying privacy rights are not easily managed – it is not up to consumers whether they will be fed an ad based on previous website

visits or purchases it will just happen. Indeed, according to a survey of 1,000 persons conducted by Ipsos Public Affairs and released by Microsoft in January 2013, forty-five percent of respondents felt they had little or no control over the personal information companies gather about them while they are browsing the Web or using online services. And, even before the prevalence of online tracking consumers were faced with offline tracking that similarly took something away from them without ever directly paying them back for any loss in privacy. *See* Steve Bibas, A Contractual Approach to Data Privacy, 17 Harv. J. Law & Public Policy 591 (Spring 1994) ("Although the ready availability of information helps us to trust others and coordinate actions, it also lessens our privacy. George Orwell presciently expressed our fear of losing all privacy to an omniscient Big Brother. Computers today track our telephone calls, credit-card spending, plane flights, educational and employment records, medical histories, and more. Someone with free access to this information could piece together a coherent picture of our actions.").

Current law does not prevent someone from collecting publicly available information to create a comprehensive consumer profile – nor should there be any such law. Similarly, there should not be the right to opt out of having your publicly recorded information sold or shared. The same rules should not apply to personal information that is not collected solely from public sources.

In order to pay for the development of the Internet we have today, there has been a measurable "loss of privacy" provided in a bartering system where one party feels the value of what is being bartered away while the other party actually quantifies with cascading/monetizing transactions what is only felt by the other party. Even the interactive advertising industry has long believed it should limit the collection of sensitive consumer data. According to a study conducted by the Ponemon Institute, 67 percent of responding online advertisers believe "limiting sensitive data collection for OBA purposes is key to improving consumer privacy and control when browsing or shopping online." Leading Practices in Behavioral Advertising & Consumer Privacy: A Study of Internet Marketers & Advertisers, at 2, The Ponemon Institute (February 2012).

To address the fundamental imbalance existing between the owners of this new "asset class" arising from the relinquishment of certain privacy rights and those companies who obtain access to such data, Alastair Mactaggart launched in 2017 a California ballot initiative that lead to the enactment of the California Consumer Privacy Act (CCPA). Now that CCPA has been enacted and will come online in 2020 – albeit in a weakened form due to the many amendments recently signed into the law, Mr. Mactaggart filed on October 2, 2019 a new ballot initiative that presumably will strengthen CCPA. Respectfully, it is suggested that the Senate follow the path taken with CCPA and by Mr. Mactaggart rather than the path taken in the EU by way of its General Data Protection Regulation (GDPR) – a comprehensive and costly law that dictates how companies are to conduct business by, among other things, mandating certain governance requirements and cross-border transfer prohibitions.

Whereas GDPR ultimately looks to protect the EU and its residents from countries with lesser data processing safeguards, the path begun by CCPA – and likely to continue with Mactaggart's latest ballot initiative – The California Privacy Rights and Enforcement Act of 2020 (Mactaggart 2020 Ballot Initiative), focuses more on protecting individuals on a fundamental level. For example, GDPR does not attribute any value to the new asset class of consumer data – so long as

companies are compliant with GDPR's processing requirements and have a legal basis to conduct such processing, data subjects will largely be without recourse. Under the paternalistic GDPR framework, data subjects are provided with specific rights, including the right to erasure, processing, portability, access and correction, etc., yet are never informed whether these rights are in any way transferable or of any value apart from GDPR's implementation.

The California Privacy Rights and Enforcement Act of 2020

Unlike in California, New York has no constitutional inalienable right to "pursuing and obtaining safety, happiness, and privacy." Accordingly, it would be easy to pass a comprehensive privacy law in New York that reaches lower than CCPA. That would be a mistake. CCPA's underlying goals dovetail exactly with what New York should strive to achieve. For example, CCPA has as its main mission the desire to bring transparency to the current use of consumer data. Before the enactment of CCPA, California was like all other states in that its residents could not learn what personal information a business had collected about them, how such information was being used, and how to prevent such use from taking place. This is another fundamental difference between the US and EU approaches. Under the EU approach, a company could continue to use and process data in unknown ways so long as the GDPR privacy regime was followed. Under the CCPA approach, consumers will always have a say in how usage takes place even when a regulated company is in full compliance with processing requirements.

