The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

VIA EMAIL TO: Eleanor Blume (eleanor.blume@doj.ca.gov) and privacyregulations@doj.ca.gov

March 8, 2019

Dear Attorney General Becerra,

The Future of Privacy Forum (FPF) respectfully submits the following comments regarding the implementation of the California Consumer Privacy Act of 2018 (CCPA).[1]

FPF is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF is supported by the privacy officers of more than 150 companies and by leading foundations, with an advisory board of academic, civil society and industry members. We bring together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.[2]

We commend the Office of the Attorney General (AG) for its sincere and multi-faceted solicitation of feedback from diverse stakeholders and the public in recent months, including through public forums, testimony before the California Assembly, and requests for comments. Specifically, the AG has requested input on several enumerated areas outlined in Cal. Civ. Code § 1798.185. We respond primarily to these topics, and hope that our associated resources can assist the AG's office in its efforts to craft well-informed and meaningful rules and guidance.

We write to:

1. ***Commend the State of California for addressing important data protection rights, including transparency, access, deletion, and reasonable security, for personal information.*** California has long been a leader in data privacy, and in the last year has served as a legislative model for other states as well as sparking a serious national conversation regarding a federal privacy law. While FPF supports a strong, comprehensive, baseline federal privacy law, we believe that states that do advance legislation should do so in ways that provide consumers with comprehensive protections that are in line with the Fair Information Practice Principles (FIPPs) and take into account interoperability with the EU General Data Protection Regulation (GDPR).

2. ***Recommend that rule-making efforts recognize that data exists on a spectrum of identifiability.*** While some data is firmly linked to an individual or provably non-linkable to a person, significant amounts of data exist in a gray area — obfuscated but potentially linkable to an individual under some circumstances. We recommend that the AG take account of this spectrum of identifiability and provide incentives for companies to de-identify data using technical, legal, and administrative measures.

---

[1] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.198(a) (2018) (hereafter "CCPA").
[2] The views herein do not necessarily reflect those of our supporters or our Advisory Board.

3. ***Encourage further analysis of the impact of CCPA on socially beneficial research by non-HIPAA entities.*** Although CCPA excludes health data regulated by the Health Insurance Portability and Accountability Act (HIPAA) and related laws, its provisions govern private companies that may choose to conduct socially beneficial research using non-HIPAA data, including: consumer wearable manufacturers; health-related mobile apps; and genetic testing companies. While these companies should surely be subject to data privacy rules, we recommend that the AG take a close look at specific areas where beneficial research can be enabled or facilitated, or where restrictive requirements may pose particular challenges for researchers.

4. ***Encourage the AG to establish guidelines for data subject access requests (DSARs) that are secure, practical, and meaningful for consumers.*** The right to access one's personal information is a fundamental tenet of the FIPPs, as well as a central feature of privacy laws in the United States and around the world. At the same time, there are inherent risks for some businesses in complying with data subject access request (DSARs), and often a direct tension between access rights and other important privacy safeguards. Ultimately, access requests should be secure, practical for businesses, and meaningful for consumers.

5. ***Recommend greater clarity on the intersection of CCPA and existing student privacy laws governing education technology vendors.*** For the benefit of schools, administrators, and education technology ("edtech") vendors, the AG should clarify key points of CCPA that are applicable to education and student privacy, including: edtech vendors' CCPA obligations (if any) when they act solely on behalf of public schools or districts; the circumstances under which edtech vendors may be considered "service providers" under the law; and alternately, how edtech vendors may navigate compliance obligations of CCPA in line with federal laws governing student records and California's existing student privacy laws.

We have attached a list of other relevant resources following this letter, including FPF publications on a variety of commercial privacy topics that may be of interest to the AG. We hope that our comments and the associated resources will be helpful to the important, ongoing discussion regarding consumer privacy in the State of California.

