Legislative Affairs
One Whitehall Street
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of the New York Civil Liberties Union
before
The New York State Senate Committee on Consumer Protection and the
New York State Senate Committee on Internet and Technology
regarding
Protecting Consumer Data and Privacy on Online Platforms

November 22, 2019

The New York Civil Liberties Union (NYCLU) is grateful for the opportunity to submit the following testimony regarding protecting consumer data and privacy on online platforms. The NYCLU, the New York State affiliate of the American Civil Liberties Union, is a not-for-profit, nonpartisan organization with eight offices across the state and over 180,000 members and supporters. The NYCLU defends and promotes the fundamental principles and values embodied in the Bill of Rights, the U.S. Constitution, and the New York Constitution through an integrated program of litigation, legislative advocacy, public education, and community organizing. As part of a nationwide network of ACLU affiliates, we offer not only our own experience working at the intersection of privacy and technology, but also the lessons learned by our sister affiliates in states that have been on the cutting edge of legislating to protect privacy in the digital age.

During these Committees' June hearing on online privacy, we testified to the scope of the problem as we see it, the legal landscape that any privacy legislation will fall into, and major lessons learned and pitfalls to avoid from other states. We also offered specific feedback on Senator Thomas' New York Privacy Act.[1] Our June testimony is included as an appendix to this statement.

In this testimony, we have been asked to focus on two of the trickier legal issues that any privacy legislation must accommodate. We will also offer our recommendations for the components that any comprehensive privacy legislation should include and outline the pitfalls of a data-as-property approach to consumer data legislation.

[1] Allie Bohm, Policy Counsel, NYCLU, A Joint Public Hearing to Conduct Discussion on Online Privacy and What Role the State Legislature Should Play in Overseeing It, Testimony before the New York State Senate Committee on Consumer Protection and the New York State Senate Committee on Internet and Technology (June 4, 2019).

Legal Considerations

Drafters of comprehensive privacy legislation must ensure that any bill comports with the First Amendment to the U.S. Constitution and must also author a bill that provides a pathway for individuals to vindicate the rights it offers. This section will address each of these issues in turn.

A. The First Amendment

In *Sorrell v. IMS Health Inc.*, the Supreme Court overturned a Vermont statute that prohibited regulated entities from "selling or disseminating prescriber-identifying information for marketing," subjecting content- and speaker-based restrictions "on the sale, disclosure, and use of" personal information to heightened scrutiny.[2] Any comprehensive privacy law that proscribes the collection, use, retention, sharing, or monetization of personal information based on the purpose for the leveraging or the identity of the entity doing the leveraging is likely suspect under *Sorrell*.

A *Sorrell* problem could materialize in legislation in multiple ways, from bills that cover only a subset of entities that leverage personal information to bills that regulate only particular uses of personal information. Perhaps the most tempting way the issue arises is when well-meaning bill drafters endeavor to create a journalism carveout to any privacy bill. In addition to raising difficult questions about who qualifies as a journalist, a journalism carveout is both an identity-based (journalist) and purpose-based (news gathering and dissemination) distinction that the Supreme Court is likely to look askance at following *Sorrell*.

Fortunately, there is a constitutional way to ensure that privacy legislation does not undermine journalism – a goal we certainly share. That solution is to focus on the way personal information is collected so that legislation applies to personal information captured in exchange for any kind of consideration, including but not limited to a good or service, the placement of targeted advertisements, or a membership; as a result of an individual, household, or device's establishment or maintenance of an account with a covered entity; or as a result of an individual, household, or device's interaction with a covered entity. Although a major downside of this approach is that it would not reach data brokers that have no direct relationship with individuals, if a bill is properly drafted, it would likely ossify the data broker industry by choking off new sources of personal information.

B. Standing and Redress

Bill drafters, including Chairman Thomas in his New York Privacy Act, are right to include a private right of action in comprehensive privacy legislation. While the Attorney General and other state and local actors should certainly have a role in enforcing any privacy law, government resources are necessarily limited, and government actors will only be able to enforce in the most egregious cases. A private right of action not only allows individuals to seek redress in cases where the government chooses not to intervene, but the threat of private lawsuits is likely to incentivize companies to

[2] 564 U.S. 552, 562 – 65 (2011).

adhere to any privacy law and protect individuals' personal information. But, a necessary requisite to any private right of action is ensuring that individuals have standing to bring lawsuits. There are two ways to do this.

The first is to make clear in the legislation that a violation of the act itself or regulations promulgated thereunder with respect to an individual's personal information constitutes an injury-in-fact to that individual. This is the approach that Illinois lawmakers took in their Biometric Information Privacy Act and that the Ninth Circuit has upheld.[3]

The second is for legislation to enumerate a fulsome list of harms that arise from misuse of personal information and to confer standing on anyone who has experienced one of those harms as a result of a violation of the act or regulations promulgated thereunder. If lawmakers elect this approach, it is imperative to define harm more broadly than merely "reasonably foreseeable and material physical or financial harm" to an individual.[4] Although these harms are important, financial harm, in particular, is among the least likely to occur. That is because when financial loss arises from a data breach or misuse of data – say, where a credit card number is stolen and fraudulent purchases are made – it is often difficult to trace the stolen information to a particular privacy violation.[5] When it is possible to trace the financial harm back, banks often reimburse customers for fraudulent purchases, obviating any actual financial loss.[6] Physical harm, of course, can be devastating when it occurs. However, these two harms are a vanishingly small subset of the harms that can arise from the pervasive collection, sharing, monetization, use, and misuse of personal information.