It is recommended that the Senate study the Mactaggart 2020 Ballot Initiative very carefully given its correction of defects and weaknesses found in CCPA while pushing forward with a consumer-first mandate. This does not mean, however, the Mactaggart 2020 Ballot Initiative – which is awaiting final form approval from the California Attorney General, is not without flaws. The suggestion that a browser-based solution can address the "Do Not Sell" requirement is a likely non-starter given the 12-month wait period before a company can again request usage consent after a "Do Not Sell" request. When taking into consideration VPN usage and the ephemeral nature of a browser's tracking tools, any viable solution will likely require much more of a comprehensive technology framework that adequately considers authentication without requiring users to create an account. *See* Cal. Civ. Code § 1798.135(a)(1)–(2) (precluding companies from requiring consumers to create a new account as a means of enforcing their right to bar sales of data).

Moreover, the CCPA's Sisyphean task of creating a "Do Not Sell My Personal Information" link that is "clear and conspicuous" and yet found on every applicable website's homepage – defined as any page that collects personal information, is certainly not rectified in the Mactaggart 2020 Ballot Initiative. As it currently stands, the link will likely end up being in every footer for those site visitors with a CA IP address – even if generated by a VPN, or will simply be directed to a CCPA-specific page. As several critics of the law have correctly pointed out, this will likely be a logistical nightmare from a technical and user interface perspective.

Passage of the New York Privacy Act

Building on the ground-breaking New York Department of Financial Services data security regulation, 23 NYCRR 500 (Part 500) and its more recently enacted Stop Hacks and Improve Electronic Data Security (SHIELD) Act, New York now has another opportunity to lead the country by passing Senate Bill 5642, the New York Privacy Act (NYPA). By improving upon the good found in the Mactaggart 2020 Ballot Initiative – which will likely be amended within several weeks as per California ballot initiative law, and inserting additional language that inspires competition in the marketplace yet does not penalize small and mid-sized businesses simply because of their size, the Senate can serve all of its constituents.

Even in the heavily regulated world of financial services, Part 500 was written with exemptions for financial services businesses having less than 10 employees working in New York State or with less than $5 million in gross annual revenue. Similarly, the privacy regime found in the Mactaggart 2020 Ballot Initiative only applies to companies having annual gross revenues in excess of $25,000,000 in the preceding calendar year, companies selling the personal information of 100,000 or more consumers or households, or those companies deriving 50% of their annual revenues from selling consumers' personal information. The well-known and not so-well known bad actors in this area are obviously of the larger variety. By creating a solution that primarily applies to those who have improperly profited from data slurping at the grandest level, the costs of enforcement as well as compliance will be kept to a minimum. Accordingly, necessary components of NYPA include a very specific and unambiguous definition of what data is being protected coupled with a reasonable enforcement mechanism – one that does not penalize innocent companies with unnecessary compliance costs.

The consumer data problem is largely based on too much information being in the hands of too few data merchants. Interestingly, there are recent Congressional efforts focused on combatting large bad actors by instilling more transparency in the data collection process as well as providing consumers with more control – the ostensible goals of CCPA and the putative NYPA. As stated in their October 22, 2019 press release, U.S. Sens. Mark R. Warner (D-VA), Josh Hawley (R-MO) and Richard Blumenthal (D-CT) introduced "the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, bipartisan legislation that will encourage market-based competition to dominant social media platforms by requiring the largest companies to make user data portable – and their services interoperable – with other platforms, and to allow users to designate a trusted third-party service to manage their privacy and account settings, if they so choose." The bill expressly focuses on only those technology platforms with over 100 million monthly active users. As also stated in the press release, "Sens. Warner and Hawley have partnered on the DASHBOARD Act, legislation to require data harvesting companies such as social media platforms to disclose how they are monetizing consumer data, as well as the Do Not Track Act, which would allow users to opt out of non-essential data collection, modeled after the Federal Trade Commission's (FTC) "Do Not Call" list."

As with CCPA and the Mactaggart 2020 Ballot Initiative, these latest federal initiatives also focus on transparency – helping consumers understand what data is being collected and how; control – allowing consumers to say no to certain usage of data; and accountability – addressing the need

for adequate data security and compliance with consumer consents. These are the three pillars of a successful privacy law and should be properly incorporated into the final NYPA.

