Commenter: Craig Erickson, a California Consumer residing in Alameda, CA

Contact: craig-erickson@privacyportfolio.com

Date Submitted: 03/27/2023

**Craig Erickson’s COMMENTS ON PROPOSED RULEMAKING**

**CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING**

**Background**

As a California Consumer, I maintain a personal vendor risk program for testing businesses’ compliance with the CCPA and governing use of my personal information. In November of 2020, I voted for Proposition 24, the California Privacy Rights Act of 2020 (“CPRA”) because I share

*“the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public”*.

**Comment 1, Pursuant to Civil Code section 1798.185(a)(15)-(16):**

I ask the Agency to consider all stakeholders when issuing regulations **1798.185(a)(15)-(16),** instead of  **only** requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security, to perform (B) and (A), because consumers and government agencies can also introduce significant risk by their actions or inaction even though they cannot be legally responsible for following the guidance issued by these regulations.

(B) Consumers should be allowed to submit to the California Privacy Protection Agency on an as-needed basis, their own risk assessment findings, compliance test results, or incident reports with respect to their processing of personal information, and that the Agency should help identify and weigh the benefits against potential risks, with the goal of educating the public about which processing activities and organizational entities are deemed “high-risk”.

(A) Based on risk assessments (B) from businesses and consumers which are validated by the Agency, perform a cybersecurity audit on an annual basis, using the State of California’s current process as a model, to ensure that audits are thorough and independent. This proposal is documented in Appendix A.

(a) The *non-exclusive* factors to be considered in determining when processing may result in significant risk to the security of personal information shall include *any one of the following factors*:

a) the size of the business; b) complexity of supply-chain dependencies; c) the nature of processing activities; d) scope in terms of company size; e) sensitivity of personal information; f) vulnerability of targeted populations; g) history of non-compliance, breaches, or unlawful practices; h) absence of, or lack of access to other suppliers providing critical services to consumers.

(16) Consider issuing regulations governing access and opt-out rights with respect to any, and all use of automated decisionmaking technology, because businesses aren’t the only entities using it; government agencies use it in law enforcement; and consumers use it when transmitting opt-out preference signals or using authorized agents to send delete requests to businesses identified in email messages.

**Comment 2, I. Cybersecurity Audits; Question 1 (a) (b) (c) (d) (e):**

1.a. California State Laws and the California State Constitution require California State Agencies to have mandatory cybersecurity audits, and in some cases, Privacy Impact Assessments. These state agencies serve businesses and consumers. California already has an established Cybersecurity Program including Independent Security Audits for its agencies, which appears to meet the goals and requirements of Civil Code section 1798.185(a)(15)(A), with minimal modifications.

1.b. California’s ISA process, documented in Appendix A, helps agencies comply with other state laws that currently have, or could benefit from, cybersecurity audit requirements. These laws, which are related to security and privacy risks of processing personal information, could be more effective by sharing information and costs from CCPA-mandated risk assessments and cybersecurity audits. These current and pending legislative bills are documented in Appendix B.

1.c. and 1.d. The gaps or weaknesses of any audit or certification is the level of acceptance or validation of the assessment. Obviously, Californians would not vote for mandatory risk assessments and cybersecurity audits if existing ones met the goals and requirements of laws like Civil Code section 1798.185(a)(15)(A). The lack of transparency about what standards and controls are tested, the process, the outcomes, and who this information applies to, greatly impacts consumers’ trust in businesses and enforcement agencies. Laws are ineffective when perceived by businesses or consumers, as being unfairly enforced.

1.e. I recommend using a similar model to the existing ISA process within the State because the CPPA is a state agency, and the State uses NIST SP800-53r4 as its primary standard control framework, according to the Office of Information Security (OIS) in the State’s Information Security Policy.