Rather, harm should be defined to include but not be limited to:

- direct or indirect financial harm;
- physical harm or threats to individuals or property, including but not limited to bias-related crimes and threats, harassment, and sexual harassment;
- discrimination in goods, services, or economic opportunity – such as housing, employment, credit, insurance, education, or health care – on the basis of an individual or class of individuals' actual or perceived age, race, national origin, sex, sexual orientation, gender identity or expression, disability, and/or membership in another protected class;
- interference with or surveillance of First Amendment-protected activities by state actors;
- interference with the right to vote or with free and fair elections;
- interference with due process or equal protection under law;
- loss of individual control over personal information, nonconsensual sharing of private information, and data breach;
- the nonconsensual capture of information or communications within an individual's home or where an individual has a reasonable expectation of seclusion or access control; and
- other effects on an individual that may not be reasonably foreseeable to, contemplated by, or expected by the individual to whom the personal information relates, that are nevertheless

[3] *See Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019).
[4] S.5642 § 2, 2019-2020 Reg. Sess. (N.Y. 2019).
[5] *See* Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, WALL STREET J., June 26, 2016, https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.
[6] *Id*.

reasonably foreseeable, contemplated by, or expected by the covered entity that alter or limit that individual's choices or predetermine results.[7]

A best practice would be to codify a rebuttable presumption of harm to an individual where the act itself, or regulations promulgated thereunder, has been violated with respect to that individual's personal information.

In addition to ensuring that private individuals have standing to sue, legislation should provide *per se* statutory damages for violations of the act. Quantifying the damages associated with misuse or unauthorized use of personal information is often contentious in a litigation context. Statutory damages are effective when harm is real but hard to put a dollar figure on and incentivize covered entities to adhere to the law. Statutory damages have previously been employed, with success, in the privacy context.[8]

Recommendations for Comprehensive Privacy Legislation

There are five components that are critical to include in any comprehensive privacy legislation. This section will address each of them in turn.

A. Preventing Discriminatory Algorithms

While privacy is certainly an end in and of itself, privacy cannot be divorced from the tangible harms that arise from the abuse and misuse of personal information in the digital age. The most pernicious is the circumvention of our civil and human rights laws. For example, personal information has been leveraged to ensure that only younger men see certain job postings and to exclude African-Americans from viewing certain housing advertisements.[9] Any comprehensive privacy legislation must ensure that key civil rights protections apply to the digital world by prohibiting targeted advertising and the processing of personal information in ways that would violate our civil and human rights laws in the analog world.

But it's not enough to prohibit discrimination in the digital world only by private actors. The government must also interrogate its own use of automated decision-making for purposes that impact individuals' constitutional or legal rights, duties, or privileges. Toward this end, comprehensive privacy legislation should ensure that before any government entity in New York state acquires or deploys an automated decision system, the system undergoes and passes a civil rights audit conducted by a neutral third party; the state should impose such an audit requirement

[7] *See generally* Allie Bohm, Policy Counsel, NYCLU, A Joint Public Hearing to Conduct Discussion on Online Privacy and What Role the State Legislature Should Play in Overseeing It, Testimony before the New York State Senate Committee on Consumer Protection and the New York State Senate Committee on Internet and Technology (June 4, 2019).
[8] *E.g.* 47 U.S.C. § 551 (2001) (The Cable Privacy Act).
[9] *See* Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU SPEAK FREELY, Mar. 19, 2019, https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping.

on existing government automated decision systems as well. Furthermore, legislation should guarantee that individuals subjected to automated decisions that affect their human rights or liberty receive notice of the decision made, the involvement of an automated system, and the opportunity to contest the decision and seek human review. Finally, legislation should require that government entities that use automated decision-making systems have appropriate governing policies in place, adhere to certain transparency requirements, and have the approval of the relevant city or county council or the state legislature, following a public hearing, before acquiring the technology.

B. Meaningful Notice, Opt-in Consent, and Affirmative Obligations

Of course, any comprehensive privacy legislation must also include robust and meaningful privacy protections and mechanisms for individuals' control over their personal information.

Countless websites, apps, services, internet-connected devices, and even brick-and-mortar stores collect, retain, use, share, and monetize our personal information – often in ways we do not understand and would not agree to if we understood. Part of the problem is that when companies disclose their data collection, retention, use, sharing, and monetizing practices, they do so in legalese in the fine print of privacy policies that no reasonable person reads. Indeed, researchers at Carnegie Mellon found that it would take 76 work days for an individual to read all of the privacy policies encountered in a year.[10] Comprehensive privacy legislation should ameliorate this problem by taking the pertinent information out of the fine print of a privacy policy and requiring meaningful notice to individuals that is concise and intelligible, clear and prominent, written in clear and plain language, and leveraging appropriate visualizations to make complex information understandable by the ordinary user.

But, notice alone is insufficient. Legislation should also require individuals' affirmative, opt-in consent before covered entities collect, use, retain, share, or monetize their personal information. This is important, because default is often destiny. Many individuals never change a site's default settings, meaning that significantly more personal information will be processed under an opt-out regime than under an opt-in regime.[11] This in turn matters because personal information is just that – personal – and individuals should be in the position to decide how, when, and why it is processed and with whom it is shared. In addition, in order to ensure that opt-in consent is meaningful, comprehensive privacy legislation must prohibit the use of coercive site designs that manipulate individuals into granting their assent as well as pay-for-privacy regimes that risk making privacy a luxury good, available only to those who can afford to pay for it, and further marginalizing the most marginalized.

