December 15, 2021

The Honorable T.J. Donovan, Attorney General
State of Vermont
109 State Street
Montpelier, VT 05609

Re: Prospective 2022 privacy legislation

Dear Attorney General Donovan,

Consumer Reports[1] sincerely thanks you for soliciting input into potential privacy legislation in the 2022 legislative session. Increased privacy protections are long overdue: consumers are constantly tracked, and information about their online and offline activities are combined to provide detailed insights into a consumers' most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

Consumer Reports has developed model state privacy legislation that we urge you to consider when pursuing a privacy bill.[2] This model law uses the California Consumer Privacy Act (CCPA) as a baseline,[3] and provides additional protections to ensure that consumers' privacy rights are respected by default. It reflects our position that privacy laws should set strong limits on the data that companies can collect and share so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out.

Above all, we recommend including in any privacy legislation a strong data minimization requirement that limits data collection, use and sharing to what is reasonably necessary to

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.
[2] *Model State Privacy Act*, CONSUMER REPORTS (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.
[3] Cal. Civ. Code § 1798.100 et seq.

provide the service requested by the consumer, as outlined in our model bill. A strong default prohibition on data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially thousands of different companies,[4] or an opt-in regime, in which companies could use coercive consent dialogs to push consumers to consent to inappropriate uses of their information. Consumer Reports has documented that some California Consumer Privacy Act (CCPA) opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[5] We recommend using the following language from our model bill to shape a data minimization requirement:

> (a) A business that collects a consumer's personal information shall limit its collection and sharing of that information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention. Monetization of personal information shall not be considered reasonably necessary to provide a service or conduct an activity that a consumer has requested or reasonably necessary for security or fraud prevention.
> (b) A business that collects a consumer's personal information shall limit its use and retention of that information to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a related operational purpose, provided that data collected or retained solely for security or fraud prevention may not be used for operational purposes.

However, should you choose to pursue opt-out legislation, for example, in the context of strengthening restrictions on data brokers or giving consumers the ability to opt out of the sharing or sale of their information at all companies, we recommend including the following provisions:

- *Global Opt Out.* In the absence of strong data minimization requirements, at the very least, consumers need tools to ensure that they can better exercise their opt-out rights, such as a global opt out (with a strong data minimization requirement, however, an opt out of sharing or sale to third parties is not necessary). CCPA regulations *require* companies to honor browser privacy signals as a "Do Not Sell" signal; Proposition 24 added the global opt-out requirement to the statute. The new Colorado law requires it as well.[6] Privacy researchers, advocates, and publishers have already created a "Do Not

[4] In contrast, California's Proposition 24 limits data processing to that which is necessary to carry out the purposes for which it was collected—which could incentivize companies to collect data for additional, unnecessary purposes. See Cal. Civ. Code § 1798.100(c), https://thecpra.org/#1798.100.
[5] *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Right*s, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.
[6] Cal. Code Regs tit. 11 § 999.315(c); CPRA adds this existing regulatory requirement to the statute, going into effect on January 1, 2023, at Cal. Civ. Code § 1798.135(e) https://thecpra.org/#1798.135. For the Colorado law, see SB 21-190, 6-1-1306(1)(a)(IV)(B), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.

Sell" specification, the Global Privacy Control (GPC),[7] which could help make the opt-out model more workable for consumers.[8]

- *Authorized agent opt outs.* Similarly, allowing consumers to delegate to third parties the ability to submit opt-out requests on their behalf can help provide a practical option for consumers to exercise their privacy rights in an opt-out framework. Consumer Reports has already begun to experiment with submitting opt-out requests on consumers' behalf, with their permission, through the CCPA's authorized agent provisions. We found that consumers are enthusiastic about this option.[9]

  Authorized agent services can be an important supplement to platform-level global opt outs, by allowing for opt outs of offline data, and to help ensure that consumers can opt out of the sale of information by data brokers, with which consumers' browsers may not necessarily interact. As in California, authorized agents should also be permitted to perform access and deletion requests on behalf of consumers, for which there is not an analogous tool similar to the GPC.

  We recommend using the following language to establish a browser privacy signal and authorized agent opt outs (within an opt-out framework):

  > Consumers or a consumer's authorized agent may exercise the rights set forth in [section numbers addressing access, deletion, and opt out rights] of this act by submitting a request, at any time, to a business specifying which rights the individual wishes to exercise. Consumers may exercise their rights under [section number addressing opt out rights] via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt out.

