November 7, 2021

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814
regulations@cppa.ca.gov

Re: Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020

Dear Members of the California Privacy Protection Agency:

Me2B Alliance is pleased to submit these comments for your review. We are a human-centered, open standards developing organization, comprised of software engineers, policy analysts, UX experts, business, and philanthropic leaders with a vision of safe and respectful technology for all. We believe that safe and respectful technology is better for both consumers (Me-s) and businesses (B-s). Our mission is to create a safe and just world through human-centered standards development and independent testing of technology. Fueled by our ongoing product testing and market research with Me-s, we strive to correct the power imbalance currently experienced by Me-s; a power imbalance that is institutionalized through technology platforms, industry norms, and in some cases, regulation.

We're avid supporters of many of the principles and enhancements in the CPRA, and fully appreciate the challenges ahead in auditing and enforcing the regulation. It is with our experience in product testing for the past two years and carrying the voice of Me-s that we offer our comments, questions and suggestions below.

A Note on Global Terminology Alignment

Technically, this is an "Additional Topic", but we start with it here as it contains language that we use throughout our feedback.

We urge the CPPA to adopt the language used in the GDPR to describe data supply chains, or if unable to make these changes due to the language already in laws on the books, we urge the CPPA to write up recommendations for the CA Legislature to further clarify CCPA/CPRA where needed. The use of "first/second/third party" language is cumbersome and confusing. Instead, using GDPR terminology of *data controller* and *data processor* yields clearer descriptions of the very enmeshed (and fractal) nature of the data supply chain. In particular, under the language currently used in CCPA and CPRA, the GDPR's concept of a "joint controller" (aka co-data controller) is difficult to describe, which raises concerns since there are "joint controllers" in nearly every data supply chain in the world.

To illustrate this point let's imagine a scenario where a consumer gives consent to one entity and that entity collects and uses the data as a controller, then the controller shares the collected data with a

new processor. If the collected data is "persistent" and can be used as a "joinkey"[1] to find the person later amongst other big data sets then essentially that processor can reshare the data and upgrade themselves to controller status. The original controller sharing data with the processor is now a co-controller and is exposed to any additional liability from the sharing that occurs due to how it shared a joinkey.

The most effective joinkeys currently in use are IPv4 IP addresses, followed by IPv6 IP addresses. Network data is unique to households and devices (IPv6 is considered Personally Identifiable Information or PII under GDPR due to it being a unique address per device, whereas IPv4 can be a 'household' so it is not de facto PII for an individual). Other crucial joinkeys common today are created by device manufacturers, such as Apple's IDFA userID and on Android's AndroidID, which are shared across apps and developers. In short, joinkeys enable unrelated (and related) organizations to collaborate, build-up, and share data about an individual.

Trying to articulate the above joint controller scenario using first/second/third party language would be extremely difficult, thus our recommendation is to adopt the language of data controller, data processor, and joint controllers. This will have a related benefit of better harmonizing with the European Union, reducing legal and development costs for technology makers.

We also suggest that the CPPA adopt *joinkey* as a term to more explicitly describe the risky technology behavior related to data correlation and profile building.

QUESTIONS FROM CALL FOR PRELIMINARY COMMENTS (original question in blue, italicized, underlined font)

1. ***Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses***

a. ***When a business's processing of personal information presents a "significant risk to consumers' privacy or security.***

NOTE: We would like to briefly mention that the clarity and terminology in these regulations matter, and care should be taken to not adopt habits of clumsy language usage rife in the technology world. "Privacy" and "Security" are unclear and should never be used without a qualifier—*whose privacy? Safety and security of what or whom?* "Privacy" in popular use typically relates to human privacy. We understand "consumer security" in question 1 as human safety, meaning freedom from harm, and freedom from abuses of human rights including the right to privacy. "Security" in popular use typically relates to IT/system safety, aka cybersecurity. We interpret this question to cover the twin domains of human safety (including privacy), and cybersecurity (system security, safety and integrity). But our primary focus throughout this feedback orients on the *safety of the consumer*.

Any collected data has the potential to create significant risk to consumers if it's shared with unexpected or risky data processors (aka third parties). The risk to consumers depends on who gets the consumer's data and how the data is used.