**Comment 3, I. Cybersecurity Audits; Question 2 (a) (b) (c) (d) (e):**

2.a. The Agency should consider in its regulations for CCPA’s cybersecurity audits pursuant to Civ. Code § 1798.185(a)(15)(A) alignment with cybersecurity audits, assessments, evaluations, and best practices identified in intra-state, inter-state, and federal requirements and standards, and standards from the EU including the GDPR, the EDPB, and NIS 2.

2.b., 2.c. and 2.d. Current cybersecurity audits, assessments, evaluations, or best practices in the US include responding to self-assessment questionnaires from other businesses,and third-party certifications such as SOC2, PCI-DSS, HITRUST, FedRAMP, and ISO. Consumers do not have access to this information, which is both a gap and a weakness which impacts consumers and businesses by eroding public trust that laws are being fairly and effectively enforced.

**Comment 4, I. Cybersecurity Audits; Question 2 (e), and Question 3:**

2. e. The Agency should consider these cybersecurity audit models, assessments, evaluations, or best practices when drafting its regulations because, when aligned with common controls in other standard control frameworks, the compliance and audit process can facilitate greater acceptance and leverage information from existing best practices. However, due to the wide variety of interpretations and inconsistent audit execution, existing assessments should not be accepted in place of a state agency-initiated audit that sets the control standards and the audit methodology.

**Comment 5, I. Cybersecurity Audits; Question 4, and Question 5:**

4. and 5. Similar processes from other government agencies help to ensure that these audits, assessments, or evaluations are thorough and independent, by comparing existing cases which are also relevant to the CCPA. The Agency should also consider publishing a “Communicating our Regulatory and Enforcement Activity Policy”, as the ICO does in the UK because:

Transparency is often mentioned as a key factor in building and maintaining trust among businesses and consumers. It’s also a preventative control mechanism – when businesses and consumers know what enforcement actions are taken, why, and on whom can invoke a sense of fairness, which research has shown tends to encourage compliance.

This topic about transparency relates directly to the Agency’s question regarding the scope of cybersecurity audits:

The scope should be dependent upon the classification of business practices and business entities whose management history has been deemed “high-risk” *and should not be concealed from the public.*

For example, the Agency should also consider “trust services” (NIS 2) that are essential to identity verification, or data brokers that operate CDNs or other services that must be resilient for serving the public interest.

Article 2 of The Network and Information Security (NIS 2) Directive, the EU-wide legislation on cybersecurity states: *“2. Regardless of their size, this Directive also applies to entities … where:*

*(a) services are provided by:*

*(i) providers of public electronic communications networks or of publicly available electronic communications services;*

*(ii) trust service providers;*

*(iii) top-level domain name registries and domain name system service providers;*

*(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;*

*(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;*

*(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;*

*(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;”*

**Comment 6, II. Risk Assessments; Question 1 (a), and Question 5:**

The CCPA directs the Agency to issue regulations requiring businesses “whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to regularly submit to the Agency a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits and risks of such processing.

a. The risk assessment itself should determine the necessary scope and submission process for selecting which businesses should be subject to mandated cybersecurity audits. Existing state, federal, and international laws, third-party compliance audits employ a similar approach by using self-assessment questionnaires and other tools to evaluate an entity’s legal requirements and determine if the inherent risk justifies additional scrutiny or controls, even for businesses that make less than $25 million in annual gross revenue or enjoy other exemptions.

**Comment 7, Pursuant to II. Risk Assessments; Question 1 (b) (c) (d) and (e):**

Businesses evaluate other businesses through vendor risk management practices, including the use of “ratings” companies and databases such as MITRE’s CVE and US-CERT, to identify product vulnerabilities and data breach histories which can also assist with the CCPA’s risk-assessments requirements. The gaps or weaknesses of these risk assessments include lack of data quality standards in reporting and the lack of participation in sharing information about security and privacy incidents among businesses, consumers, and enforcement agencies. These weaknesses impact consumers by depriving them of critical information they need to make risk-based decisions about their vendors.