Furthermore, comprehensive privacy legislation must provide individuals with access, deletion, and portability rights and must include robust data security requirements. Finally, legislation must limit

---

[10] Alexis D. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.
[11] Lena V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PRO PUBLICA, July 27, 2016, https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world.

covered entities to sharing individuals' personal information only with authorized parties that will treat that information with similar care.

C. Application to All Personal Information

Comprehensive privacy legislation must provide meaningful protections for all personal information – that is, any information that is reasonably linkable, directly or indirectly, to a specific individual, household, or device.

Too frequently, lawmakers, federally and in other states, have sought to split the baby, providing heightened protection for so-called sensitive information like first and last name, social security numbers, and bank account numbers, and lesser protection for other personal information. This so-called sensitive/non-sensitive distinction is increasingly illogical in the digital age. Purportedly non-sensitive information can be aggregated to reveal sensitive information, and, in fact, some non-sensitive information, in isolation, may reveal sensitive information. For example, while health status is frequently considered sensitive, shopping history is not. But, if an individual is shopping at TLC Direct[12] and Headcovers Unlimited,[13] two websites that specialize in hats for chemotherapy patients, that individual's shopping history may reveal their health status.

In addition, so-called non-sensitive information can be leveraged for purposes that are quite sensitive. For example, if Cambridge Analytica is to be believed, so-called non-sensitive information, like social media likes, can be used for highly sensitive activities such as influencing how individuals vote.[14] Furthermore, sensitivity is highly subjective; different individuals are likely to perceive the sensitivity of different pieces of personal information differently. For these reasons, any line drawing around sensitivity is inherently arbitrary, and comprehensive privacy legislation should protect all personal information.

Perhaps the only distinction that merits consideration in comprehensive privacy legislation is heightened protections for biometric information. This is because biometric information, like fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and gait, is biologically unique to an individual and cannot be changed if compromised. Illinois' Biometric Information Privacy Act models this sort of heightened protection.[15]

D. Application to All Types of Processing

Comprehensive privacy legislation must govern all types of personal information processing, including, but not limited to, collection, access, use, retention, sharing, monetization, analysis, creation, generation, derivation, decision-making, recording, alternation, organization, structuring, storage, disclosure, transmission, sale, licensing, disposal, destruction, de-identifying, or other handling of personal information. Legislation that focuses solely or primarily on the sale of personal information, as California's oft-referenced law does, misses the mark. Many entities that profit off of

---

[12] TLC DIRECT, https://www.tlcdirect.org (last visited Nov. 2, 2018).
[13] HEADCOVERS UNLIMITED, https://www.headcovers.com (last visited Nov. 2, 2018).
[14] Timothy B. Lee, *Facebook's Cambridge Analytica scandal, explained [Updated]*, ARS TECHNICA, Mar. 20, 2018, https://arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal-explained/.
[15] 740 ILCS/14 (2008).

personal information do not sell that information.[16] Rather, they leverage it to sell advertisements: an advertiser approaches the entity with an audience it would like to reach (say, suburban women with children who drive minivans and like the color blue), and the entity uses the personal information it maintains to match the advertisement to the desired audience.[17] The fact that the personal information does not change hands is immaterial. Moreover, this sort of targeting enables the circumvention of our civil and human rights laws described earlier in this testimony.

E. Digital Literacy and Digital Privacy

Finally, in addition to the important safeguards recommended in this section, comprehensive privacy legislation should provide for digital literacy and digital privacy education in K-12 schools to help young New Yorkers act as informed participants in a digital world. Digital literacy curricula should help students identify online fraud, find reliable sources and information, and better understand how their online activities are tracked and recorded, where personal information posted online may go, with whom it may be shared, how it may be used, and how to best protect their digital security and digital privacy.

One of the reasons businesses and governments have so successfully convinced New Yorkers – and individuals across the country – to give away the most intimate details of our lives is that many of us do not know what we are giving away. We do not know what personal information businesses collect, how our activities are tracked and recorded, where that information goes, or how it is used once it is collected. Part of the solution lies in requiring entities to be more transparent, to give individuals more choices, and to eschew some of their most problematic practices, but the other part of the solution lies in educating New Yorkers to better safeguard our own privacy and to make informed choices about the ways in which we share information in the digital age.

And, while it would be unwise and unconstitutional to try to prohibit "fake news," digital literacy education can help provide New Yorkers with the tools and skills needed to identify accurate and misleading information online and beyond.

Data-as-Property

Finally, we were asked to provide feedback on a data-as-property model. Unfortunately, while a data-as-property model may be appealing as a tool for redistributing the profits from the sale of personal information, this approach undermines, rather than advances, individuals' privacy and raises serious free expression, economic justice, and implementation concerns.

[16] *E.g.* Kurt Wagner, *This is how Facebook uses your data for ad targeting*, RECODE, Apr. 11, 2018, https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg.
[17] *Id*. Some entities are also set up to find look-alike audiences with similar traits to a pre-populated list an advertiser provides. Some also permit an advertiser to target particular individuals. UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).

A. Privacy and Free Speech Concerns Associated with a Data-as-Property Model

The data-as-property model is based on the premise that individuals should be paid when their personal information is sold and re-sold. To effectuate that, an elaborate tracking and monitoring system would need to be created and deployed to identify who owns personal information, who has sold it, who must pay for it, and who must be paid. This would require that a unique, universal tracker be attached to all personal information so that sellers can ascertain if an individual has granted permission to sell the information, if any limitations have been placed on its sale, and to enable the individual to be paid. It is quite possible that all personal information would need to be tagged with a tracker so that potential sellers know when permission to sell has been denied and from whom to request permission.