[1] A *joinkey* is a unique identification or key used to correlate multiple disparate pieces of data or files. The terminology comes from database query languages which have *join* and *joinkey* functions to correlate multiple information fields and/or files together. For our purposes in the context of this feedback, the *joinkey* is the method by which executable code uniquely identifies a person and correlates multiple disparate pieces of information to that person, often across multiple data controllers and processors. In other words, joinkeys are dangerous, persistent pieces of metadata used to build and share information about data subjects.

Risks From Adtech
Today, digital advertising is a vast network of ungoverned data sharing. Adtech infrastructure in particular consists of an unbounded network of data processors and co-data-controllers, sharing their collected consumer data with other data processors. This has led to the creation of very detailed personal profiles about consumers that can pose a real risk and cause systemic harms and programmatic violations of personal privacy.

Question for CPPA: How will the CPPA address, audit and protect people from the illegal data collection and privacy risks associated with realtime bidding and the adtech infrastructure?[2]

Risks from Data Brokers
Related to adtech infrastructure harms, the Me2BA believes that data brokers present a significant risk to consumers' privacy. There is an inherent asymmetry of power between data brokers and consumers. Most consumers are unaware of the practices used by data brokers; put simply the behavior exhibited by data brokers lacks transparency and accountability.[3]

This criteria is problematic on multiple levels:
1. Firstly, "direct relationship" is not defined. We recommend that a direct relationship corresponds to the existence of a "Me2B Marriage"--i.e. that the consumer has an account on the service.
2. However, the direct relationship criteria alone is inadequate, as many businesses will be excluded from the definition of data brokers, even though they run a similar data-centric business model. Data collectors who *do have* direct relationships with data subjects can take advantage of this as a loophole to get out of being classified as a data broker. For example, Facebook would not be deemed a data broker under this definition because all of their users have a direct relationship with the platform.[4]
3. Me2B strongly recommends all entities in the data supply chain who participate in the selling of data, or the unsafe practice of sharing ***joinkeys*** be classified as a "data broker."

Question for the CPPA: What will the CPPA implement to make our current data broker registrations more effective?
We know that the regulations intended to address issues involving data brokers by requiring data brokers to register annually with the Attorney General's office.[5] While regulations intended to give consumers an additional tool to control the collection and sale of their personal information, "too often, consumers were unable to make a Do Not Sell request or gave up on the process altogether."[6]

Question for the CPPA: Can the CPPA liaise with the Vermont Attorney General to determine why some advertising and audience companies are registering as data brokers in one state, but not the other? Is there any way that Vermont and California could join forces to tackle the problems of unregistered data brokers, and data broker registration loopholes?

---

[2] Refer to the Irish Council for Civil Liberties current litigation in Hamburg, Germany https://www.iccl.ie/rtb-june-2021/
[3] Federal Trade Commission, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information (2014) https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more
[4] Sherman, Justin, Federal Privacy Rules Must Get "Data Broker" Definitions Right (2021) https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right#
[5] CAL CIVIL CODE § 1, Title 1.81.48, Part 4 of Division 3.
[6] Consumer Reports (2020) https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

Me2B encourages the CPPA to evaluate how they can work together with Vermont in their shared vision of data broker registrations. We could envision a streamlined process of sharing information which could help both states quickly determine which companies failed to register (while recognizing inter-state sharing may require Federal participation or oversight). It might also be worth pooling your resources together to team up on certain investigations of data brokers.

In late 2019, the Attorney General's Office estimated that 4,000 data brokers exist worldwide and at least 1,000 will register in California.[7] Yet only 489 data brokers have registered in CA. Many of the registered data brokers did not have opt-out links on their homepage and some even asked consumers to provide sensitive data in order to process their request. In most cases, individuals complained that they did not even receive a notification acknowledging that their request had been processed. This information comes from a study, Consumer Reports did with 500 plus individuals who contacted 214 data brokers registered in CA, ultimately the study found that when consumers tried to exercise their right to opt out of the sale, they found enormous variations in how companies handled the requests. [8]

We have a list of data brokers who have registered in California, now what?
The public is still unaware of any investigations involving the business practices of registered data brokers. Regulations that are not enforced ultimately do not serve their intended purpose. If the law does not have teeth a business will simply ignore the regulations and go about their usual business practices.