1. Addressing privacy through comprehensive data protection rights

The Future of Privacy Forum (FPF) has long supported a comprehensive, baseline federal privacy law that would fill the gaps between existing sectoral regimes and provide both regulatory clarity for businesses and a consistent set of protections for individuals across state lines.[3] Although we are encouraged by recent legislative activity in Congress, the path to a national law remains uncertain. In the absence of a federal law, states that do advance legislation should seek to do so in ways that provide consumers with comprehensive protections in line with the Fair Information Practice Principles (FIPPs) and taking into account interoperability with the EU's General Data Protection Regulation (GDPR).[4]

---

[3] Long Overdue: Comprehensive Federal Privacy Law, Future of Privacy Forum (Nov. 15, 2018), https://fpf.org/2018/11/15/fpf-comments-on-a-national-baseline-consumer-privacy-law/ (last visited Mar. 8, 2019); FPF Comments to the U.S. Department of Commerce, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (2018), https://www.ntia.doc.gov/files/ntia/publications/ntia_request_for_comments_future_of_privacy_forum.pdf.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj. (hereafter "GDPR").

For these reasons, we commend the State of California for addressing several key data protection rights—including transparency, access to data, deletion, and reasonable security—that are aligned with global norms as well as with long-standing American traditions. Privacy as a common law right in the United States was established over a hundred years ago,[5] later codified in the Second Restatement of Torts,[6] and written into the constitutions of many states, including California, to explicitly protect the right to privacy and private life.[7] Comprehensive privacy values were articulated more fully in 1973 in the globally influential FIPPs published by the U.S. Department of Health, Education, and Welfare.[8] The FIPPs have since been embodied in United States and international laws, including the EU's GDPR.

As the AG considers additional rule-making and guidance to further the purposes of the CCPA, the FIPPs can provide a foundation for a holistic view of data protection that goes beyond notice and choice, including principles of: individual control, respect for context, focused collection, and responsible use, security, and accountability.[9] In some areas, GDPR may also serve as a reference for U.S. lawmakers, with an understanding that the U.S. approach to privacy will likely diverge from the EU in some areas, such as in the breadth of data subject rights, or in balancing privacy with other constitutional values, including the First Amendment. **See Attachment 1** (Comparing Privacy Laws: GDPR vs. CCPA).

2. Data identifiability and personal information

The concept of "personal information" and its related aspects—including de-identification, anonymization, and pseudonymization—are at the crux of all privacy regulation, and the focus of considerable attention in a growing body of technical and legal literature. FPF has many years of significant experience working with experts on a range of modern de-identification practices, and a core part of our mission is to help identify and develop leading practices on this issue.[10] We observe that most personal information exists on a spectrum of identifiability, and recommend that lawmakers find ways to incentivize companies to reduce data identifiability, while addressing the challenges that it may present for compliance with other privacy safeguards (such as access to data, discussed below).

We first note that CCPA's broad definition of personal information is in many respects aligned with existing legal standards[11] and evolving norms[12] in the United States, as

---

[5] Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[6] Restatement (Second) of Torts § 652B-E (1977) (describing the four privacy torts: Public Disclosure of Privacy Facts; Intrusion upon Seclusion; False Light; and Appropriation of Name or Likeness).
[7] The constitutions of eleven U.S. states have specifically enumerated rights to privacy or private life. *Privacy Protections in State Constitutions*, National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (last visited Mar. 8, 2019), including, of course, California. Cal. Const., art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining . . . privacy.").
[8] Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health & Human Services, https://aspe.hhs.gov/report/records-computers-and-rights-citizens (last visited Mar. 8, 2019).
[9] Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health & Human Services, https://aspe.hhs.gov/report/records-computers-and-rights-citizens (last visited Mar. 8, 2019).
[10] *See generally, e.g.,* De-Identification 201 Secure Multi-Party Computation Webinar, Future of Privacy Forum (Feb. 12, 2018), https://youtu.be/_B1wdzFWpD0 (last visited Mar. 8, 2019); De-Identification 201 Differential Privacy Webinar, Future of Privacy Forum (Feb 16, 2018), https://www.youtube.com/watch?v=oKT-RrX82x0&feature=youtu.be (last visited Mar. 8, 2019); Digital Data Flows Masterclass, Future of Privacy Forum (2018) (Class Three), https://fpf.org/classes-archives/ (last visited Mar. 8, 2019); Brussels Privacy Symposium, Future of Privacy Forum (2016), https://fpf.org/brussels-privacy-symposium/ (last visited Mar. 8, 2019).
[11] *See, e.g.*, the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506. Personal information under COPPA includes "persistent identifiers," defined as "identifier[s] that can be used to recognize a user over time and across different Web sites or online services . . . [including] a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier." 16 C.F.R. § 312.
[12] Jessica Rich, *Keeping Up with the Online Advertising Industry*, Federal Trade Commission (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