The use of these trackers would have serious negative impacts on privacy in the digital age, as well as on the ability to communicate anonymously online. The loss of anonymity is likely to undermine the free exchange of ideas and, in particular, ideas that individuals are exploring, but do not necessarily endorse, opinions that are unpopular, and information from whistleblowers.

B. Economic Justice Issues

A data-as-property law will have the perverse effect of incentivizing individuals to sell their personal information, rather than to protect it. This is particularly true for already economically disadvantaged New Yorkers who may have greater difficulty saying no to additional income than more economically secure New Yorkers do. Adopting a model where individuals with less wealth are likely to end up with less privacy should give lawmakers pause.

A government endorsed data-as-property model would exacerbate the existing digital divide,[18] where individuals enduring socioeconomic or regional economic disadvantages – including, disproportionately, people of color – already have less privacy; they rely on cheaper, unencrypted cell phones, free email, and other more affordable, but less secure, technology. The digital divide is a privacy divide, and the data-as-property model would only worsen it.

C. Implementation Concerns

In addition to undermining privacy, free expression, and economic justice, a data-as-property model would be difficult to implement as lines blur with regard to who "owns" personal information. What happens when someone wants to sell personal information, like a group photograph, that pertains to multiple individuals? Does everyone have to agree and be paid? Does a single party have veto power? To whom does the personal information in this group photograph belong anyway?

Rather than focus on a data-as-property model, the legislature should concentrate on meaningful comprehensive privacy legislation that includes the components described above.

[18] Gry Hasselbach & Pernille Tranberg, *Privacy is creating a new digital divide between the rich and poor*, THE DAILY DOT, Oct. 23, 2016, https://www.dailydot.com/layer8/online-privacy-data-ethics/.

Conclusion

The NYCLU appreciates the opportunity to testify today and stands ready to assist the Committees, Chairman Thomas, and other interested legislators as you craft comprehensive privacy legislation for New York State.

Appendix

Legislative Affairs
One Whitehall Street
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of the New York Civil Liberties Union
before
The New York State Senate Committee on Consumer Protection and the New York State Senate Committee on Internet and Technology
regarding
A Joint Public Hearing to Conduct Discussion on Online Privacy and What Role the State Legislature Should Play in Overseeing It

June 4, 2019

The New York Civil Liberties Union (NYCLU) is grateful for the opportunity to submit the following testimony regarding online privacy and the role the state legislature should play in overseeing it. The NYCLU, the New York State affiliate of the American Civil Liberties Union, is a not-for-profit, nonpartisan organization with eight offices across the state and over 190,000 members and supporters. The NYCLU defends and promotes the fundamental principles and values embodied in the Bill of Rights, the U.S. Constitution, and the New York Constitution through an integrated program of litigation, legislative advocacy, public education, and community organizing. As part of a nationwide network of ACLU affiliates, we offer not only our own experience working at the intersection of privacy and technology, but also the lessons learned by our sister affiliates in states that have been on the cutting edge of legislating to protect privacy in the digital age.

It is no longer possible to participate in society without providing personal information to private companies and other third parties that may, in and of itself reveal intimate details of one's life, or that, when combined with other data and analyzed, may expose such information. The consequences can be profound. For example, personal information has been leveraged to ensure that only younger men see certain job postings and to exclude African-Americans from viewing certain housing advertisements.[19] Cambridge Analytica put consumer privacy on the map in

[19] *See* Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU SPEAK FREELY, Mar. 19, 2019,

March of last year when the public learned that it had obtained more than 50 million Facebook users' personal information from an unsavory app developer and purported to use that information to engage in "psychographics" to convince voters to cast their ballots for Mr. Trump.[20] During the 2016 election, personal information was also used to target advertisements to African-Americans urging them not to vote.[21] Reporting on these and other phenomena, the *New York Times* observed in September that exploitation of personal information enables "unequal consumer treatment, financial fraud, identity theft, manipulative marketing, and discrimination."[22] Against this backdrop, the Committees' consideration of online privacy and the state legislature's role in overseeing it could not be timelier.

This testimony will proceed by explaining the scope of the problem as we see it, as well as a brief overview of the legal landscape that any privacy legislation will fall into. It will then outline two of the major lessons learned and pitfalls to avoid from our sister states. Finally, it will offer specific feedback on Senator Thomas' New York Privacy Act.

A. Scope of the Problem

When we at the NYCLU began to work on consumer privacy, we made a list of the harms that stem from the pervasive collection, retention, sharing, monetization, use, and misuse of personal information. Here are some of the harms we are cognizant of:

Entities – whether businesses, employers, schools, landlords, health insurers, or credit-issuing agencies – can use amassed personal information to limit individuals' awareness of and access to opportunities. This can be deliberate or inadvertent, and, depending on the opportunity in question, amassed personal information and sophisticated algorithms can be used to circumvent our civil and human rights protections. As described above, some employers have consciously targeted advertisements to keep older workers from learning of certain job opportunities,[23]

---

https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping.

[20] Timothy B. Lee, *Facebook's Cambridge Analytica scandal, explained [Updated]*, ARS TECHNICA, Mar. 20, 2018, https://arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal-explained/.

[21] Natasha Singer, *Just Don't Call It Privacy*, NYTIMES, Sept. 23, 2018, https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.

[22] *Id*.