We believe that the current penalties for failing to register as a data broker are a mere slap on the wrist for these businesses. As it stands the penalty is not sufficient enough for it to matter to data brokers. Given that their profits far outweigh the fines, many data brokers might feign ignorance until they get caught and be completely ok with paying the fine. Arguably for data brokers the reward outweighs the risk.

We would assume that data brokers would pay closer attention to attaining compliance if the fines for non-compliance were tied to a percentage of their revenue instead of an arbitrary maximum cap. Therefore, we propose that the maximum cap be amended to include a percentage of the data broker's revenue.

"Valuable consideration" should be described in a way to make businesses realize that they have these obligations. Since many businesses fall into that gray area of sharing, we recommend expanding language in the Data Broker Registration to include a Data Sharing Registry.

In sum, the CPPA and the AG's office should prioritize enforcement of data brokers, which in turn would incentivize data brokers to comply with the regulations.

b. What businesses that perform annual cybersecurity audits should be required to do, including what they should cover in their audits and what processes are needed to ensure that audits are "thorough and independent."

When looking at annual audits through a wider lens we run across a troublesome issue. Organizations conducting audits or certifications are merely providing snapshots of the business for a moment in time. Thus, the organization's assessment of the business will become obsolete as soon as the business releases new software, which would ultimately render any kind of audit

[7]Department of Justice, Data Broker Registration - Finding of Emergency (2019)
https://oag.ca.gov/sites/all/files/agweb/pdfs/hdc/dbr-finding-emergency.pdf
[8] Waddell, Kaveh, California's New Privacy Rights Are Tough to Use, Consumer Report Study Finds (2021)
https://www.consumerreports.org/privacy/californias-new-privacy-rights-are-tough-to-use/

results invalid. This could lead to businesses gaming the system. As such, this issue should be analyzed further and addressed.

Perhaps there should be some ability to repeatedly audit businesses. However, that would require vast resources (such as personnel and automated tools) to keep up with all the software updates and provide accurate reporting. See more in our response to question 3, below.

In any case, we urge that CPPA programmatically publish a list of audit results to the public. This list should show not only current "passing" apps and websites, but should also highlight apps/websites that have passed and then subsequently "failed".

Me2BA suggests implementing policies that would encourage businesses to disclose additional information in safety and privacy labels. We recommend using a carrot and a stick approach.

For example, if a business voluntarily discloses accurate (validated) safety and privacy information, then that business will receive additional days to cure a violation. Currently, safety/privacy labels for apps are either inadequate or missing, and safety/privacy labels for websites are non-existent.

We propose better self-disclosure requirements and validated labels in app stores that include the following:

(a) All data processor company names (third parties) whether via SDK or via inclusion of domains/URLs in the apps with whom data is being shared.
(b) All data processor company names (third parties) from whom the data controller (first party) receives data.

Currently, there is no standard safety or privacy label for websites. We suggest the following as a starting point:

(a) Websites must publish update dates in a way that's easy for the public to see.
(b) Websites must publish the authenticated business owner of the site that's easy for people to see.
(c) Websites must identify all data processor company names (third parties) with whom data subject data is being shared.
(d) Websites must identify all data processor company names (third parties) from whom the data controller (first party) receives data.

c. What businesses that submit risk assessments to the Agency should be required to do, including what they should cover in their risk assessments, how often they should submit risk assessments, and how they should weigh the risks and benefits of processing consumers' personal information and sensitive personal information.

Risk assessments relate to cybersecurity. Risk assessments protect the integrity of the IT infrastructure and protect against data theft.

Are risk assessments the right tool for disclosing and auditing of the data supply chain? We would prefer to have validated, timestamped and complete safety and privacy labeling of services.

d. When "the risks to the privacy of the consumer [would] outweigh the benefits" of businesses' processing consumer information, and when processing that presents a significant risk to consumers' privacy or security should be restricted or prohibited.

We discussed these issues in section 1A.

