common sense kids action™

Considerations for Comprehensive State Privacy Proposals

March 2020

Privacy is essential to kids' safety and well-being, in the home, at school, and in our communities.[1] Common Sense Media, and its policy arm Common Sense Kids Action (together, "Common Sense"), has been active in advancing kids' and families' privacy rights at the state and federal level over the last two decades from student privacy protections to updates to the federal Children's Online Privacy Protection Act ("COPPA"), to co-sponsoring the California Consumer Privacy Act ("CCPA").

States are considering a variety of different privacy protections to student privacy rules, safeguards for connected toys, and restrictions on facial recognition. As states consider comprehensive privacy protections, Common Sense recommends that state proposals:

1. Include strong and clear definitions of what personal data is covered and how it can be de-identified;
2. Explain how companies collect, use, and share data in terms parents and kids can understand and provide easy mechanisms to access, delete, and move data;
3. Restrict secondary uses of information and mandate data minimization requirements;
4. Limit data disclosures to unknown third parties and business affiliates;
5. Include additional protections to safeguard the personal data of vulnerable children and teens, such as prohibitions on behavioral advertising and third-party disclosure;
6. Ensure any affirmative obligation on families or individuals to opt-out to protect their privacy be easy to effectuate and easily understandable and accessible;
7. Avoid overbroad and unnecessary exceptions for businesses who may be covered, usually only in part, by federal laws like COPPA;
8. Carefully consider what privacy and security requirements, if any, small businesses should be exempt from following;
9. Include reasonable data security provisions; and
10. Provide strong individual redress and enforcement mechanisms when companies violate an individual's privacy.

[1] According to a Common Sense Media survey, 97percent of parents and 94 percent of teens say it is "important" for sites to ask permission before selling or sharing their personal information.

common sense kids action™

I. CLEAR AND STRONG DEFINITIONS OF "PERSONAL INFORMATION" AND "DEIDENTIFIED INFORMATION" ARE ESSENTIAL

The actual protection provided by any privacy law fundamentally depends upon the definitions of (1) what "personal information/data" is covered and (2) what businesses have to do to de-identify that information to get out from the law.

1. **A broad definition of "personal information" or "personal data" is needed to protect privacy.** Historically, companies have taken a narrow view as to what information constitutes personal information -- obvious identifiers like name or Social Security numbers were all that needed to be protected. But when in-store shopping purchases can be used to infer pregnancy status and location to infer religion, and family loyalty club memberships and online browsing history are assessed by colleges before students even apply, more must be protected.[2] Laws like the CCPA recognize how sensitive and personal even seemingly innocuous data can be. Privacy law must also cover data no matter whether it is collected online or offline as this distinction has become meaningless as companies append and blend together data from my different sources.

   The inclusion of household-level data is especially important. Companies evade privacy rules by mislabeling data as "household-level information." The Data Marketing Association long argued that phone numbers were not personal information because they were associated with a household.[3] More recently, a coalition of industry trade associations argued that information used to identify individual mobile phones should not be viewed as personal information because "devices are often shared by several people and are not personally identifying."[4] Marketers and advertisers have also resisted the suggestion that IP addresses and other technical information can be personally identifiable information.[5]

---

[2] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html; Audie Cornish, *How Political Campaigns Are Using 'Geofencing' Technology To Target Catholics At Mass*, NPR (Feb. 6, 2020), https://www.npr.org/2020/02/06/803508851/how-political-campaigns-are-using-geofencing-technology-to-target-catholics-at-m; Douglas MacMillan & Nick Anderson, *Student tracking, secret scores: How college admissions offices rank prospects before they apply*, Washington Post (Oct. 14, 2019), https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/.

[3] Chris Hoofnagle, Comments on the CCPA (Mar. 8, 2019), https://hoofnagle.berkeley.edu/2019/03/08/comments-on-the-ccpa/.

[4] Letter from California Chamber of Commerce et al. to Senator Bill Dodd 4, Business Community Requests to Be Included in AB 375 Clean-Up Legislation (Aug. 6, 2018), *available at* https://www.eff.org/document/2018-08-06-calchamber-proposals-re-sb-1121.