well as with the broad definition of personal data in GDPR.[13] To the extent that there is uncertainty around this alignment, for example due to the inclusion in CCPA of the term "inference" or the phrase "capable of being associated with," we recommend that the AG provide clarification using existing U.S. laws and the GDPR as points of reference. Similarly, the inclusion of "household data" in CCPA may be perceived as broader than typical statutory descriptions of personal information. In most cases we are aware of, a household is reasonably linked to an identifiable person. However, this an area where the AG can create guidance that would reduce confusion, including for businesses that process data related to, for example: residential buildings; real estate; smart meters; utilities; or data from "smart homes."

Within this range of "personal information" defined broadly in CCPA, it is important to note that most data exists on a spectrum of identifiability. **See Attachment 2: A Visual Guide to Practical De-Identification.** While some data is firmly linked to an individual or provably non-linkable, significant amounts of data exist in a gray area – obfuscated, but potentially linkable to an individual under some circumstances. As a result, determining when data is no longer "personal" and may be considered "de-identified" is a complex technical and legal question. According to the Federal Trade Commission (FTC), data are not "reasonably linkable" to an individual to the extent that a company: (1) takes reasonable measures to ensure that the data are de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data (the "Three-Part Test").[14] Commercial entities operate within this legal framework and take this definition into account, often in addition to standards of de-identification found in other longstanding U.S. federal laws.[15]

In contrast, under GDPR, information is considered "anonymous" when it "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[16] GDPR requires taking into account "all the means reasonably likely to be used" to identify an individual, including whether an individual can be "singled out" by a controller or another person.[17] In determining "all means" reasonably likely to be used, GDPR also takes into account "all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."[18]

In addition, GDPR creates legal incentives for "pseudonymisation," defined as a process which results in personal data not being able to be attributed to a specific person without the use of additional information, provided that this information is kept separately and is subject to technical and organisational measures.[19] While many GDPR safeguards still apply to "pseudonymized personal data," the regulation nonetheless provides incentives for organizations to rely on pseudonymization by, for example: recognizing that pseudonymization is an appropriate safeguard to legitimize

---

[13] The GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject') . . . directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, Art. 4(1)(1).
[14] Protecting Consumer Privacy in an Era of Rapid Change, Federal Trade Commission (2012), at 21, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[15] The Health Insurance Portability and Accountability Act (HIPAA) defines de-identified data as "information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information." 45 CFR § 164.514(a). Under the Family Educational Rights and Privacy Act (FERPA), records are considered de-identified "after the removal of all personally identifiable information provided that the educational agency or institution or other party has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information." 34 CFR § 99.31(b)(1)).
[16] GDPR, Recital 26.
[17] *Id*.
[18] *Id*.
[19] GDPR, Art. 4(5).

processing for additional, compatible purposes to the initial ones;[20] or to ensure compliance with the obligation of "data protection by design";[21] as a measure of security of processing;[22] or to allow processing of personal data for scientific research.[23]

In many cases, the ability to fully or partially de-identify personal data through technical, legal, and administrative measures will allow a company to retain some utility of data (e.g., for research, as we discuss below), while significantly reducing privacy risks. New advances in de-identification and related privacy-enhancing technologies (PETs) are continuing to emerge, including development of approaches such as differential privacy, synthetic data, and secure multiparty computation.[24] As a result, it is wise for lawmakers to find ways to incentivize companies to reduce data identifiability, while recognizing that it may create challenges for compliance with other consumer rights, such as data subject access request (DSARs).