Yet we must emphasize that oversight and transparency are essential in striking the right balance between a consumer's fundamental right to privacy and a data broker's business purpose.

The CPPA should consider adding in clear language to supplement the current regulations subjective interpretation of "reasonably needed to achieve the operational purpose of the business." We suggest amending the term "business purpose" to "reasonably legitimate business purpose," as interpreted by an objective independent third party approved by the CPPA or Attorney General. Adding in an objective component to the subjective interpretation of a business purpose would hopefully deter a business from broadly asserting that any use of consumer data is considered a legitimate and essential business purpose. We bring this up because it is foreseeable that this will be a contentious point with data-centered businesses. As these businesses will likely assert that every collection and use of data is "reasonably needed to achieve the operational purpose of the business."

2.Automated Decisionmaking

a. What activities should be deemed to constitute "automated decisionmaking technology" and/or "profiling."

It's important to clarify here the difference between "profile building" and "automated decisionmaking". It's also important to note that both activities have harms for consumers. The act of "profile building" should be further distinguished from "using profiles in decision-making in software". Profiling building relates to ad tech infrastructure, discussed at length in question 1.

Automated decisionmaking should be defined as any automated function/algorithm that uses as input one or more pieces of personal information (demographic or psychographic information in particular) to influence the outcome of the decision or function—whether it's small or large function. Technology makers' ability to anticipate unintended consequences is poor, reflecting a lack of maturity and discipline in the development process. CPPA should consider proactively mandating use of best practices for autonomous system design and development, such as Privacy by Design, IEEE's "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems"[9], and the Me2BA's own forthcoming specifications for safe and respectful technology[10].

b. When consumers should be able to access information about businesses' use of automated decision-making technology and what processes consumers and businesses should follow to facilitate access.

In short, we recommend instituting better disclosures. A safety and privacy label should disclose:

- Profile building activities performed by the service.
- Profile use and provenance (especially if the profile is not solely created by the data controller).
- How profiles are used in the automated decision-making algorithms, including what information is used, and how it is used; this information should be provided for any automatic determination, whether it is small or large.
- If determinations are further sold or shared with external entities (either data controllers or data processors).

In addition to this proactive disclosure, the individual should be able to easily request and obtain detailed information, including:

- A copy of all the profile information associated with the individual used by the automated decision-making software,

[9] Ethically Aligned Design, First Edition (2019) ead1e.pdf (ieee.org)

[10] Me2BA, Attributes of Safe & Respectful Me2B Commitments (2021) https://me2ba.org/library/recommendation-attributes-of-safe-respectful-me2b-commitments/

- A copy of the details of the automated decision, specifically, information provided should clearly enumerate the rationale for the decision outcome.

c. What information businesses must provide to consumers in response to access requests, including what businesses must do in order to provide "meaningful information about the logic" involved in the automated decision-making process.

See response 2b above.

d. The scope of consumers' opt-out rights with regard to automated decision-making, and what processes consumers and businesses should follow to facilitate opt outs.

We object to the mechanism of "opt-out" as it does not promote the safety and wellbeing of people (and isn't harmonized with global norms). Instead, we support the practice of easy to use, opt-in methods.

Specifically, we advocate for:
- Safe and respectful default settings, proportional to the nature of the automated decisions,
- The elimination of coercive harmful patterns used to manipulate people into vendor-preferred behaviors, and
- [In the absence of respectful defaults] People must be able to reasonably disable "smart" capabilities. For example, Twitter allows the user to change the feed to a chronological-based view, effectively disabling the default "top tweets" feed setting. (Disturbingly, however, the Twitter UX refers to the "top tweets" setting as "Home," which is a dark pattern and disrespectful default).

3.Audits Performed by the Agency

a. ***What the scope of the Agency's audit authority should be.***

Question for the CPPA: Is it feasible for a single entity to manage audits? Is it practical to rely on?
The Agency must be equipped to:
- Conduct audits on services with suspected or confirmed violation as reported by California residents.
- Perform re-audits of previously audited services to ensure ongoing validity of prior findings.
- Conduct ongoing audits in a cost-effective manner, possibly through the use of an authorized ecosystem of testing facilities.