[5] Jessica Rich, *Keeping Up with the Online Advertising Industry*, FTC BLOG (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

We support the broad definition of personal information included in the CCPA:

> *"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.*[6]

The CCPA also includes additional qualifiers and examples of information that can be personal information. Explicit callouts to inferential data, geolocation information, technical identifiers, and household-level information reflects needed pushback against existing industry proposals which are exceedingly narrow. Geolocation data, in particular, is highly sensitive, often revealing religious activities and health information, and is incredibly difficult, if impossible, to deidentify.[7] Lawmakers should resist any effort to carve out technical information from the definition of personal data.

2. **Definitions of "deidentified data" or "deidentified information" should not be so broad as to undermine a privacy bill's scope of coverage.** Deidentification has become tremendously contentious. Not only do deidentification techniques fail, but "anonymous" information can also present real risks to individuals and communities. While companies reasonably want an escape valve from having to give the same level of protection to all information at all times, businesses can be quick to claim information is sufficiently deidentified or even anonymous when it is not.[8]

   Scoping what information is properly de-identified warrants careful consideration. At minimum, we recommend using a standard based off of the Federal Trade Commission's ("FTC") three-pronged test that requires companies to:
   - Take "reasonable measures" to deidentify information;
   - Make a "public commitment" to process data in a deidentified fashion and not attempt to reidentify data; and
   - Contractually prohibit downstream recipients from reidentifying the data.[9]

---

[6] Cal. Civ. Code § 1798.140(o)(1).
[7] Stuart A. Thompson and Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html ("Yet companies continue to claim that the data are anonymous. In marketing materials and at trade conferences, anonymity is a major selling point — key to allaying concerns over such invasive monitoring.").
[8] Joseph Jerome, *De-Identification Should Be Relevant to a Privacy Law, But Not an Automatic Get-Out-of-Jail-Free Card* (Apr. 1, 2019), https://cdt.org/insights/de-identification-should-be-relevant-to-a-privacy-law-but-not-an-automatic-get-out-of-jail-free-card/.
[9] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, (2012).

common sense kids action™

II. COMPANIES SHOULD EXPLAIN HOW THEY COLLECT, USE, AND SHARE DATA IN UNDERSTANDABLE TERMS AND RIGHTS TO ACCESS, DELETE, AND PORT INFORMATION SHOULD BE EASY TO USE

People do not read privacy policies or terms of service,[10] and very few people think businesses do a good job explaining what they do with individuals' information. Only a third (36 percent) of teenagers agree that social networking sites do a good job explaining what they do with users' data, and nearly the same proportion (34 percent) disagree. Fifty-four percent of parents believe that social networking sites and apps do not do a good job explaining what they do with users' data.[11] While laws should move away from placing so much reliance on "notice and consent" for exercising privacy rights, it is still critical that companies describe plainly and clearly what they are doing.

Privacy laws should ensure that any disclosures are **(1) easily understood by the average consumer, (2) are accessible to individuals with disabilities, and (3) are available in the language primarily used to interact with the consumer**.[12] For example, privacy laws can require that disclosures:

- Use plain, straightforward language and avoid technical or legal jargon. Disclosures should be appropriate to the age and level of understanding of the user, which is particularly important where children or teenagers are concerned.[13]
- Use formats that draw the consumer's attention to the notice and makes the notice readable, including on smaller screens. Connected devices and other smart "Internet of Things" products raise special considerations and notices should be provided at the point of purchase or sale.[14]
- Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
- Be reasonably accessible to consumers with disabilities and for online notices, follow recognized industry standards such as the Web Content Accessibility Guidelines.

---

[10] David Kravets, *TOS Agreements Require Giving up First Born-and Users Gladly Consent*, Ars Technica (July 12, 2016), www.arstechnica.com/tech-policy/2016/07/nobody-reads-tos-agreements-even-ones-that-demand-first-born-as-payment/.

[11] Quarterly Survey Series, Common Sense Media and SurveyMonkey (June 11, 2018), https://www.commonsensemedia.org/research/quarterlysurveyseries.

[12] Cal. Civ. Code § 1798.185(a)(6).

[13] GDPR Recital 58.

[14] Somewhere at the point of purchase a product's information collection capabilities should be made clear, including what triggers information collection, where more information can be found, how security patches and updates are provided (and for how long), and whether the device can be used in 'dumb' mode.