[23] Julia Angwin, Noam Scheiber, & Ariana Tobin, *Facebook Job Ads Raise Concerns About Age Discrimination*, NYTIMES, Dec. 20, 2017, https://www.nytimes.com/2017/12/20/business/facebook-job-ads.html.

and landlords have prevented racial minorities from seeing certain housing advertisements.[24]

Even when advertisers are not acting deliberately to discriminate, individuals' opportunities may be inadvertently limited as a result of the online advertising industry functioning as intended. For example, Leigh Freund of the Network Advertising Initiative testified at November's Federal Trade Commission hearings on Big Data, Privacy, and Competition that "women are less likely to see employment ads for careers in the science/technology/engineering/math field . . . simply because they have higher value to other advertisers because women do more shopping."[25]

In addition, as entities increasingly turn to sophisticated algorithms and automated decision-making to place ads, screen resumes, or even, in government hands, to make bail decisions, decide where to deploy police, or to make child custody decisions, the training data used to develop the algorithms can have outsized impacts on individuals' opportunities and outcomes.[26] Algorithms work by identifying correlation, not causation, and the training data used to "teach" algorithms what patterns to look for often reflect and then magnify entrenched historical biases.[27] For example, researchers at Carnegie Mellon and the International Computer Science Institute found that user "profiles . . . pegged as male were much more likely to be shown ads for higher-paying executive jobs than those . . . identified as female – even though the simulated users were otherwise equivalent."[28] Amazon, famously, pulled the plug on its resume-screening algorithm, because the algorithm, trained on Amazon's predominantly-male existing workforce, systematically downgraded female resumes and elevated male applicants.[29]

---

[24] Julia Angwin, Ariana Tobin, & Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, PROPUBLICA, Nov. 21, 2017, https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

[25] Leigh Freund, President and CEO, Network Advertising Initiative, Competition and Consumer Protection Issues in Online Advertising, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

[26] There are also entities that wish to use amassed personal information and algorithms for admirable purposes – to engage in affirmative action and to target opportunities and messages specifically to more marginalized communities. *See* Public Interest Privacy Legislation Principles (Nov. 13, 2018), https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf.

[27] Karen Hao, *What is machine learning? We drew you another flowchart*, MIT TECH. Rev., Nov. 17, 2018, https://www.technologyreview.com/s/612437/what-is-machine-learning-we-drew-you-another-flowchart/.

[28] Sarah Wachter-Boettcher, *Why You Can't Trust AI to Make Unbiased Hiring Decisions*, TIME, Oct. 25, 2017, http://time.com/4993431/ai-recruiting-tools-do-not-eliminate-bias/.

[29] Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, REUTERS, Oct. 9, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

In government hands, algorithms trained on historical policing and criminal justice system data are likely to lock up more black and brown people simply because the training data reflect the systematic racism that has been endemic in the criminal justice system since before the nation's founding.[30]

In addition to race, sex, and age discrimination and other forms of discrimination based on protected classes, amassed personal information can be used to engage in unfair price discrimination. For example, *Wall Street Journal* investigators discovered that Staples.com shows individuals who live near rival stores lower prices.[31] Because stores are more likely to be situated in wealthier areas, this practice often means that Staples charges poorer people higher prices.[32]

Pervasive collection and use of personal information can exacerbate information disparities and contribute to the erosion of trust and free expression as individuals find themselves facing personalized, curated newsfeeds that reflect their own points of view or customized recommended videos that show increasingly radicalized versions of their own perspectives.[33] And, as described above, at its most extreme, manipulation of these curated newsfeeds and targeted advertising, coupled with stores of personal information, may be used influence individuals' selections in the voting booth.[34]

Collection and pooling of personal information also creates treasure troves for government access. This is because the antiquated third-party doctrine dictates that personal information, once shared with a third party, forfeits all Fourth Amendment protections, and the government need not go before a court, show that there is good reason to believe that the information will turn up evidence of a crime, and get a warrant in order to obtain it.[35] The government can simply get the information from

---

[30] *See* The Use of Pretrial "Risk Assessment" Instruments: A Shared Statement of Civil Rights Concerns (July 30, 2018), http://civilrightsdocs.info/pdf/criminal-justice/Pretrial-Risk-Assessment-Full.pdf.
[31] Jennifer Valentino-DeVries, Jeremy Singer-Vine, & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL STREET J., Dec. 24, 2012, https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.
[32] *Id*.
[33] Conor Friedersdor, *YouTube Extremism and the Long Tail*, THE ATLANTIC, Mar. 12, 2018, https://www.theatlantic.com/politics/archive/2018/03/youtube-extremism-and-the-long-tail/555350/.
[34] Timothy B. Lee, *Facebook's Cambridge Analytica scandal, explained [Updated]*, ARS TECHNICA, Mar. 20, 2018, https://arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal-explained/; Natasha Singer, *Just Don't Call It Privacy*, NYTIMES, Sept. 23, 2018, https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.
[35] *See generally* Jay Stanely, *The Crisis in Fourth Amendment Jurisprudence*, AM. CONST. SOC'Y ISSUE BRIEF, May 2010, at 2, https://www.aclu.org/files/assets/ACS20Issue20Brief20-20Stanley204th20Amendment1.pdf.

the third party without ever telling the individual to whom the information pertains. This means that e-mails receive less protections than physical mail stored in an individual's filing cabinet and photos stored on Facebook or Flickr are more vulnerable than those kept in an album at home.[36]

The personal information third parties collect online may be useful to federal government actors going on fishing expeditions for undocumented immigrants or to the federal Drug Enforcement Agency, should New York legalize marijuana, seeking marijuana users, growers, and industry participants. Moreover, the pooling of personal information in third party hands threatens to undermine the critical criminal justice safeguards the framers thought wise to include in the Fourth Amendment.