Due to the scale and dynamic nature of technology, the magnitude of the auditing task can't be overstated. Currently, there are over 4 million mobile apps in the Apple store and 2 million in the Google Play store. We question the practicality of a single auditing entity being sufficient. Just auditing the entire list of registered California data brokers (489 data brokers) would be a difficult task for one entity.

Recognizing that resources are finite, we suggest that the CPPA foster an eco-system of approved auditors. We believe that there is a large community that would be willing and able to help.

We further propose an industry-oriented prioritization approach to developing an authorized ecosystem. Namely, the CPPA should prioritize what industry and subindustry they plan to audit in a given year (for instance). Focusing on one industry at a time allows the CPPA to fully develop the skills and scale of audit capabilities, as well as to attract the right industry domain experts who can provide useful information and research.

b. *The processes the Agency should follow when exercising its audit authority, and the criteria it should use to select businesses to audit.*

We suggest a two-prong approach, with dedicated (and connected) resources for each track to ensure progress:
- Ongoing, industry-specific auditing, and
- One-off audits based on suspected or confirmed violation reports from the public.

Ongoing Audits:
As discussed in Section 3A, for ongoing, systemic audits, we recommend an industry prioritization schema. the CPPA should not be selecting specific businesses for audits. Rather, the CPPA should focus on selecting industries. This procedure would naturally bring forth thorough and nonbiased information, ultimately revealing the largest and most aggressive businesses in an industry.

We recommend that the CPPA develop a prioritizing mechanism for selecting businesses to audit. We propose that the CPPA base its auditing decisions on a variety of factors such as the:
(a) Vulnerability of key user groups;
(b) Magnitude of user population affected by technology;
(c) Inherent sensitivity of data used in service (e.g. healthcare).

We also recommend that the Agency cultivate an authorized ecosystem of trusted auditing facilities, which can augment the Agency's reach and capacity. With the right ecosystem, the Agency could perhaps focus on validating specific findings, reducing the bulk of the job.

Violation Reports:
There should be an easy method for the public to report suspected and confirmed CPRA violations. This method should allow for such reporters to be anonymous if they are reporting a violation taking place in an anonymous state of the Me2B lifecycle (see below for more details). There should also be a dedicated team that triages these reports, and is tasked with reproducing and validating the reported violations. Great care will need to be taken in crafting a good violation form, to ensure that adequate information is collected in order to validate the reported violation.

c. *The safeguards the Agency should adopt to protect consumers' personal information from disclosure to an auditor.*

The Me2BA believes in identification minimization, and that any kind of identification must be proportional to the state of the Me2B relationship (see response 4a below). In this particular case, we advocate for the option of anonymous reporting.

4. Consumers' Right to Delete, Right to Correct, and Right to Know

a. *The new rules and procedures, or changes to existing rules and procedures, needed for consumers to make requests to correct inaccurate personal information.*

Identification During CPRA Right to Delete, Correct and Know Requests and Responses
The Me2BA believes that online services should mirror the states of identification that we experience in the real world. These states are loosely mapped to: anonymous, recognized, and known (see Figure 1, below). The "known" state maps to the "Me2B marriage" state--i.e. the state of having an account and being signed in.