Notice obligations are a start, but privacy laws like the CCPA go further by giving individuals more rights to their information. Individuals also should be given the ability to easily (1) access, (2) delete, and (3) move their personal information.

III. COLLECTION AND USE LIMITATIONS ARE NEEDED TO RESTRAIN PRIVACY-INVADING DATA PRACTICES

While giving individuals privacy rights can be an important first step, privacy legislation should place actual limits on the collection and use of data to ensure privacy by default. While the CCPA puts in place several new rights to data, the law's actual obligations are mainly related to providing disclosures at the point of collection and controls around selling data. There are no substantive restrictions on whether a business should collect information in the first place (provided it gives notice), nor are there limitations on how companies may use personal data for their own purposes.

The EU General Data Protection Regulation ("GDPR"), by contrast, requires that personal information being processed is **adequate**, **relevant**, and **limited to what is necessary**.[15] Other proposals in states across the U.S. attempt to implement minimization requirements and restrict secondary uses of information. (Secondary use is generally thought of as any use of personal data that is not necessary to fulfill the consumer's request or for other truly operational purposes like addressing fraud.) Unfortunately, many minimization proposals are often tied to limiting use to disclosures made in privacy policies that no one reads. This gives companies a huge amount of discretion. Any privacy requirement connected to a privacy policy disclosure will likely have minimal impact on privacy-invading business practices.

We recommend including provisions that affirmatively mandate companies minimize the amount of information they collect and restrict non-operational data uses without meaningful and informed consent:

> (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.*
> (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 directly related operational purpose, provided that data collected or retained solely for security or fraud prevention may not be used for operational purposes.*

IV. RESTRICTING DATA DISCLOSURES TO AND PROCESSING BY THIRD PARTIES AND BUSINESS AFFILIATES SHOULD BE TOP OF MIND

[15] GDPR Article 5(1).

While states like California and Nevada have enacted laws to address the sale of personal information (and serious legislation in Washington state also emphasizes data sales), lawmakers should focus on restricting disclosures to third parties and processing activities by companies individuals have not provided their information to. As privacy expert Chris Hoofnagle has documented, data brokers frequently engage in barter exchanges without "selling" information, even though the end result is the same for consumers.[16] Though the CCPA's definition of sale is broad enough to encompass such transactions for consideration, we have also seen advertising companies[17] and social media platforms[18] put forward contorted rationales for why they do not "sell" information since the CCPA went into effect in January 2020. **The end result is that companies are engaged in a range of unrelated and unnecessary business activities that undermine the privacy of families.**

We recommend legislation include broad definitions of "sale" and narrow any exceptions for "business purposes" or "operational purposes." Including an exception that lets companies determine that their actions are "consistent with a consumer's reasonable expectations" is incredibly broad and an invitation to let businesses collect, use, and trade personal information without restraint. Consumer expectations are impossible for companies to know generally, so there is no reason to expect businesses can determine what sort of data sharing individuals actually want.[19]

We also recommend restricting disclosures among business affiliates. A June 2019 Pew survey found that only 29% of those surveyed knew that Facebook owned Instagram,[20] and few consumers truly comprehend the tangled web of corporate affiliates that freely share data among themselves. If an individual cannot clearly understand that the personal information they provide to a business will be shared with an affiliate, this sharing is inappropriate.

---

[16] Chris Hoofnagle, Comments on the CCPA (Mar. 8, 2019), https://hoofnagle.berkeley.edu/2019/03/08/comments-on-the-ccpa/.

[17] Coalition Letter to the Interactive Advertising Bureau re: CCPA Compliance Framework for Publishers & Technology Companies (Nov. 5, 2019), *available at* https://advocacy.consumerreports.org/wp-content/uploads/2019/11/Consumer-and-Privacy-Group-Comment-on-IAB-CCPA-Framework.pdf.

[18] Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, Wall St. J. (Dec. 12, 2019), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345.

[19] *See* Carolyn Nguyen, Director, Microsoft Technology Policy Group, Contextual Privacy, Address at the FTC Internet of Things Workshop (Nov. 19, 2013), *available at*: http://www.ftc.gov/sites/default/files/documents/public_events/internet-thingsprivacy-securityconnectedworld/final_transcript.pdf.