- *Controls over targeted advertising.* We recommend strong definitions of sharing or sale, personal information, and deidentification, as laid out in our model bill, to ensure that pseudonymous information is covered by the opt out—providing key consumer controls over ad tracking. In California, many companies have sought to avoid the CCPA's opt-

[7] Global Privacy Control, https://globalprivacycontrol.org.
[8] Another model to consider is Senator Wyden's Mind Your Own Business Act, which outlines a system to facilitate global opt-outs through registries as well as persistent opt-out signals for both unauthenticated and authenticated data. S. 1444, § 6 (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1444/text.
[9] Ginny Fahs, *Putting the CCPA into Practice: Piloting a CR Authorized Agent*, CONSUMER REPORTS (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8; Maureen Mahoney et al., *The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act*, CONSUMER REPORTS (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf.

out by claiming that much online data sharing is not technically a "sale"[10] (appropriately, Prop. 24 expands the scope of California's opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out).[11] For example, we recommend the following definition of sharing or sale, which is included in our model bill:

> "Share" [or sell] means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

Further, to be comprehensive, the definition of personal information should include information "that identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household, or consumer device."

- *No verification requirement for opting out*. Similarly, it's important to not require identity verification for opt-out requests. With a verification requirement, companies could require that consumers set up accounts in order to exercise their rights under the law—and hand over even more personal information. Consumers shouldn't have to verify their identity, for example by providing a driver's license, in order to opt-out of targeted advertising. Further, much of that data collected online (including for targeted advertising) is tied to a device and not an individual identity; in such cases, verification may be impossible, rendering opt-out rights illusory. In contrast, the CCPA pointedly does not tether opt out rights to identity verification.[12]

- *Strong enforcement*. So-called "right to cure" provisions in administrative enforcement, which was included in Virginia's Consumer Data Protection Act, have no place in privacy legislation. This "get-out-of-jail-free" card ties the AG's hands and signals that a company won't be punished for breaking the law. Further, given the AG's limited resources, a private right of action is key to incentivizing companies to comply. In addition, it's appropriate that consumers are able to hold companies accountable in some way for violating their rights. We would prefer a private right that would also afford consumers monetary relief, but empowering consumers to obtain injunctive relief and costs is a significant step forward.

---

[10] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs To Act*, CONSUMER REPORTS (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb; *The State of Authorized Agent Opt Outs*, *supra* note 9, at 16.

[11] Maureen Mahoney, *Consumer Reports Urges Californians to Vote Yes on Proposition 24*, CONSUMER REPORTS (Oct. 23, 2020), https://medium.com/cr-digital-lab/consumer-reports-urges-californians-to-vote-yes-on-proposition-24-693c26c8b4bd.

[12] Cal. Civ. Code § 1798.130(a)(2).

Below, we suggest several private right of action options to consider. Consumer Reports' model bill includes a private right of action based on the CCPA's private right of action for a negligent data breach. Key aspects of this language are that a violation is an injury in fact, and that there is a limited right to cure for certain violations where cure might be possible (notably, there is no right to cure with respect to the core substantive privacy protections).

> (a) A consumer who has suffered a violation of this Act may bring a lawsuit against the business that violated this Act. A violation of this Act shall be deemed to constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this Act.
> (b) A consumer who prevails in such a lawsuit shall obtain the following remedies:
> (1) Damages in an amount not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> (2) Injunctive or declaratory relief, as the court deems proper.
> (3) Reasonable attorney fees and costs.
> (4) Any other relief the court deems proper.
> (c) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.
> (d) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible and the behavior underlying the violations was unintentional, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. A cure shall not be possible for violations of sections 103, 104, 105, 110, 115, 120, 125, 126, 127, and 128. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.
> (e) A consumer bringing an action shall notify the Attorney General within 30 days that the action has been filed.

The New York Privacy Act, which Consumer Reports supports, includes a private right of action. However, it is less protective than that in CR's model bill, since it applies only to those who can show injury — potentially a high bar for privacy violations.[13]

> Any consumer who has been injured by a violation of section eleven hundred two of this article may bring an action in his or her own name to enjoin such unlawful act or practice and to recover his or her actual damages or one thousand dollars, whichever is greater. The court may also award reasonable attorneys' fees to a prevailing plaintiff. Actions pursuant to this section may be brought on a class-wide basis.

The Civil Rights & Judiciary Committee Striker of the 2021 Washington Privacy Act, language which Consumer Reports supports, has a modest private right of action, with injunctive relief only.[14] We would prefer a private right that would also afford consumers monetary relief, but empowering consumers to obtain injunctive relief and costs would be a significant step forward and would help incentivize compliance.