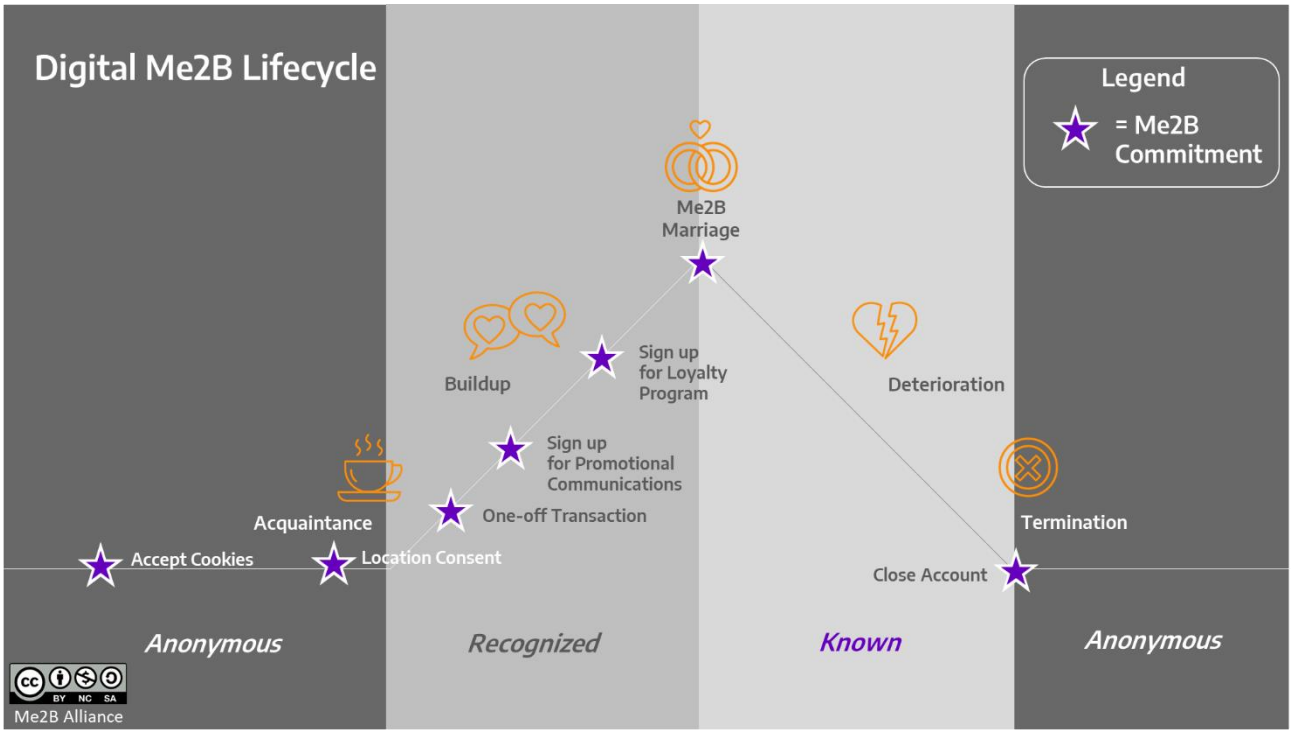
When a user is in the earliest stage of the Me2B relationship, they should be virtually anonymous (but that is not currently the situation). If, for instance, a user exercises a website, without ever providing uniquely identifying information (e.g. never provides an email, name or other

information), they have a reasonable expectation that they are, in fact, *not* being uniquely identified. Thus, it would be nonsensical for such a person to provide personally identifying information in a CPRA rights related request to a business, because that person never identified themselves in the use of the service. However, since, as noted above, we know correlation by personally identifiable joinkeys is happening even in the anonymous state, it would be illuminating to make such a request and see the information being collected while in this anonymous state.

It is a rather quixotic problem: how to make requests in light of the level of identification taking place in the service? It seems people *must* provide PII no matter what to exercise any of the rights (delete, correct, know), not only for vendors to map to existing joinkeys, but also to be able to respond to the individual.

Another question is: should these requests and responses be remembered by the service? If the user has an account, should these requests and responses be recorded and remembered in the user's account history? What if the user doesn't have an account and never provided identification information? We don't recommend that the service start tracking the user just to keep a record of these requests.

Figure 1: Me2B Relationship Lifecycle



b. How often, and under what circumstances, a consumer may request a correction to their personal information.

No feedback at this time.

c. How a business must respond to a request for correction, including the steps a business may take to prevent fraud.

No feedback at this time.

d. When a business should be exempted from the obligation to take action on a request because responding to the request would be "impossible, or involve a disproportionate effort" or because the information that is the object of the request is accurate.

No feedback at this time.

e. A consumer's right to provide a written addendum to their record with the business, if the business rejects a request to correct their personal information.

No feedback at this time.

5. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information

a. What rules and procedures should be established to allow consumers to limit businesses' use of their sensitive personal information.

The Me2BA continues to advocate for respectful default behavior. Specifically, the selling of personal information should not be the default, instead, we should allow people to opt-in to the selling of personal information.