[20] *See, e.g.*, Melissa Locker, *Did you know Facebook owns Instagram? Most Americans don't*, Fast Company (Oct. 9, 2019), https://www.fastcompany.com/90415447/did-you-know-facebook-owns-instagram-most-americans-dont.

common sense kids action™

V. ADDITIONAL PROTECTIONS ARE NEEDED TO SAFEGUARD THE DATA OF CHILDREN AND TEENS

Children's information is especially sensitive. Kids' privacy protections have been a focus for families and policymakers at the state and federal level, and special protections for minors have been a key piece of both the CCPA and the GDPR.[21] For example, the GDPR recognizes that because children are "less aware of the risks, consequences and safeguards" of data processing, they merit "specific protections" when children's data is used for marketing or collected to create a user profile.[22] Children and teens' information should not be tracked or shared without their or their parents' opt-in consent. Certain practices, like behavioral advertising, should be off limits for minors.

First, we would recommend that the data of minors be defined as sensitive and be subject to opt-in consent requirements. This is consistent with the CCPA, which provides an opt-in to the sale of information for consumers less than 16 years of age.[23] Specifically, the CCPA mandates:

- For children under 13, parents or guardians must provide affirmative authorization before a business is permitted to sell the personal information of children.
- For teens aged 13-15, a minor must provide affirmative authorization before a business is permitted to sell their personal information.

Other proposals would extend these opt-in consent requirements to minors under 18, as well.

Second, certain particularly problematic practices should be off limits. Commercially tracking and profiling children and teens to serve them behavioral ads based on their personal information or online activity should not be allowed. There should be no fiction of consent in this situation.

Third, we would caution against assigning opt-in consent requirements to parents or guardians for teenagers. Teens should be treated differently from eight-year-olds, and mandating that parents provide consent before a teenager can use any app or share their personal information is likely to encourage teens to lie, could inadvertently "out" teens to parents, and will ultimately undermine teenagers' privacy rights.

Lastly, it is essential to prevent businesses from being willfully ignorant of children accessing their sites, services, or products. The CCPA addresses ongoing concerns that businesses effectively bury their head in the sand when it comes to collecting information from children:

---

[21] Ariel Fox Johnson, *Improving COPPA: A Road Map for Protecting Kids' Privacy in 2020 and Beyond*, *Common Sense Kids Action* (Jan. 30, 2020), https://www.commonsensemedia.org/kids-action/blog/improving-coppa-a-road-map-for-protecting-kids-privacy-in-2020-and-beyond.

[22] GDPR Recital 38.

[23] Cal. Civ. Code § 1798.120(c).

- Businesses must comply if they have "actual knowledge" of a consumer's age, which under the CCPA includes businesses "who willfully disregard a consumer's age."[24]

The legal concept of actual knowledge is "[k]nowledge of information that would lead a reasonable person to inquire further."[25] Unfortunately, due to successful lobbying by companies at the FTC,

"actual knowledge" is more strictly interpreted in the age context and many companies will claim that they do not know someone is a child if they do not know their birthdate -- even though they tell advertisers they can reach a individual 10-year-old, or even though the company tracks a child to and from middle school while watching TV shows aimed at fourth graders. Any state privacy law should prevent companies from being willfully ignorant of children accessing their services. The problem with including protections only for "known child[ren]" as in some proposals is that companies may think the best practice is to avoid gaining strictly interpreted actual knowledge in the first place.[26]

The CCPA's inclusion of willful disregard of a user's age is consistent with global moves to better protect children's privacy. Indeed, it does not even go as far as many proposals, which are even better for kids. Some proposals that sites be liable if they have actual or constructive knowledge of children.[27] And the UK's Age Appropriate Design Code applies to all sites "likely to be accessed by children."[28]

VI. INDIVIDUALS SHOULD NOT HAVE TO JUMP THROUGH UNNECESSARY HOOPS IN ORDER TO MAKE PRIVACY CHOICES, INCLUDING COMPLICATED "OPT-OUTS"

We generally support opt-in provisions before personal information is collected, used, or shared. Opt-out rights or other protections that occur after-the-fact have a long history of being hard-to-use and difficult-to-find, often by design so individuals do not take advantage of their rights.[29] Defaults are sticky and hard to change.