Statutory Recognition of Personal Data as Property

It is respectfully suggested that the innovative use of a Data Fiduciary concept that is found in the current NYPA bill draft be replaced with something not currently found in either CCPA or the Mactaggart 2020 Ballot Initiative, namely a formal statutory acknowledgment that New York residents have a statutory property right in their personal data. It is believed the current Data Fiduciary format will cause enforcement efforts to turn into an unpredictable exercise given determining what specific fiduciary requirements apply to a specific fact pattern will always be wide open to judicial interpretation. On the other hand, providing for specific statutory rights that are fixed and delineated in the law will make transparency, control and accountability much easier to enforce.

The privacy community has long toyed with ascribing property rights to personal data. *See* Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1379 (2000) ("One answer to the question "Why ownership?" then, is that it seems we simply cannot help ourselves. Property talk is just how we talk about matters of great importance. In particular, it is how we talk about the allocation of rights in things, and personally-identified information seems "thingified" (or detached from self) in ways that other sorts of private matters—intimate privacy, for example—are not. On this view, the "propertization" of the informational privacy debate is a matter of course; it merely testifies to the enormous power of property thinking in shaping the rules and patterns by which we live.").

There is an extremely narrow opportunity to get this right given there will be significant pushback from both data merchants as well as the privacy lawyers typically retained to protect them. Indeed, numerous persons have for many years voiced preemptive opposition to such an approach. *See generally* Sarah Jeong, We don't allow people to sell their kidneys. We shouldn't let them sell the details of their lives, either, The New York Times (July 5, 2019) ("Legally vesting ownership in data isn't a new idea. It's often been kicked around as a way to strengthen privacy. But the entire analogy of owning data, like owning a house or a car, falls apart with a little scrutiny. A property right is alienable — once you sell your house, it's gone. But the most fundamental human rights are inalienable, often because the rights become meaningless once they are alienable. What's the point of life and liberty if you can sell them?"); Mark MacCarthy, Privacy Is Not A Property Right In Personal Information, Forbes (November 2, 2018) ("Some commentators new to the privacy debate are quick to offer what they think is a clever idea: assign property rights over personal information to the user and let the marketplace decide what happens next. Whether this idea is meritorious has big implications for how we think about things like data portability and consent. Turns out it's wrong.").

As referenced by Mr. MacCarthy in his position piece, some claim the notion of personal data as property conflicts with the reality, for example, that medical information can simultaneously belong to patients, schools, pharmacies, doctors, pharmaceutical companies, EMR software vendors, advertising companies and Internet service providers. These opponents of data property rights wonder how property ownership rights will be allocated – for resulting payments or veto

power, to constituent owners?

It can also be argued that personal data continually percolates around the world and constitutes a "social good" that can never be owned by individuals. For example, it is the underpinning of a good deal of medical research that ends up curing disease. Information concerning a consumer's interaction with others presumably also allows participants to these interactions to also claim ownership of related data to themselves. Moreover, it is easy to argue the First Amendment should bar the creation of a data property regime given it might potentially stifle speech between parties.

The "social good" argument is likely the one with the broadest appeal. For example, on November 11, 2019 The Wall Street Journal exposed Google's "Project Nightingale" and its resulting company access to the health information maintained by Ascension – one of the nation's leading health systems. In a November 11, 2019 blog post, Google explained that this arrangement was to support Ascension "with technology that helps them to deliver better care to patients across the United States." What is noticeably absent from the blog post is whether Google will also obtain access to patient medical records in a deidentified or other manner. This is noteworthy given last year researchers at Google announced a way to predict a person's blood pressure, age, and smoking status simply from an image of their retina. In order to do so, however, Google first had to analyze retinal images from 284,335 patients. Given health research is obviously a "social good" the use or sale of deidentified protected health information (PHI) has long been an accepted use of medical data. Oregon's failed Senate Bill 703 would have been the first in the nation to require specific consent for the sale of deidentified PHI that is now currently sold each year for billions.