It is problematic that our regulations place the burden on the data subject to opt into privacy. Instead the responsibility should be on the business to receive the data subject's viable permission. In the absence of stated preferences, businesses should default to the most conservative behavior of having the data subject opt in. We suggest aligning with GDPR's protections and requiring consent for data usage to be provided by "clear affirmative action." We recommend that consumers be required to opt-in to the sharing or selling of their data, which will ensure that a consumer understood and freely gave their permission through an affirmative action prior to the collection of the data. In addition, this will incentivize businesses to provide an easily understandable user-interface and will provide an easier path to a global privacy signal standard.

Clearly, default settings advantage the default position. There is an undue industry influence here. As you know, California consumers are automatically defaulted into allowing the sale of information until they opt-out. Since consumers must currently "opt-out" instead of "opt-in," users sometimes have to navigate purposefully-broken websites that restrict clicks, scrolling, engagements and prevent users from being able to express their lack of consent for data sales. Moreover, consumers are often confused by the negative statements and controls.

Users are also less likely to change the default settings. Researchers have found that "several possible reasons for not changing the default settings exist, such as: cognitive and physical laziness; perceiving default as correct, perceiving endorsement from the provider; using the default as a justification for choice, lacking transparency of implication, or lacking skill." [11] Thus, requiring consumers to opt out of selling their data is essentially a default setting that allows collectors to sell consumer data.

[11] Johnson, Defaults, Framing and Privacy: Why Opting In-Opting Out (2002) https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf

GDPR on the other hand, approaches consent from a position where a website can't use UI/UX tricks, locked-in pop-ups, infinite scrolling and other "scroll & click tricks" to collect consent or make it possible to opt-out.

Under the GDPR, consent for data usage must be provided by "clear affirmative action." The EU, UK and Germany have held up support for opting-in.

> The Court of Justice of the European Union found that the consent in which a website user must give to the storage of and access to cookies on his or her equipment is not validly constituted by way of a prechecked checkbox which the user must deselect to refuse his or her consent. [12]
>
> The German Federal Court of Justice decided that the use of cookies for creating user profiles for the purposes of advertising or market research requires the user's consent.[13] Furthermore, finding that the user's consent cannot be obtained by way of a pre-ticked checkbox which the user can uncheck.[14]
>
> The United Kingdom's Information Commissioner's Office has defined clear affirmative action to mean that someone must take deliberate action to opt in, even if this is not expressed as an opt-in box. [15]

The key point is that all consent must be opt-in consent since there is no such thing as opt-out consent. Failure to opt out is not consent. We should not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way.

We strongly recommend changing the default from an opt-out of selling my data to opt-in to selling my data. Doing so will result in a privacy-respecting default, an easier to understand user-interface, and an easier path to a global privacy signal standard. Additionally, global harmonization will reduce the net cost of technology, reducing both software complexity and legal compliance costs for technology makers.

b. *What requirements and technical specifications should define an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information.*

We believe that California should not mandate default technology behavior that violates the GDPR, and that any specifications should be produced with an eye towards global harmonization.

We note that CPRA builds from the initial simple binary signal of "do not sell" into a more nuanced capability for people to limit use on a per business/service basis. The "do not sell" signal is making good progress in standardization via the Global Privacy Control consortia and the W3C, but it doesn't cover the additional signals in CPRA, namely, to limit the use or disclosure of consumer's data on a business by business (or service by service) basis. Developing standardized methods to

---

[12] Courts of Justice of EU, Press Release on Storing cookies requires internet users' active consent (2019) https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf

[13] *id.*

[14] *id.*

[15] Consultation: GDPR consent guidance (2017) https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

convey these kinds of signals is nuanced and complicated, and needs to be considered in a global standards body. Note that IEEE P7012 WG - Machine Readable Personal Privacy Terms is defining a machine-readable Information Sharing Agreement generalized schema, which bears legally binding permissions, conditions, and preferences on a per-data-field basis.

c. ***What technical specifications should be established for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.***

Note that there are age authenticating standards under development specifically for children, such as IEEE 2089.1 .

Question for CPPA: Has the CPPA considered making technical recommendations, such as the use of Verifiable Credentials?