---

[24] Cal. Civ. Code § 1798.120(d).
[25] Actual Knowledge, Black's Law Dictionary (11th ed. 2019).
[26] The Future of the COPPA Rule: An FTC Workshop, (Oct. 7, 2019) (Panel 1, statement of Laura Moy, Associate Professor, Director of the Communications & Technology Law Clinic, and Associate Director of the Center on Privacy & Technology at Georgetown University Law Center).
[27] COPPA 2.0.
[28] U.K. ICO Age Appropriate Design Code, "Services Covered" https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.
[29] *See* @jasonkint, Twitter (Jan. 1, 2020), https://twitter.com/jason_kint/status/1212431443772788737; *see also* Jack Marshall, *Is AdChoices a Waste of Time?*, Digiday (Apr. 9, 2013), https://digiday.com/marketing/is-adchoices-a-waste-of-time/.

Any provisions that require affirmative choice should minimize burdens on consumers. For example, any opt-out provision should give individuals an ability to globally opt-out of privacy invading practices. Dozens of companies and data brokers operate different opt-out controls. It is not possible for an individual to self-manage their privacy, and burdening adults, let alone teenagers, to individually opt-out from data disclosures from every company they come across is neither fair nor practical. [30]

The California Attorney General is considering regulations under the CCPA that may treat browser- or device-based "Do Not Track" signals as a binding opt-out request. Specifically, one version of the proposed regulations state that:

> *A business shall treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out.*[31]

We recommend this approach.

VII. AVOID OVERBROAD EXCEPTIONS FOR BUSINESSES THAT MAY ALSO HAVE OBLIGATIONS UNDER FEDERAL LAWS (COPPA, FERPA, HIPAA, GLBA, ETC.)

Industry stakeholders continue to push for carve outs for their privacy-invasive protections, often justifying these exceptions on the grounds that they are already regulated by federal privacy laws. These exemptions are often unwarranted. The Health Insurance Portability and Accountability Act ("HIPAA"), Gramm-Leach-Bliley Financial Modernization Act ("GLBA"), and the Children's Online Privacy Protection Act ("COPPA") each allow states to provide stronger protections for health, financial and children's information that go beyond federal protections. Further, the federal laws often only apply in limited circumstances. HIPAA, for example, only applies to information collected by "covered entities," which does not cover the complete universe of health information that can be collected by apps and services online. COPPA applies to a limited set of operators of sites and services, and does not apply to telecommunications carriers or solely brick and mortar companies.

We are particularly concerned with privacy proposals that exclude entirely from their coverage data regulated by COPPA. These exceptions are redundant and unnecessary. COPPA already preempts inconsistent state laws, and any proposal that touches on privacy protections for children or teens should not automatically be deemed as inconsistent with federal law. Otherwise, these exceptions leave children open to gaps in protection. Further, the Federal Trade

---

[30] Danial Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review 1880 (2013).
[31] California Attorney General, CCPA First Modified Regulations (Feb. 07, 2020), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf.

Commission, which enforces COPPA, has made clear that states are empowered to offer protections to teenagers aged out of the COPPA framework.[32]

State lawmakers must not include carve outs without careful consideration and debate, and exceptions should be tailored to specific concerns, not provide a blanket exemption from state privacy protections.

VIII. ENSURE SMALL BUSINESSES ALSO PROTECT INDIVIDUALS' PRIVACY

The concern that requiring small businesses and startups to take consumer privacy seriously is an unfair burden may be well-intentioned, but exempts small businesses from any responsibility to take care of the information they collect about their customers. The reality is that many smaller apps and companies collect information from children, in school and at home.

While we recognize the practical need for a sliding scale for compliance, we do not believe it should be based purely on the size of a company. Further, requirements to secure information and provide access, correction, and deletion rights are obligations *any* business can meet. If a customer requests to know what information a business holds about her, there is no principled reason why even a small business should refuse such a request.