The collection and retention of personal information does not merely create a target for law enforcement. It creates a bullseye for data thieves – whether those seeking profit or those seeking to interfere in U.S. elections.[37] Data breaches – as well as misuse of personal information – can lead to financial harm, reputational harm, emotional harm, or physical harm. The revelation of personal information can undermine an individual's job prospects or family and friend relationships and can increase the risk of future harms. As individuals grapple with these harms, they may be reluctant to participate fully in digital life and to utilize online services.[38]

---

[36] The Supreme Court last year in *Carpenter v. United States* made clear that the third-party doctrine does not automatically apply to individuals' location records held by their cell phone providers. Although the lesson of Supreme Court's holding should apply equally to any digital database of personal information held by a third party, government entities continue to access personal information without a warrant. *Cf.* Nathan Freed Wessler, *The Government Needs to Get a Warrant if It Wants Access to Our Private Health Information*, ACLU SPEAK FREELY, May 29, 2019, https://www.aclu.org/blog/privacy-technology/medical-and-genetic-privacy/government-needs-get-warrant-if-it-wants-access.

[37] *See generally* Robert S. Mueller, III, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION (2019).

[38] *E.g.* Avi Goldfarb, Rotman Chair in Artificial Intelligence and Healthcare, Rotman School of Management, University of Toronto, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018) (testifying that "it's much harder to get people to fill out surveys than it used to be."); Lior Strahilevitz, Sidley Austin Professor of Law, University of Chicago Law School, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018) (testifying that fewer people answer their cell phones today "if it's an unrecognized number."); Amalia Miller, Associate Professor of Economics, University of Virginia, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018) (testifying that if individuals "don't feel that their data are safe, they may not download apps on their phone . . . They may shut off Facebook or never post their child online because they don't feel that privacy is protected" and observing that the U.S. has been slower to adopt electronic medical records, leading to "greater mortality, greater infant mortality.").

Compounding these problems, individuals in New York State, like individuals across the nation, do not know or consent to the manner in which entities collect, use, retain, share, and monetize their personal information. This misunderstanding is, at least in part, due to obfuscation on the part of the entities leveraging individuals' personal information. Researchers at Carnegie Mellon found that it would take 76 work days for individuals to read all of the privacy policies they encounter in a year.[39] Although the advertising industry developed a common logo and slogan to notify individuals of the opportunity to opt-out of targeted advertising, following market research, the industry selected the slogan and logo that few individuals understood, seemingly to discourage opt-out.[40] Moreover, entities that collect, use, retain, share, and monetize personal information have specialized knowledge about the algorithms and data security measures they use, as well as about how they collect, use, retain, share, and monetize personal information, that the average individual is unlikely to know or understand.

Although individuals may not fully understand how entities collect, use, retain, share, and monetize their personal information, they demonstrate time and again that they care about privacy. Ninety-two percent of Facebook users alter the social network's default privacy settings, indicating that they wish to choose with whom they share personal information.[41] Similarly, ninety-two percent of Americans believe companies should obtain individuals' permission before sharing or selling their personal information.[42] The same percentage believe that entities should be compelled to provide individuals with a list of all the data they have collected about them,[43] and more individuals in the United States use Microsoft's dashboard to access the personal information Microsoft has about them than individuals in Europe do.[44]

---

[39] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.
[40] *See* FPF Staff, *Online Behavioral Advertising "Icon" Study*, FUTURE OF PRIVACY FORUM (Feb. 15 2010), https://fpf.org/2010/02/15/online-behavioral-advertising-icon-study/; Jonathan Mayer, *Tracking the Trackers: The AdChoices Icon*, STANFORD LAW SCHOOL: THE CENTER FOR INTERNET & SOCIETY (Aug. 18, 2011), http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon.
[41] Emil Protalinksi, *13 million US Facebook users don't change privacy settings*, ZDNet, May 3, 2012, https://www.zdnet.com/article/13-million-us-facebook-users-dont-change-privacy-settings/.
[42] Christopher Boone, Vice President of Real World Data and Analytics, Pfizer, The Business of Big Data, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).
[43] *Id*.
[44] Julie Brill, Corporate Vice President and Deputy General Counsel for Global Privacy and Regulatory Affairs, Microsoft, Former Enforcers Perspective: Where Do We Go From Here? What is Right, Wrong, or Indeterminate about Data Policy?, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 8, 2018).

B. The Legal Landscape

Drafters seeking to author privacy legislation for New York State are not painting on a clean canvas. Federally, numerous sectoral laws cover aspects of privacy in the digital age.[45] At the state level, New York State already has a data breach notification law,[46] along with other sectoral privacy laws.[47] This is not to say that the field is covered – many of these laws are out-of-date, and comprehensive privacy legislation bringing New York into the digital age is much needed. However, any legislation must be carefully crafted to interact well with existing New York and federal privacy laws.

Moreover, comprehensive privacy legislation must be carefully tailored to comport with Supreme Court precedent. In *Sorrell v. IMS Health Inc.*, the Supreme Court overturned a Vermont statute that prohibited regulated entities from "selling or disseminating prescriber-identifying information for marketing," subjecting content- and speaker-based restrictions "on the sale, disclosure, and use of" personal information to heightened scrutiny.[48] Any comprehensive privacy law that proscribes the collection, use, retention, sharing, or monetization of personal information based on the purpose for the leveraging or the identity of the entity doing the leveraging is likely suspect under *Sorrell*.