Not-for-profit Organizations, with few exceptions, are currently exempt from complying with the CCPA. According to page 2 of “*Findings from ICO information risk reviews at eight charities”, April 2018,* charitable organizations can be large or small, and engage in very high-risk processing. Under the section entitled, “*Typical processing of personal data by charities*”, the ICO writes, *“The charities involved process a limited amount of sensitive personal data as defined by the DPA, including staff sickness records and sometimes donor or service user information relating to health and receipt of benefits. Some charities also process information relating to children and vulnerable people.”*

This is why I propose the Agency send a risk assessment to every organization registered with the California Secretary of State, not only for the purpose of determining inherent risk but also for increasing the public’s awareness of these new regulations and the standards used in these assessments.

**Comment 8, Pursuant to II. Risk Assessments; Question 2:**

I cannot predict what harms, if any, particular individuals or communities are likely to experience from a business’s processing of personal information.

Identifying what processing of personal information is likely to be harmful to these individuals or communities, could be discovered through robust reporting process, which would accept input from individual consumers and/or consumer advocacy organizations such as the Identity Theft Resource Center. I recommend not codifying in law or regulations assumptions or current trends which may not hold true in the future, in favor of capturing incident-reporting metrics instead.

**Comment 6, Pursuant to II. Risk Assessments; Question 3 (a):**

a. To determine what processing of personal information presents significant risk to consumers’ privacy or security under Civil Code § 1798.185(a)(15), the Agency should (a) follow an approach similar to those outlined in the European Data Protection Board’s Guidelines on Data Protection Impact Assessment.

**Comment 9, Pursuant to II. Risk Assessments; Question 3 (b) and (e):**

b. e. The agency should consider the PIA Methodology from CNIL for Privacy Impact Assessments because of its widespread adoption and online tools for conducting them. The Agency should also consider the ISO/IEC JTC 1/SC 27/WG 5 N1320, WG 5 Standing Document 4 (SD4) – Standards Privacy Assessment (SPA). This document determines whether to apply the SPA process by asking three questions concerning the Standard or Specification Under Review (SUR):

*1. Will the SUR involve technology that will process PII, or will it involve technology that could link information to an identifiable individual?*

*2. If the SUR will not process PII or involve technology that could link information to an identifiable individual, will it generate PII?*

*3. If the SUR will not generate PII, will it involve technology that will be used in a network device by an individual?*

*If the answer to any of these questions is affirmative, then the SPA process should be applied to the SUR.*

The beauty of this approach lies in its granularity, as applied to an entire product offering or introducing a new feature.

In addition, the ISO/IEC JTC 1/SC 27/WG 5 N1320, WG 5 Standing Document 4 (SD4) – Standards Privacy Assessment (SPA) uses this criteria for defining (e) What processing, if any, does not present significant risk to consumers’ privacy or security:

*“This standard [or specification] does not define technology that will process Personally Identifiable Information (PII), nor will it create any link to PII.*

*Furthermore, the standard [or specification] does not define technology that will be deployed in a network device and used by an individual.”*

**Comment 10, Pursuant to II. Risk Assessments; Question 3 (c):**

The risk assessment should be used initially to determine what personal information is processed by an entity, and what their legal obligations are in complying with the CCPA, so that all stakeholders including businesses, consumers, and the Agency can judge for themselves if a cybersecurity audit should be required based on the design of appropriate controls. To protect trade secrets and security measures, only the resulting status should be reported for each entity when or if the entity’s status is queried by users through an online tool provided by the CPPA.

**Comment 11, Pursuant to II. Risk Assessments; Question 4 (a) (b), Question 6 (a) (b):**

The minimum content required in risk assessments should be based on a subset of the most fundamental controls in NIST SP 800-53 r5 which are directly applicable to the CCPA Regulations, and can be mapped to controls in other frameworks such as NIST Cybersecurity Framework, NIST Privacy Framework, and the NIST Framework for Improving Critical Infrastructure, Center for Internet Security Controls, OWASP, and ISO.