Overall, we recommend that the AG be aware of the complexity and breadth of legal and technical literature on this topic. We hope our resources in this field can be of assistance to the AG and are available to engage further.

3. Enabling socially beneficial private research

We encourage the AG to interpret and implement CCPA, to the greatest extent possible, in ways that support meritorious, socially beneficial academic and private research in fields such as medicine, public health, or environmental impact. Although CCPA excludes data regulated by the California Medical Information Act (CMIA), the Health Insurance Portability and Accountability Act (HIPAA), and Federal Policy for the Protection of Human Subject ("the Common Rule"),[25] its provisions govern many companies that conduct similar research, such as: consumer wearable manufacturers; health-related mobile app developers; and genetic testing companies.

For example, it is helpful that CCPA contains an exception to consumer deletion requests for data that is necessary to engage in *"peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws . . . if the consumer has provided informed consent."*[26] An important way that the AG might further enable beneficial research might be to permit companies to meet this requirement through self-regulatory mechanisms that are approved by the AG. Examples of self-regulatory mechanisms that the AG might approve include:

- *Voluntary compliance with the Common Rule.* The Common Rule provides ethical standards for research involving human subjects that is conducted, supported, or otherwise subject to regulation by federal agencies.[27] Companies that are not subject to the Common Rule often comply with its requirements voluntarily, receiving approval from an institutional review board (IRB) and obtaining informed consent from research subjects.

- *Corporate ethical review processes.* While informed consent may be feasible in a controlled research setting with a well-defined group of individuals, such

[20] GDPR, Art. 6(4)(e).
[21] GDPR, Art. 25(1).
[22] GDPR, Art. 32(1)(a).
[23] GDPR, Art. 89(1).
[24] Commission on Evidence-Based Policymaking, *The Promise of Evidence-Based Policymaking* (2017), *available at* https://www.govexec.com/media/gbc/docs/pdfs_edit/090617cc1.pdf.
[25] Cal. Civ. Code § 1798.145(6)(c)(1)(A-C).
[26] Cal. Civ. Code § 1798.105(d)(6).
[27] 45 CFR 46 (amended 2018). Currently, 20 US agencies and departments intend to follow the revised Common Rule and their CFR numbers. *See* US Department of Health & Human Services, *Federal Policy for the Protection of Human Subject ('Common Rule')* https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html (last visited Mar. 8, 2019).

> as a clinical trial, it is usually untenable for researchers analyzing large datasets of millions, or billions, of data subjects.[28] Ethical review processes (also sometimes referred to as consumer subject review boards, or corporate ethics boards) may serve an important goal of helping researchers identify and balance the risks and benefits of this kind of research, including to individuals, the company, and the public interest.[29]

Legal mandates that require companies to obtain continual permission from individuals for future uses are appropriate in many commercial contexts (for example, obtaining opt-in permission from consumers who have exercised the right to opt out of sales under CCPA). However, such mandates may also create burdens for researchers using purchased or licensed data, who do not know what insights a future study might reveal, and who may rely on datasets containing individuals that they cannot contact or who have been de-identified.

As FPF noted in a report from a 2015 inter-disciplinary workshop, *Beyond IRBs: Designing Ethical Review Processes for Big Data Research*,[30] companies that engage in private research on large datasets have the opportunity to reap tremendous social benefits by analyzing data from cities, governments, health care institutions, schools, social networks, and search engines--but they must do so in a way that protects privacy, fairness, equality, and the integrity of the scientific process. In the words of one commentator, this may be "the biggest civil rights issue of our time."[31] For these reasons, we encourage the AG to recognize the challenges of consent and deletion requirements for researchers, while engaging in rule-making and guidance that will incentivize companies to voluntarily comply with strong privacy and ethical frameworks.

4. Establishing guidelines for Data Subject Access Requests (DSARs)

The right to access one's personal information is a fundamental tenet of the FIPPs, as well as a central feature of privacy laws in the United States and globally. In many contexts, the right of access is an "enabling" right, meaning that it opens the door to other data protection rights, such as data portability, the rights to correct, supplement, or rectify data, and the right of deletion.