In addition, the Supreme Court has cast doubt on the constitutionality of mandatory disclosures and notifications.[49] Although commercial speech is often held to a more lenient standard of review than other types of speech, "the Supreme Court does not necessarily apply rational basis review every time the government compels"

---

[45] *E.g.* 5 U.S.C. 552a (the Privacy Act of 1974); 12 U.S.C. 3401 et seq. (the Right to Financial Privacy Act of 1978); 15 U.S.C. 1681 et seq. (the Fair Credit Reporting Act); 15 U.S.C. 1692 et seq. (the Fair Debt Collection Practices Act); 15 U.S.C. 6501 et seq. (the Children's Online Privacy Protection Act); 15 U.S.C. 6801 et seq. (Title V of the Gramm-Leach-Bliley Act); 18 U.S.C. 119; 18 U.S.C. 123; 18 U.S.C. 206; 20 U.S.C. 1232g (the Family Educational Rights and Privacy Act of 1974); 20 U.S.C. 1232h; 42 U.S.C. 2000aa et seq. (the Privacy Protection Act of 1980); 42 U.S.C. 1320d-2 note (the Health Insurance Portability and Accountability Act of 1996); 47 U.S.C. 222, 227.

[46] N.Y. Gen. Bus. Law § 899-aa (McKinney).

[47] *E.g.* N.Y. Educ. Law § 2-d (McKinney) (protecting student privacy); N.Y. Lab. Law § 203-d (McKinney) (protecting employee privacy); N.Y. Gen. Business Law § 899-aa (Information Security Breach and Notification Act"); and N.Y. Technology Law § 208 (same, applicable to state entities); Personal Privacy Protection Law, N.Y. Public Officers Law, Article 6-A, §§ 91-99 (McKinney) (regulating the manner in which the state collects, maintains and disseminates personal information); N.Y. Civil Rights Law § Section 79-L (McKinney) (providing confidentiality for genetic test records). See also 23 NYCRR § 500 et seq. (establishing "Cybersecurity Requirements for Financial Services Companies").

[48] 564 U.S. 552, 562 – 65 (2011).

[49] *See generally NIFLA v. Becerra*, 585 U.S. ___, ___ (2018).

commercial speech. "The Court has evaluated some restrictions and prohibitions . . . under intermediate scrutiny, and others under strict scrutiny. Moreover, the commercial speech doctrine is less likely to apply when the speech regulation at issue is content based,"[50] as required privacy notifications may be.

It is incumbent on drafters and advocates to take the time to understand the relevant case law to ensure that the consumer privacy law New York ultimately adopts can withstand constitutional scrutiny, because that law will inevitably be challenged by the entities whose practices it regulates.

C. Lessons from Other States

New York also has the opportunity to learn from the other states, like California,[51] that have already enacted consumer privacy legislation, as well as to learn from Europe's experience implementing the General Data Protection Regulation. Here are two lessons we hope New York legislators take to heart:

1. Any Comprehensive Privacy Legislation Must Reach More Than Just Sale

Legislation that focuses solely or primarily on the sale of personal information, as California's law does, misses the mark. Many entities that profit off of personal information do not sell that information.[52] Rather, they leverage it to sell advertisements: an advertiser approaches the entity with an audience it would like to reach (say, suburban women with children who drive minivans and like the color blue), and the entity uses the personal information it maintains to match the advertisement to the desired audience.[53] The fact that the personal information does not change hands is immaterial for individuals' experiences. They are aware that companies monetize their personal information even if that information is not literally sold. Moreover, this sort of targeting enables many of the harms described earlier in this testimony – from preventing women and older workers from seeing job postings and people of color from seeing housing ads to targeting ads to encourage African-Americans to stay home on election day.

---

[50] *Stuart v. Loomis*, 992 F. Supp. 2d 585, 593 (M.D.N.C. 2014) (internal citations omitted).
[51] Cal. Civ. Code § 1798.175 et seq. (West).
[52] *E.g.* Kurt Wagner, *This is how Facebook uses your data for ad targeting*, RECODE, Apr. 11, 2018, https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg.
[53] *Id.* Some entities are also set up to find look-alike audiences with similar traits to a pre-populated list an advertiser provides. Some also permit an advertiser to target particular individuals. UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).

2. Any Comprehensive Privacy Legislation Must Cover All Personal Information

Federally, too many of the proposed privacy bills maintain the so-called sensitive/non-sensitive distinction. This distinction, which provides heightened protections for so-called sensitive information, like first and last name, social security numbers, and bank account numbers, and lesser protections to other personal information, is increasingly illogical in the digital age. So-called non-sensitive information can be aggregated to reveal sensitive information, and, in fact, some non-sensitive information, in isolation, may reveal sensitive information. For example, while health status is frequently considered sensitive, shopping history is not. But, if an individual is shopping at TLC Direct[54] and Headcovers Unlimited,[55] two websites that specialize in hats for chemotherapy patients, her shopping history may reveal her health status. In addition, so-called non-sensitive information can be used for purposes that are quite sensitive. For example, if Cambridge Analytica (and, for that matter, the Obama campaign)[56] is to be believed, so-called non-sensitive information, like social media likes, can be leveraged for highly sensitive activities such as influencing how individuals vote. In addition, sensitivity is highly subjective; different individuals are likely to perceive the sensitivity of different pieces of personal information differently. For these reasons, any line drawing around sensitivity is inherently arbitrary. Comprehensive privacy legislation must instead provide meaningful protections for all personal information – that is, any information that is reasonably linkable, directly or indirectly, to a specific individual, household, or device – and not merely for so-called sensitive information.