Where privacy laws can become burdensome on small business is when they become overly prescriptive and heavy on record-keeping or reporting requirements. For instance, the proposed Washington Privacy Act asks companies to undertake risk assessments for their use of information. These sorts of assessments are common for Fortune 500 businesses and companies engaged in sophisticated data mining and data analytics practices that already demand the attention of privacy lawyers. Exempting mom-and-pop shops from these sorts of practices may be warranted -- especially if mom-and-pop shops do not partake in data mining and consumer profiling. The GDPR, for example, requires comprehensive documentation and record-keeping of how companies think about privacy, but lessons some of the record-keeping requirements for businesses with less than 250 employees that process information only occasionally.[33]

We recommend any privacy legislation take into account a company's business model, such as whether the company makes a certain amount of profit from processing, selling, or sharing data. The CCPA applies based on a business' revenue, sheer number of individuals whose data is processed, or if a company is generally engaged in data processing activities such that it derives 50% of more of its annual revenues from data sales.

---

[32] *See* Amicus Brief, Fraley v. Facebook *available at* Press Release, FTC Files Amicus Brief Clarifying Role of Children's Online Privacy Protection Act (Mar. 21, 2014), https://www.ftc.gov/news-events/press-releases/2014/03/ftc-files-amicus-brief-clarifying-role-childrens-online-privacy.

[33] GDPR Article 30(5).

common sense kids action™

IX. ESTABLISH RIGOROUS DATA SECURITY REQUIREMENTS

Too often ignored in privacy debates is the need also to ensure that information is collected and stored securely. If information is not kept securely and open to attack, even the best privacy practices will offer little protection. Lax data security continues to be a problem that faces families whenever they incorporate technology into their homes and daily lives. The growth of always-on devices and "Internet of Things" offerings for children must be met with additional protections to preserve children's privacy in the home and beyond.[34] Yet concerningly, security on these devices is often lacking.[35]

While data security requirements may be paired with privacy and breach notification legislation, it is not uncommon for security to be absent or to receive less focus than breach notification or privacy requirements.[36] **This is particularly problematic where states propose privacy laws with a definition of "personal information" that diverges from the definition used in separate breach or security laws, creating gaps in protection.**

We recommend including reasonable security requirements in any privacy proposal. One model is California's SB 327, which mandates that connected devices must be equipped with a security feature that is designed to protect personal information in the device, appropriate to the device and the nature of the information. Detailed security requirements can be helpful, but sometimes can become obsolete too soon. At minimum, lawmakers should include minimum reasonable security requirements:

> *A business or service provider shall implement and maintain reasonable security procedures and practices, including administrative, physical, and technical safeguards, appropriate to the nature of the information and the purposes for which the personal information will be used, to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification.*

X. CONSUMERS DESERVE STRONG REDRESS AND ENFORCEMENT MECHANISMS

A privacy law is only as strong as how it is enforced. In just the first month of 2020, we have seen:

---

[34] Common Sense Kids Action, *Good and Bad Toys for Families* (Apr. 20, 2017), https://www.commonsensemedia.org/kids-action/blog/good-and-bad-toys-for-families.

[35] See generally Gordon Chu et al., Security and Privacy Analyses of Internet of Things Toys, 6 IEEE INTERNET OF THINGS J. 978 (2019), https://arxiv.org/pdf/1805.02751v1.pdf. The "smart pet" the paper tested is a Cloudpet, which Amazon and other retailers subsequently pulled due to its security vulnerabilities. Alfred Ng, *Amazon Will Stop Selling Connected Toy Filled with Security Issues*, CNET (June 5, 2018), https://www.cnet.com/google-amp/news/amazon-will-stop-sellingconnected-toy-cloud-pets-filled-with-security-issues/.

[36] Harley Geiger, *Updating Data Security Laws - A Starting Point*, Rapid7 (May 4, 2018), https://blog.rapid7.com/2018/05/04/updating-data-security-laws-a-starting-point/.

- A facial recognition vendor scrape millions of photos from social media platforms and the internet to match any photo of unknown people to their online images without any notice, consent, or easy way to opt-out;[37]
- Dating apps be accused of sharing dating choices and precise location with advertising and marketing companies in violation of existing privacy laws;[38] and
- Widespread failures to comply with the spirit of the CCPA's data access and deletion provisions.[39]

We recommend providing expansive redress and enforcement mechanisms in any proposal. There are a variety of ways to strengthen enforcement:

1. At a baseline, additional significant financial and personnel support must be provided to the state Attorney General. This is critical in order for any privacy law to be effective.
2. Cities and localities should be equal partners in enforcement.
3. Private rights of action should be included to empower individuals to enforce their rights.