In spite of this, there are inherent risks for some businesses in complying with DSARs, and often a direct tension between access rights and other important privacy practices, such as collection minimization, and privacy by design (or data protection by design).[32] This is a particularly prevalent issue for companies that do not have a direct relationship with consumers (often referred to as "third parties"), particularly

---

[28] In the words of danah boyd and Kate Crawford: "It may be unreasonable to ask researchers to obtain consent from every person who posts a tweet, but it is problematic for researchers to justify their actions as ethical simply because the data are accessible." danah boyd & Kate Crawford, Critical Questions for Big Data, 15(5) INFO. COMM. & SOC. 662 (2012).

[29] *See* Future of Privacy Forum, Beyond the Common Rule: Ethical Structures for Data Research In Non-Academic Setting (2015), https://fpf.org/wp-content/uploads/Polonetsky-Tene-final.pdf; Dennis D. Hirsch, et al., Roundtable: Beyond IRBs: Designing Ethical Review Processes for Big Data, 72 Wash. & Lee L. Rev. Online 406–98 (2016); Ryan Calo, Consumer Subject Review Boards: A Thought Experiment, 66 Stan. L. Rev. Online 97 (2013).

[30] In 2015, FPF convened an interdisciplinary workshop, *Beyond IRBS: Designing Ethical Review Processes for Big Data*. The workshop brought together researchers, including lawyers, computer scientists, ethicists, and philosophers, as well as policymakers from government, industry, and civil society to discuss a blueprint for infusing ethical considerations into organizational processes in a data rich environment. *See* Roundtable: Beyond IRBs: Designing Ethical Review Processes for Big Data, 72 Wash. & Lee L. Rev. Online 406–98 (2016), https://scholarlycommons.law.wlu.edu/wlulr-online/vol72/iss3/; Future of Privacy Forum & Washington and Lee School of Law, *Beyond IRBs: Designing Ethical Review Processes for Big Data*, https://bigdata.fpf.org/ (last visited Mar. 8, 2019).

[31] Alistair Croll, *Big data is our generation's civil rights issue, and we don't know it*, O'Reilly Radar, Aug. 2, 2012, http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it.html (last visited Mar. 8, 2019).

[32] *See, e.g.,* M. Veale et al., *When data protection by design and data subject rights clash*, Intl. Data Privacy L., Vol. 8, No. 2 (2018), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081069.

when they collect or receive personal information that falls somewhere on a spectrum of less readily identifiable data. This includes, for example: IP addresses; cookie identifiers; mobile advertising identifiers (Ad IDs); or other persistent identifiers that are commonly used for online and mobile advertising.[33]

For third parties that process less readily identifiable personal information (such as cookie IDs), it can often be challenging if not impossible to validate that the person making an access request is in fact requesting his or her own data. As a result, companies must carefully tailor the scope of their access tools in light of: the sensitivity of the data; their relative ability to identify the data without taking extra steps to re-identify it;[34] and their ability to adequately verify that the data belongs to the requester while avoiding onerous requests that she or he provide validating documents. For example, a company that processes geo-location data tied to an advertising identifier may find that it is too sensitive to disclose in an access request, due to the revealing nature of the information and the potential for abuse, including identity theft or domestic violence. Yet reasonable compliance might include confirmation that the data exists, a description of its geographic scope and time period, and/or the option to have the data deleted.

Ultimately, access requests should be:

- **Secure**. Access request mechanisms, such as "download my data" tools, should be required to be provided in ways that ensure the data is transmitted safely and securely, using reasonable technical, legal, and administrative safeguards that are proportional to the sensitivity of the underlying data.
- **Practical for Businesses.** Access requests should not require businesses to take steps to re-identify individual data that has been de-identified, nor incentivize them to make overly burdensome requests to consumers for additional information for purposes of validation.
- **Meaningful for Consumers.** In some cases, individuals may be primarily interested in learning about the existence of data held by a company, or may be concerned primarily with categories of information, such as how they have been characterized or placed into a particular marketing segment. In other cases, they may be satisfied instead with having the data deleted. As the AG considers options for regulatory flexibility that might prove practical for businesses, they should still ensure that access requests meet the underlying needs of individuals.

