



November 22, 2019

Senator Kevin Thomas  
Legislative Office Bldg.  
Room 947  
Albany, NY 12247

**Re: The New York Privacy Act**

Dear Senator Thomas:

I write today on behalf of the Electronic Frontier Foundation, a non-profit, non-partisan advocacy organization that works to protect civil liberties in the digital age. Thank you for the opportunity to offer feedback on S. 5642, The New York Privacy Act. EFF represents more than 30,000 active donors and members across the country dedicated to digital liberty, including a long history of fighting to protect online privacy. We have been deeply involved in the passage and amendment of the California Consumer Privacy Act, as well as in conversation with legislators considering privacy legislation in states across the country and at the federal level.

EFF believes that there are several components necessary for strong privacy laws that provide true consumer protections. Chief among these are a **private right-of-action** and **bans on pay for privacy**.<sup>1</sup>

We thank you for including a private right of action in the New York Privacy Act. This is a critical right for consumers. It is not enough for government to pass laws that protect consumers from corporations that harvest and monetize their personal data.<sup>2</sup> Such laws must also have bite, to ensure companies do not ignore them. The best way to do so is to empower ordinary consumers to bring their own lawsuits against the companies that violate their privacy rights.

Often, government agencies will lack the resources necessary to enforce the laws, or regulated companies will “capture” the agency, and shut down enforcement actions. Strong enforcement is vital to strong privacy law, and people should be empowered to act in the interest of their own privacy.

We do have a suggestion for how to strengthen the private right of action. As written, it is limited to people who have been injured by a violation of the statute. Some companies will argue that this means a person cannot bring a lawsuit based solely on the violation of their statutory privacy rights, but only if they can also prove a financial or physical injury. This would render the private right of action ineffective in many cases. So, we

---

<sup>1</sup> <https://www.eff.org/deeplinks/2019/06/effs-recommendations-consumer-data-privacy-laws>

<sup>2</sup> <https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy>

request that you remove this element of the private right of action, and allow anyone who has suffered a violation of their statutory privacy rights to bring a lawsuit.

Companies must also be unable to force consumers to pay for exercising their privacy rights. New legislation should include a ban on such pay-for-privacy schemes,<sup>3</sup> which forbid companies from denying goods, charging different prices, or providing a different level of quality to users who choose more private options.

Absent non-discrimination rules, companies will adopt and enforce “pay-for-privacy” schemes. But corporations should not be allowed to require a consumer to pay a premium, or waive a discount, in order to stop the corporation from vacuuming up—and profiting from—the consumer’s personal information. Pay-for-privacy schemes undermine the fundamental human right to privacy. They discourage all people from exercising that right. They also lead to unequal classes of privacy “haves” and “have-nots,” depending upon the income of the user.

In addition to the top priorities outlined above, EFF also champions a right to **opt-in consent**, a right to **know**, and a right to **data portability**.

- **Opt-in consent** is better than opt-out consent. The default should be against collecting, using, and sharing personal information. Many consumers cannot or will not alter the defaults in the technologies they use, even if they prefer that companies do not collect their information. Any request for opt-in consent should be easy to understand and tell people clearly what data companies want to gather, how they will use it, how long they will keep it, and with whom they will share it<sup>4</sup>. Such consent should be renewed any time the operator wishes to use or share data in a new way, or gather a new kind of data. And people should be able to withdraw consent, including for particular purposes, at any time.
- Users should have an affirmative “**right to know**” what personal data companies have gathered about them, where they got it, and with whom these companies have shared it—including the government. This includes the specific items of personal information, and the specific third parties who received it and provided it, and not just categorical descriptions of the general kinds of data, recipients, and sources. Companies must have an effective verification process to guard against fraudulent requests.<sup>5</sup> There are also some limits that can be placed on consumers’ right to know. For example, there needs to be an exception for news gathering,

---

<sup>3</sup> <https://www.eff.org/deeplinks/2019/02/payoff-californias-data-dividend-must-be-stronger-privacy-laws>

<sup>4</sup> <https://www.eff.org/deeplinks/2019/02/designing-welcome-mats-invite-user-privacy-0>

<sup>5</sup> <https://www.eff.org/document/eff-consumer-data-privacy-comment-california-attorney-general>

which is protected by the First Amendment, when undertaken by professional reporters and lay members of the public alike.

- Users should have a legal right to obtain a machine-readable, electronic copy of the data a business has collected about them. Such “**data portability**” lets a user take their data from a service and transfer or “port” it elsewhere.<sup>6</sup> This allows people to move their data to other services, and also provides an opportunity for people to analyze their own information. Regardless of whether you are “porting” your data to a different service or to a personal spreadsheet, data that is “portable” should be easy to download, organized, tagged, and machine-parsable.

We also note the New York Privacy Act’s inclusion of information fiduciary rules, which state that a company should have a duty to exercise loyalty and care in how it uses that information. EFF supports information fiduciary rules.<sup>7</sup> Professions that already follow fiduciary rules—such as doctors, lawyers, and accountants—have much in common with the online businesses that collect and monetize users’ personal data. However, such rules should not stand alone as a replacement for the other fundamental privacy protections.

Finally, as you continue to discuss the development of the New York State Privacy Act, we offer a few things to avoid when drafting laws to protect consumer privacy.

For one, data privacy laws should not expand the scope or penalties of **computer crime laws**—existing computer crime laws are already far too broad.<sup>8</sup> Second, any new regulations must be judicious and narrowly tailored, avoiding **tech mandates** that cannot be responsive to future developments. Third, policymakers must take care that any of the above requirements don’t create an unfair burden for small companies, nonprofits, open source projects, and similar groups. To avoid **one-size-fits-all rules**, they should tailor new obligations based on size of the service in question, or the entity’s revenue.

The above outlines some of the most important principles EFF would like policymakers to consider when drafting privacy legislation. Thank you for your attention and consideration, and for your work on this critically important issue.

---

<sup>6</sup> <https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability>

<sup>7</sup> <https://www.eff.org/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy>

<sup>8</sup> See, for example, our call for reforms to the Computer Fraud and Abuse Act: <https://www.eff.org/issues/cfaa>

EFF testimony regarding The New York Privacy Act  
November 22, 2019  
Page 4 of 4

We are eager to continue the conversation as you continue to develop this bill. Please reach out any time to Hayley Tsukayama, EFF's legislative activist, at [hayleyt@eff.org](mailto:hayleyt@eff.org) or 415-436-9333 x161.

Sincerely,

A handwritten signature in black ink, appearing to read "Hayley Tsukayama", with a long horizontal flourish extending to the right.

Hayley Tsukayama  
Legislative Activist  
Electronic Frontier Foundation  
(415) 436-9333 x 161