No matter how ultimately couched, however, all of the paternalistic arguments against individuals having property rights in their data still miss the mark. First, simply because a privacy right may be perceived as "inalienable" – as it is under the California Constitution, does not mean there cannot be transferable "compensation units" derived from such rights. Indeed, certain inalienable rights, *e.g.*, right to freedom, right to property, etc., may be suspended entirely during a trial and after conviction based on the *voluntary* commission of a crime. It happens every day throughout the country. Why should a person be precluded from voluntarily transforming certain ascribed privacy rights into tradeable ownership interests for a set duration and upon a specific set of circumstances? No one currently corrals persons living on the streets claiming they need to assert their right to privacy despite the fact public sleeping, eating, and defecation are obviously knowing waivers of the right to privacy. Similarly, persons every day voluntarily join loyalty clubs to obtain product savings while trading away unknown personal data in an unknown surveillance arrangement. Such conduct certainly does not mean the inalienable "right to privacy" was completely shredded up and destroyed by such individuals.

The fact that multiple parties may claim ownership rights in the same personal data also does not negate the fact an ownership regime can viably exist – only that it will require careful coordination and adequate technology to implement. Moreover, any argument based on the First Amendment also misses the mark in the same way no one has a First Amendment right to produce a copyright-protected play without proper consent from the owner.

Providing consumers with the ability and "statutory right to trade one's personal data" – even if the fair market value of such data might be actually quite minimal, is the actual specific ownership right that should be set forth in the NYPA. Noted academics long ago suspected this might be the correct road to eventually take. *See* Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1391 (2000) ("A successful data privacy regime is precisely one that guarantees individuals the right to trade their personal information for perceived benefits, and that places the lowest transaction cost barriers in the way of consensual trades. If individuals choose to trade their personal data away without placing restrictions on secondary or tertiary uses, surely it is their business. On this view, choice rather than ownership is (or should be) the engine of privacy policy. What matters most is that personal data is owned at the end of the day in the manner the parties have agreed.") (emphasis added); *Id*. at 1383 ("A relational approach to personally-identified data might, but need not, assign "ownership" or control of exchange based on possession."); Richard A. Posner, The Right of Privacy, 12 Ga. L. Rev. 393, 394 (Spring 1977) ("People invariably possess information, including facts about themselves and contents of communications, that they will incur costs to conceal. Sometimes such information is of value to others: that is, others will incur costs to discover it. Thus we have two economic goods, "privacy" and "prying." . . . An alternative [economic analysis of privacy] is to regard privacy and prying as intermediate rather than final goods, instrumental rather than ultimate values. Under this approach, people are assumed not to desire or value privacy or prying in themselves but to use these goods as inputs into the production of income or some other broad measure of utility or welfare.") (emphasis added).[1]

Current efforts at creating a statutory privacy regime can actually be considered precursors to a statutory "transactional property" approach. Under CCPA: "A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information." Cal. Civ. Code § 1798.125(b)(1). Indeed, the healthcare privacy regime of HIPAA long understood the possibility PHI might be sold by a covered entity. *See* 45 CFR § 164.508(a)(4)(i) ("Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.").[2]

A transactional property approach would empower consumers without placing unnecessary barriers on the "social good" use of data. Consumers could either choose to accept new statutory protections or lease their data based on an economic model that would allow for the transparency needed to determine whether their data is even sellable. If data is not actually sellable, consumers

[1] In his 1977 article, the now-retired Judge Posner applied a very narrow definition of privacy before rejecting the attribution of property rights to personal data or the need for statutory intervention to better protect an individual's privacy rights. Posner, 12 Ga. L. Rev. at 422 ("Broadly stated, the trend has been toward expanding the privacy protections of the individual while contracting those of organizations, including business firms. This trend is the opposite of what one would expect if efficiency considerations were motivating privacy legislation.").

[2] It is worth noting that given NYPA will apply a more stringent standard for the protection of PHI, HIPAA should not preclude the suggested framework. *See* 45 CFR § 160.203 (There is an express exemption under HIPAA for State law when that "State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted" under HIPAA).

should be limited in how they can prevent companies from using their data given the countervailing social good inherent in the free exchange of consumer data. If there is no existing viable market for a consumer's data, there should not be any associated requirement that a company pay any set amount for such data or be precluded from using such data in a deidentified format. In other words, the burdens claimed by opponents of a property approach would be mitigated – consumers would only be given a piece of the pie and not the whole pie and any purported "veto power" would never really come into existence. Moreover, a regulatory framework that allows market dynamics to actually dictate the applicability of protections afforded to consumers is likely the fairest approach to both consumers and data merchants alike.