Finally, we note that this is not an issue unique to CCPA, and we recommend that the AG look to existing guidance from U.S. and international sources, including: U.S. federal agencies;[35] the Office of the Privacy Commissioner of Canada;[36] the UK

---

[33] As we discussed in a 2015 report on cross-device tracking, some companies may also engage in probabilistic identification of devices, particularly for purposes of associating devices for advertising attribution (measurement and reporting), or as an alternative to cookies where browsers block or limit the placement of third-party cookies. *See* Jules Polonetsky & Stacey Gray, Future of Privacy Forum, *Cross-Device: Understanding the State of State Management* (2015) (at 9), *available at* https://fpf.org/wp-content/uploads/2015/11/FPF_FTC_CrossDevice_F_20pg-3.pdf. In reaction to the perceived risks of this kind of statistical identification or "data fingerprinting," Apple's Safari recently eliminated support for the Do Not Track (DNT) standard. *Safari 12.1 Beta 3 Release Notes*, *Developer Documentation*, Apple, https://developer.apple.com/documentation/safari_release_notes/safari_12_1_beta_3_release_notes (last visited Mar. 8, 2019).

[34] In several places, CCPA states that companies are not obligated to take steps to re-identify individuals, which is good policy and aligns with GDPR's Article 11, which states that data controllers "shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of [compliance]." GDPR, Art. 11.

[35] See, e.g., Federal Communications Commission (FCC) Privacy Act Manual (FCCINST 1113.1) (2017). https://www.fcc.gov/sites/default/files/fcc-privacy-act-manual.pdf.

[36] Office of the Privacy Commissioner of Canada, Responding to access to information requests under PIPEDA, What businesses need to know (February 2014), https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/giving-individuals-access-to-their-personal-information/02_05_d_54_ati_02/ (last visited Mar. 8, 2019).

Information Commissioner's Office (ICO);[37] the European Commission;[38] and the Ireland Data Protection Commission.[39] Because the GDPR has not been in effect for very long, there remains a broad diversity in approaches that global companies are currently taking to comply with access requests. As far as possible, we recommend taking into account interoperability with GDPR to facilitate regulatory clarity for businesses as well as consistent expectations for individuals.

5. The intersection of CCPA with California's education privacy laws

FPF has significant expertise working with stakeholders at the intersection of privacy and education. FPF's Education Privacy team has testified before Congress[40] and the Federal Commission on School Safety,[41] was invited to speak at the 2017 FTC and U.S. Department of Education workshop on Student Privacy and EdTech, and publishes extensive resources for parents, students, educators, edtech vendors, practitioners, and policymakers.[42] FPF also co-founded the Student Privacy Pledge, a self-regulatory framework that safeguards student privacy regarding the collection, maintenance, and use of student personal information.[43]

We recommend that for the benefit of schools, administrators, and education technology ("edtech") vendors, the AG should clarify key points of CCPA that are applicable to edtech, and its interaction with existing state and federal education privacy laws. Specifically, we recommend greater clarity for understanding when edtech vendors may be considered "service providers" under the law; and alternately, how edtech vendors may navigate compliance obligations when they are subject to overlapping requirements under CCPA, the Federal Educational Rights and Privacy Act (FERPA),[44] and the Student Online Personal Information Protection Act (SOPIPA).[45]

As a threshold issue, we recommend that the AG clarify that a "service provider" under CCPA may include edtech vendors. Edtech companies support schools — including their teachers, students and parents — to manage student data, carry out school operations, support instruction and learning opportunities, and develop and improve products and services intended for educational use.[46] Edtech vendors range