> A consumer alleging a violation of section 103 or 107 (6), 4 (8), or (9) of this act may bring a civil action in any court of competent jurisdiction. Remedies shall be limited to appropriate injunctive relief. The court shall also award reasonable attorneys' fees and costs to any prevailing plaintiff.

- *Non-discrimination.* Consumers have a fundamental right to privacy, and should not be charged for exercising their privacy rights. As outlined in our model bill, privacy legislation should strictly prohibit companies from offering a different price based on whether or not a consumer has opted out of the sale of their information. However, we have also supported compromise legislation in the Washington Privacy Act, which not only clarifies that consumers cannot be charged for exercising their rights under the law, but it makes it clear that legitimate loyalty programs, that reward consumers for repeated patronage, are supported by the law:

> A [business] may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subsection does not prohibit a [business] from offering a different price, rate, level, quality,

[13] The New York Privacy Act (2021), https://www.nysenate.gov/legislation/bills/2021/s6701.
[14] Civil Rights and Judiciary Committee (SB 5062), https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Amendments/House/5062-S2%20AMH%20CRJ%20H1373.1.pdf.

or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program. If a consumer exercises their rights pursuant to [section number] of this act, a [business] may not sell personal data to a third-party [business] as part of such a program unless: (a) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.[15]

- *Definition of consent and prohibition on dark patterns.* In the context of an opt in or opt out bill, a strong definition of consent can help ensure that privacy laws that are based on consent can be useful for consumers. Too often, companies often use dubious dark patterns to nudge users to click "OK," providing the veneer, but not the reality of, knowing consent.[16] We suggest the following language to consider, should you pursue consent-based legislation.

  (a) CONSENT.—
  (1) It shall be unlawful for a covered organization to collect, use, or disclose personal information unless
  (A) the individual to whom the data pertains has given affirmative express consent to such collection, use, or disclosure
  i) The general nature of the data processing shall be conveyed in clear and prominent terms in such a manner that an ordinary consumer would notice and understand them.
  ii) An individual may consent to data processing on behalf of his or her dependent minors
  (B) such collection, use, or disclosure is necessary and for the sole purpose of:
  a) protecting against malicious, deceptive, fraudulent, or illegal activity; or
  b) detecting, responding to, or preventing security incidents or threats; or
  (C) the covered organization is compelled to do so by a legal obligation.
  (2) REVOCATION.—
  (A) In General.— A covered organization shall provide an effective mechanism for an individual to revoke their consent after it is given.

[15] *Id.*
[16] *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent,* PRIVACY INTERNATIONAL (last visited Aug. 28, 2020), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.

(B) Effect.— After an individual revokes their consent, the covered organization shall cease collecting, using, or disclosing the individual's personal information as soon as practicable, but in no case later than 15 days after the individual revokes consent.

Further, a prohibition on dark patterns—deceptive interfaces that push consumers to take actions that they did not intend—can help ensure that consumers are able to exercise their preferences in a consent-based privacy law. Current CCPA regulations prohibit the use of dark patterns in CCPA opt outs;[17] and Proposition 24, which amends the CCPA and will go into effect in 2023, includes a prohibition of the use of dark patterns in obtaining consent, for example, consent to opt back into the sharing or sale of personal information.[18] Colorado's newly passed privacy law includes a nearly identical prohibition on dark patterns in obtaining consent.[19]

- *Data security requirements.* A comprehensive privacy bill would expand the definition of personal information to any information that could reasonably be linked, directly or indirectly, to a particular consumer, household, or device. As such, a privacy bill should ensure that the existing data security requirement in Vermont law covers this expanded definition of personal information, so that companies are required to use reasonable security protocols to safeguard the confidentiality and integrity of covered information. Information in online accounts and browsing activity can be very sensitive and should be protected from hackers.

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Vermont consumers have the strongest possible privacy protections.

Sincerely,

Maureen Mahoney
Senior Policy Analyst

Justin Brookman
Director, Technology Policy

[17] Cal. Code Regs tit. 11 § 999.315(h).
[18] Cal. Civ. Code §1798.140(h).
[19] Colorado Privacy Act, SB 21-190 (2021), https://www.google.com/url?q=https://leg.colorado.gov/bills/sb21-190&sa=D&source=editors&ust=1639343861044000&usg=AOvVaw3MQRCsi1rHmLyp9ppkB2Pl.