Creation of the New York Data Protection Corporation

Similar to the way the Mactaggart 2020 Ballot Initiative proposes the creation of a new California agency, namely the California Privacy Protection Agency (CPPA), it is suggested that the Senate include in the NYPA creation of a public benefit corporation tasked with helping ensure the necessary framework for NYPA can actually get implemented. In other words, unlike in California where the proposed CPPA will only buttress the enforcement and regulatory work done by the California Attorney General's Office, the New York Data Protection Corporation (DPC) would coordinate with the private sector to ensure the requirements of NYPA are viable and able to come to life. The creation of the DPC will ensure the many problems currently visited on those companies looking to comply with CCPA never come to life in New York. There is analogous precedent for the creation of the DPC found in the environmental arena.

It is not likely in dispute that the primary purpose of an environmental regulation is to either prevent potential toxins from infiltrating land, water and air or to remove and properly dispose of them if already released. Addressing improperly used consumer data similarly needs a massive cleanup effort and can take a page from how environmental concerns were previously addressed. To that end, in 1970 the New York State Environmental Facilities Corporation (EFC) was created by the New York State Environmental Facilities Corporation Act.

As a public benefit corporation of the State, EFC is a corporate entity separate and apart from the State. State law empowers the EFC to provide financing for certain environmental projects as well as "render technical advice and assistance to private entities, state agencies and local government units on sewage treatment and collection, pollution control, recycling, hazardous waste abatement, solid waste disposal and other related subjects." Indeed, as stated by the EFC on its website: "Our mission is to provide low-cost capital and expert technical assistance for environmental projects in New York State. Our purpose is to help public and private entities comply with federal and State environmental protection and quality requirements in a cost-effective manner that advances sustainable growth. We promote innovative environmental technologies and practices in all of our programs." (emphasis added).

Similarly, the DPC would provide technical assistance in conformance with NYPA's mandate to protect consumer data. At a basic level, there is never the need to grant access to all data for all purposes to all companies interested in consumer data. Whether by evaluating current zero-knowledge proof solutions – where a verifier has "zero knowledge of" information unnecessary for an actual verification, or determining the feasibility of certain self-sovereign identity

solutions, the DPC can ultimately provide the necessary "secret sauce" for a successful NYPA. Statutory efforts to legislate on privacy will forever be hamstrung if implementation technology remains an afterthought that simply will sort itself out after a law is passed. The goal of the DPC will be to ensure there are adequate technical means available to execute on the legislation passed – not to pick technology sides or inadvertently delay private sector efforts at technology development. Should the Senate continue to move in the direction it has previously plotted, it will need to collaborate with the private sector to determine how best to implement the NYPA statutory framework. And, the only real way to practically make that happen will be to rely on a separate entity such as the DPC.

Providing for a Private Right of Action

Even though CCPA innovated by allowing for statutory damages and a private right of action after certain data breaches, heavy lobbying precluded the inclusion of a private right of action for all privacy violations of the law. It is respectfully suggested that the Senate provide in NYPA the ultimate in enforcement vehicles for any law, namely the private right of action coupled with the ability to recoup legal fees. It is not believed, however, that statutory damages would help achieve higher compliance levels or assist consumers in any appreciable way so such penalties should not be incorporated into NYPA.

Conclusion

The NYPA is a well-thought out piece of legislation that will go a long way in protecting New Yorkers. Nevertheless, the old adage "Go Big or Go Home" comes to mind when looking at NYPA. To that end, it is respectfully believed that the "Big" components needed in NYPA consist of the following:

1. Recognition of a "transactional property right" in consumer data rather than a Data Fiduciary obligation on the part of data merchants;
2. Development of a compliance framework that only applies to larger companies or those maintaining significant consumer data;
3. Insertion of requirements that focus on the three established privacy pillars of transparency, control and accountability; and
4. Creation of a "New York Data Protection Corporation" – a public corporation largely tasked with ensuring that what is statutorily required under NYPA is feasible from a technological and market perspective.

Thank you for your consideration of these comments. If you have any questions, please contact Paul E. Paray *at* paulp@paraylaw.com *or* (201) 281-5134.