---

[37] *Guide to the General Data Protection Regulation (GDPR)*, *Right of Access*, Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ (last visited Mar. 8, 2019); *Responding to access to information requests under PIPEDA*, Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/giving-individuals-access-to-their-personal-information/02_05_d_54_ati_02/ (last visited Mar. 2019); Complying with COPPA: Frequently Asked Questions, Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions (last visited Mar. 8, 2019).
[38] *How can I access my personal data held by a company/organisation?*, *Policies, Information and Services*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/how-can-i-access-my-personal-data-held-company-organisation_en (last visited Mar. 8, 2019).
[39] *Limiting Data Subject Rights and the Application of Article 23 of the General Data Protection Regulation*, Data Protection Commission, https://www.dataprotection.ie/en/individuals/know-your-rights/restriction-individual-rights-certain-circumstances-article-23-gdpr (last visited March 8, 2018).
[40] FPF Testifies Before Congress on Promoting and Protecting Student Privacy, FERPA SHERPA (May 18, 2018), https://ferpasherpa.org/fpf1/ (last visited Mar. 8, 2019).
[41] FPF Testifies Before Federal Commission on School Safety, FERPA SHERPA (July 11, 2018), https://ferpasherpa.org/fpf-testifies-before-federal-commission-on-school-safety/ (last visited Mar. 8, 2019).
[42] The Education Privacy Resource Center, FERPA SHERPA, https://ferpasherpa.org/ (last visited Nov. 9, 2018).
[43] 350 leading education technology companies have signed the pledge. *See* The Student Privacy Pledge , Future of Privacy Forum & The Software & Information Industry Association (2019), https://studentprivacypledge.org/ (last visited Mar. 8, 2019).
[44] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.
[45] Student Online Personal Information Protection Act, Cal. Bus. & Prof. Code § 22584 (2014). SOPIPA was the first law in the United States to comprehensively address student privacy.
[46] The US Department of Education refers to edtech vendors as "vendors and other third party providers who are developing, or selling educational technology apps or services that utilizes or collect or uses Students' Personally Identifiable Information." *BY AUDIENCE: Education Technology Vendors,* US Department of Education, https://studentprivacy.ed.gov/audience/education-technology-vendors (last visited Mar 8, 2019).

from some of the largest technology companies in the world to a rapidly growing world of start-ups and small businesses.[47]

Currently, CCPA defines a service provider as a business that:

> *". . . processes information on behalf of a **business** and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any [other] purpose . . ."*[48]

It is good policy, and in line with existing legal norms, to exclude service providers from compliance obligations related to access, deletion, and control, on the basis that they are under contractual limitations and do not retain further rights to retain, use, or disclose data.[49] However, CCPA's definition appears to exclude service providers who process data on behalf of non-businesses, such as non-profits and government entities. Yet it is certainly within the spirit and purpose of CCPA to apply this exclusion equally to service providers who process data on behalf of government entities, who frequently use contracted vendors for services such as direct mailing, customer management, or IT support.

In the context of K-12 education, many edtech vendors process data on behalf of schools or school districts. Under the federal law FERPA, schools and school districts must maintain direct control over data they share with third parties without parental consent. This means that an edtech provider receiving student data under this exception is only allowed to use, disclose, or retain data as allowed by the school or school district. Furthermore, California's leading student privacy law, SOPIPA, and its companion AB1584 also require privacy protections and contractual restrictions that protect student privacy. While in some respects SOPIPA is clearly more privacy protective than CCPA,[50] in other ways the interaction between the laws might not be as clear.

As a result, it could create intractable conflicts for an edtech vendor to be obligated to respond to CCPA access or deletion requests while under a contract or other legal obligation that simultaneously reserves access and deletion rights to the school or district. This does not mean students or parents would be limited in accessing their data; it simply means that they would be required to go through existing FERPA-mandated processes to access their data through the school or district.

Overall, we recommend further engagement on the intersection of CCPA with existing state and federal laws, including SOPIPA, COPPA, and FERPA. In addition to the fact that many edtech companies are small businesses without robust legal compliance programs, further guidance will also help bring regulatory for schools, school districts, and school administrators who negotiate privacy and data use conditions related to educational products and services.