We are concerned with scenarios where data controllers collect data from users under 13 and share this data with processors who then re-share data.

Question for CPPA: Is CPPA considering a way to ensure that data is deleted such as an audit log to confirm that the data of children was deleted?

d. ***How businesses should process consumer rights that are expressed through opt-out preference signals.***

No additional feedback.

e. ***What businesses should do to provide consumers who have previously expressed an opt-out preference via an opt-out preference signal with the opportunity to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information.***

Our primary guidance here is that businesses must not employ manipulative practices in the UX (I.e. dark patterns) in order to get people to opt back into data selling. We have published clear recommendations around how a website or app should behave with respect to online transactions in our "Attributes of Safe and Respectful Me2B Commitments".

Additionally, it's clear that people need software tools to manage their online relationships at scale. A trusted browser can be such an agent to manage permissions and preferences outside of the Me2B Marriage state.

8. Definitions and Categories

a. ***Updates or additions, if any, that should be made to the categories of "personal information" given in the law.***

No feedback.

b. ***Updates or additions, if any, that should be made to the categories of "sensitive personal information" given in the law.***

No feedback.

c. Updates, if any, to the law's definitions of "deidentified" and/or "unique identifier."

No feedback.

d. Changes, if any, that should be made to the definition of "designated methods for submitting requests" to obtain information from a business.

See comments in question 4a.

e. Further defining the business purposes for which businesses, service providers, and contractors may combine consumers' personal information that was obtained from different sources.

No feedback.

f. The changes, if any, that should be made to further define when a consumer "intentionally interacts" with a person.

What is Intentional interaction? In Me2BA terminology, each Me2B Commitment is an intentional interaction. Every time the individual is faced with a choice to transact—even if only setting cookies or preferences— it is a quid pro quo ("Me2B Deal") that reflects the individual's personal "behavioral economics" of the value of the gives and gets, as well as the individual's attitude and level of trust towards the product and company.

Each Me2B Commitment should uphold all of the Attributes of Respectful Commitment. Please see the Me2B formal Recommendation Attributes of Respectful Commitments.[16]

There are different intensities of commitments, which create an important experiential context for users that is currently inadequately understood and reflected in any standard and regulation. All commitments are intentional interactions and should be safe, respectful, and proportional to the intensity of the commitment. All commitments also have inherently different levels of user identification.

There is a special kind of commitment that we call the Me2B Marriage, which is when the individual creates an account on the service. At this point—and *only* at this point in the relationship--the individual is signaling that they wish to be remembered, recognized and personally responded to.

9. Additional Topics

a. Transparency

Inevitably issues with technology companies violating the privacy of consumers will arise.

Question for the CPPA: When a public scandal erupts, how can the CPPA respect the privacy of the business while also providing a feedback loop to the public about investigations that are open or ongoing?

[16] Me2B formal Recommendation Attributes of Respectful Commitments (2021) https://me2ba.org/library/recommendation-attributes-of-safe-respectful-me2b-commitments/

We think there should be some sort of public registrar listing businesses that have been disciplined as well as a public registrar listing businesses that are currently under investigation. This promotes transparency and allows the ability for consumers to submit additional information about any business that is under investigation.

Please consider confirming open investigations and/or initiating a call for complaints against various businesses and/or industries that you identify as fit for investigation. Alerting the public about your broad intention to investigate will promote efficiency and ensure that individuals don't need to keep reaching out and will provide consumers with clarity that their specific issue is already on your radar.

b. Data Deletion

Mass Deletions initiated by the data subject must automatically flow to all downstream data processors (not just the data controller). If we follow data deletion along a data supply chain, we see that typically a data controller shares data with a data processor without the consumer's knowledge or permission. Data deletion should follow the same path. *We would like to see the data controller be required to send a message on behalf of the user, and become their de facto "authorized agent" in an attempt to enforce a mass-deletion of all improperly shared user data.*

There needs to be a standardized and automated method for data controllers to propagate mass-deletion requests to all downstream data processors.

These questions also speak to much-needed changes in software supply chain relationships, duties, and contracts.

Thank you for your time and consideration.

Sincerely,

Me2B Alliance

www.me2ba.org