D. The New York Privacy Act and Recommendations

The preceding pages of this testimony sought to paint a robust picture of the landscape the legislature is wading into. This is not to suggest either that the legislature could or should solve for every single one of the harms identified in the first part of this statement in comprehensive privacy legislation nor is it to suggest that legislators should throw your hands up and walk away. It is, however, to illustrate that this issue is complex, and if we do not have an idea of the problems we seek to solve, we are unlikely to address them. The NYCLU strongly urges the legislature to give comprehensive privacy legislation the attention it deserves and not to rush to pass a bill this session.

---

[54] TLC DIRECT, https://www.tlcdirect.org (last visited Nov. 2, 2018).
[55] HEADCOVERS UNLIMITED, https://www.headcovers.com (last visited Nov. 2, 2018).
[56] Tim Murphy, *Inside the Obama Campaign's Hard Drive*, MOTHER JONES, Sept./Oct. 2012, https://www.motherjones.com/politics/2012/10/harper-reed-obama-campaign-microtargeting/.

The Committees are taking an important step by holding this hearing. In addition, the legislature is not starting from a blank slate. More than 105 privacy bills have been introduced this session, some of which contain good ideas. The remainder of this testimony will focus on S.5642, the New York Privacy Act, one of the bills specifically under consideration today.

Senator Thomas' S.5642 introduces a number of important ideas to the privacy debate in New York. Notably, the bill advances the concept of a data fiduciary,[57] recognizing that entities that collect, use, retain, share, and monetize personal information have specialized knowledge about the algorithms and security measures they use, as well as about how they collect, use, retain, share, and monetize personal information, that the average individual is unlikely to understand. Just as banks, lawyers, and medical providers, given their specialized knowledge, have special duties to individuals, entities collecting intimate personal information in the digital age and benefiting from similarly specialized knowledge should have similar obligations.

The bill also codifies a requirement that entities conducting business in New York State adhere to an individual's do not track selection,[58] something that is not required under current law. At present, although an individual can choose to add a do not track extension to her internet browser, websites can decide whether or not to honor the selection. Senator Thomas' bill would fix this problem and comport the law to individuals' expectations and desires.

The bill also contains important safeguards for individuals, including the ability to restrict the collection, processing, and transmission of their personal information, as well as access, correction, deletion, transparency, and data portability rights.[59] Finally, the bill contains some algorithmic decision-making protections.[60]

There are also areas where S.5642 could improve. For example, although the bill contains a robust and comprehensive list of privacy risks[61] – strongly suggesting that Senator Thomas has carefully considered what problems comprehensive privacy legislation should solve for – the data fiduciary section only obligates a covered entity to refrain from using personal information in ways that "will result in reasonably

[57] S.5642 § 2, 2019-2020 Reg. Sess. (N.Y. 2019).
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*

foreseeable and material physical or financial harm" to an individual.[62] Although these harms are important, financial harm, in particular, is among the least likely to occur. That is because when financial loss does arise from a data breach or misuse of data – say, where a credit card number is stolen and fraudulent purchases are made – it is often difficult to trace the stolen information to a particular privacy violation.[63] When it is possible to trace the financial harm back, banks often reimburse customers for fraudulent purchases, obviating any actual financial loss.[64] Physical harm, of course, can be devastating when it does occur. However, these two harms are a vanishingly small subset of the harms that can arise from the pervasive collection, sharing, monetization, use, and misuse of personal information.

The bill also fails to articulate whether the consent for personal information processing must be opt-in or opt-out.[65] This is important, because default is often destiny. Many individuals never change a site's default settings, meaning that significantly more personal information will be processed under an opt-out regime than under an opt-in regime.[66] This in turn matters because personal information is just that – personal – and individuals should be in the position to decide how, when, and why it is processed and with whom it is shared.

In addition, although S.5642 begins to tackle algorithmic decision-making, it does not do so holistically and fails to sufficiently address the civil rights harms that can arise from algorithmic decision-making, in part because the legislative language is not sufficiently airtight and in part because bill carves out public algorithmic decision systems.[67]

Finally, in addition to the important safeguards articulated in this bill and beyond, New Yorkers need digital literacy and digital privacy education that helps us to identify online fraud, as well as reliable sources and information, and that enables us to better understand how online activities are tracked and recorded, where personal information posted online may go, with whom it may be shared, how it may be used, and how to best protect our digital security and digital privacy. One of the reasons businesses and governments have so successfully convinced New Yorkers – and

---

[62] *Id*.
[63] *See* Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, WALL STREET J., June 26, 2016, https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.
[64] *Id*.
[65] S.5642 § 2, 2019-2020 Reg. Sess. (N.Y. 2019).
[66] Lena V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PRO PUBLICA, July 27, 2016, https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world.
[67] S.5642 § 2, 2019-2020 Reg. Sess. (N.Y. 2019).

individuals across the country – to give away the most intimate details of our lives is that many of us do not know what we are giving away. We do not know what data businesses collect, how our activities are tracked and recorded, where that information goes, or how it is used once it is collected. Part of the solution lies in requiring companies to be more transparent, to give individuals more choices, and to eschew some of their most problematic practices, but the other part of the solution lies in educating New Yorkers to better safeguard their own privacy and to make better choices about the ways in which they share and consume information in the digital age.

E. Conclusion

The NYCLU appreciates the opportunity to testify today and stands ready to assist the Committee, Chairman Thomas, and other interested legislators as you craft comprehensive privacy legislation for New York State.