---

[47] In 2017, of the nearly $9.52 billion in edtech investment, "[c]onsumer companies raised $3.85 billion in 2017, and corporations came in slightly below at $3.79 billion." Robyn Shulman, *EdTech Investments Rise to a Historical $9.5 Billion: What Your Startup Needs to Know.* Forbes (Jan. 26, 2018) https://www.forbes.com/sites/robynshulman/2018/01/26/edtech-investments-rise-to-a-historical-9-5-billion-what-your-startup-needs-to-know/#5064e8a93a38 (last visited Mar. 8, 2019). Edtech vendors provide thousands of products to students. *See* The EdSurge Product Index, EdSurge (2019), https://www.edsurge.com/product-reviews (last visited Mar. 8, 2019).

[48] Cal. Civ. Code § 1798.140(v).

[49] GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, Art. 4(1)(2).

[50] For example—assuming that SOPIPA covers a similar range of personal information (which is not clear)—while CCPA requires that consumers must be permitted to opt out of the sale of data, SOPIPA completely prohibits the commercial sale of data for its covered entities (edtech providers).

Additional Resources

Finally, FPF has published a broad range of technical, legal, and policy analysis on other commercial privacy issues that may be of interest to the AG. Below are a few highlights from recent months (for more visit www.fpf.org):

- **The Internet of Things (IoT) and People with Disabilities.** In January 2019, FPF published *The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions*, a report that examines the nuances of privacy considerations for people with disabilities using IoT services and provides recommendations to address privacy considerations, which can include transparency, individual control, respect for context, the need for focused collection and security.[51]

- **Artificial Intelligence (AI) and Machine Learning (ML).** In October 2018, FPF released the *Privacy Expert's Guide to AI and Machine Learning*, a guide for non-programmers to understand the technological basics of AI and ML systems, and to address privacy challenges associated with the implementation of new and existing ML-based products and services.[52]

- **Digital Data Flows "Masterclass" Series.** In October 2018, FPF launched a "Masterclass" series for U.S. and European regulators and staff who are seeking to better understand the data-driven technologies at the forefront of data protection law & policy. The program features experts on machine learning, biometrics, connected cars, facial recognition, online advertising, encryption, and other emerging technologies.[53]

- **Facial Recognition**. In September, 2018, FPF published the infographic *Understanding Facial Detection, Characterization, and Recognition Technologies*,[54] along with *Privacy Principles for Facial Recognition Technology in Consumer Applications*.[55] These resources are intended to help policymakers better understand and evaluate the growing use of consumer-facing technologies used for facial detection, characterization, and recognition.

- **Non-HIPAA Health Data.** In July 2018, FPF published *Privacy Best Practices for Consumer Genetic Testing Services*,which provides a privacy policy framework for the collection, protection, sharing, and use of genetic data by consumer genetic and personal genomic testing companies.[56] FPF also released *Best Practices for Consumer Wearables and Wellness Apps and Devices*, a detailed set of guidelines that provide practical privacy protections for consumer-generated health and wellness data.[57]

---

[51] Future of Privacy Forum, The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions (Jan. 31, 2019), https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf.
[52] Future of Privacy Forum, The Privacy Expert's Guide to Artificial Intelligence and Machine Learning (2018), https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf.
[53] Digital Data Flows Masterclass, Future of Privacy Forum (2018), https://fpf.org/classes-archives/ (last visited Mar. 8, 2019).
[54] Future of Privacy Forum, Understanding Facial Detection, Characterization and Recognition Technologies (2018), https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf.
[55] Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications (2018), https://fpf.org/wp-content/uploads/2018/09/FR-Final-doc1_publish.pdf.
[56] Future of Privacy Forum, Privacy Best Practices for Consumer Genetic Testing Services (2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.
[57] Future of Privacy Forum, Best Practices for Consumer Wearables and Wellness Apps and Devices (2016), https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf.

We hope these comments and attached resources will be useful to the rule-making process in the State of California, and look forward to engaging further on these important issues.

Sincerely,

Stacey Gray
Policy Counsel

Carson Martinez
Policy Fellow

Amelia Vance
Director of Education Privacy

Future of Privacy Forum
1400 Eye St. NW Ste 510,
Washington, DC 20005

Attachment 1: "Comparing Privacy Laws: GDPR vs. CCPA"
Attachment 2: "A Visual Guide to Practical De-Identification"
Resources also available at www.fpf.org