1. **Attorneys General must be given sufficient resources and incentives to enforce privacy laws.** The California Consumer Privacy Act ("CCPA") illustrates the importance of dedicated resources for enforcement. With its passage, Common Sense worked hard to ensure the California Attorney General had sufficient resources to enforce the law, supporting a $700,000 funding bill for CCPA enforcement. Even with this additional funding, the California Attorney General has conceded that it will likely prosecute no more than **three cases per year** under the CCPA.[40] (Similarly, the Washington Attorney General anticipated that an additional 3.5 full-time employees would be sufficient for three investigations per year under the Washington Privacy Act.) This degree of enforcement is inadequate to address the challenge before us.

   Companies also must not be given free passes for violating the law. "Rights to cure" violations of the law prior to being subject to any potential fine by the Attorney General is inappropriate. This places an undue strain on the Attorney General's already limited investigative resources and lets companies get away with bad behavior until they are caught.

---

[37] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[38] Natasha Singer & Aaron Krolik, *Grindr and OkCupid Spread Personal Details, Study Says*, N.Y. Times (Jan. 13, 2020), https://www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html.
[39] Greg Bensinger, *So far, under California's new privacy law, firms are disclosing too little data — or far too much*, Wash. Post (Jan. 21, 2020), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/.
[40] Yuri Nagano, *California Attorney General Plans Few Privacy Law Enforcement Actions, Telling Consumers to Take Violators to Court*, S.F. Public Press (May 15, 2019), https://sfpublicpress.org/news/2019-05/california-attorney-general-plans-few-privacy-law-enforcements-telling-consumers-to-tak.

2. **Cities and localities should be permitted to enforce any state privacy law, and any preemption of their ability to enact stronger protections should be limited.** The movement toward "smart cities" and public-private partnerships have given cities an important interest in ensuring companies are responsible partners that protect citizens' privacy. Cities can also act as enforcement multipliers. City attorneys have proven

   themselves to be strong privacy enforcers across the country, and they should be permitted to enforce state privacy laws.[41]

3. **Private rights of action can be an effective tool for individuals to obtain redress and combat bad practices for the benefit of all.**[42] While Attorneys General often must look for patterns of abuse, this ignores privacy harms at the individual level and accepts non-compliance as inevitable.

   It is important to note that lawmakers can scope a private right of action to avoid any alleged excessive litigation. For instance, a private right of action could minimize statutory damages and emphasize injunctive relief. Injunctive relief forces companies to stop practices that violate the law. This is a good potential middle ground, and has precedent in federal law. For example, Title III of the Americans with Disabilities Act prohibits discrimination on the basis of disability in places of public accommodation, but private plaintiffs are only allowed to seek equitable relief like removals of barriers or obstacles rather than any financial awards.[43] Another option modeled after the Fair Credit Reporting Act[44] is to specify exactly which provisions in a privacy law could be subject to private litigation. The CCPA, for example, permits a private right of action for certain data breaches.

---

[41] *E.g.*, Sam Dean, *L.A. is suing IBM for illegally gathering and selling user data through its Weather Channel app*, L.A. Times (Jan. 4, 2019), https://www.latimes.com/business/technology/la-fi-tn-city-attorney-weather-app-20190104-story.html. *See generally* Ira Rubinstein, *Privacy Localism*, 93 Wash. L. Rev. 1961 (2018), *available at:* http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1853/93WLR1961.pdf (arguing that local privacy efforts have the potential to help shape emerging privacy norms for an increasingly urban future, inspire more robust regulation at the federal and state levels, and inject more democratic control into privacy-invasive technology).

[42] *E.g.*, Joseph Jerome, *Private right of action shouldn't be a yes-no proposition in federal US privacy legislation*, IAPP Privacy Perspectives (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/.

[43] Arlene Haas, *Essential Guide to ADA Title III Enforcement: Private Party Lawsuits* (Jan. 10, 2017), https://www.burnhamnationwide.com/final-review-blog/essential-guide-to-ada-title-iii-enforcement-private-party-lawsuits.

[44] *See, e.g.*, Alexandra Everhart Sickler, *The (Un)Fair Credit Reporting Act*, 28 Loy. Consumer L. Rev. 238 (2015-2016).