As a theoretical construct, I have proposed in Appendix C, a subset of selected NIST controls which provide acceptable standards for cybersecurity and information risk practices that are necessary for complying with the CCPA Regulations.

(a) The GDPR and the Colorado Privacy Act are laws which are subject to change, making these a poor choice for the CCPA’s risk assessments. A better choice would be to base risk assessments on standard, mature control frameworks like NIST, which is a commonly used by state and federal government agencies and all companies that do business with these agencies.

(b) Additional content is not required in risk assessments for processing that involves automated decisionmaking, including profiling because several controls included in my proposed NIST subset covers underlying dependencies like data quality and provenance, which are marked with an asterisk in Appendix C. Additional content may be required for mandated cybersecurity audits according to relevant risk factors.

**Comment 12, Pursuant to II. Risk Assessments; Question 6 (a):**

Businesses should only submit summary risk assessments formatted as a self-assessment questionnaire issued by the Agency, for the purpose of identifying risk factors ascribed to their company.

The Agency should not accept any other risk assessment conducted by the business because most other assessments will likely be outdated and not aligned with CPPA standards which are not yet defined.

These summaries should include a relevant subset of controls based on the NIST standard, similar to my Comment 11, which is documented in Appendix C. They should be submitted at least once annually, or within 90 days of a change in ownership.

**Comment 13, Pursuant to II. Risk Assessments; Question 6 (b):**

Businesses should designate a company officer that attests to the completeness, accuracy, *and currency* of risk assessment summaries, signed by the designated officer under penalty of perjury, like NIS 2 attestations in the EU, or Sarbanes Oxley in the US.

Combined with other proposals I’ve made in these comments, these summaries can be verified or refuted by incident reporting and complaints from consumers and other enforcement agencies.

**Comment 14, Pursuant to II. Risk Assessments; Question 7:**

All organizational entities registered with the California Secretary of State should be required to submit an initial risk assessment, which consists of no more than 100 self-assessment questions designed to identity high-risk processing and high-risk entities. These self-assessment questions are provided alongside the NIST controls I mapped to CCPA Regulations in Appendix C.

**Comment 15, Pursuant to III. Automated Decisionmaking; Question 3 and Question 4:**

Automated Decisionmaking, and any privacy risks associated with its use is not limited to CCPA-covered entities. Businesses which are exempt from the CCPA due to revenue threshholds have been reluctant to acknowledge their status, which effectively defrauds consumers regarding their CCPA rights according to controlled privacy experiments I have conducted over a two year period. I anticipate that business start-ups, who are eager to accelerate their market positions but less eager to implement privacy controls, will claim to use AI, ML, Deep Neural Networks, etc. This is problematic because it could be nearly impossible for the Agency to determine who is using this technology, especially if companies make false representations or fall under the revenue threshold to avoid public embarrassment AND regulatory scrutiny.

**Comment 16, Pursuant to III. Automated Decisionmaking; Question 3 (a) (d) (e) (f) and Question 5:**

The Agency should consider all regulatory frameworks regarding the use of Artificial Intelligence (AI) because AI is the baseline technology underlying Automated Decisionmaking technologies. In particular, the Agency should consider:

* [Regulatory framework proposal on artificial intelligence | Shaping Europe’s digital future (europa.eu)](https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai)
* explaining-decisions-made-with-artificial-intelligence-1-0.pdf from the ICO
* guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf from the ICO

# The Agency should also consider which AI systems the EU has identified as high-risk in its Regulatory framework proposal on artificial intelligence, for inclusion in its criteria for defining high-risk factors:

* critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
* educational or vocational training, that may determine the access to education and professional course of someone’s life (e.g. scoring of exams);
* safety components of products (e.g. AI application in robot-assisted surgery);
* employment, management of workers and access to self-employment (e.g. CV-sorting software for recruitment procedures);
* essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan);
* law enforcement that may interfere with people’s fundamental rights (e.g. evaluation of the reliability of evidence);
* migration, asylum and border control management (e.g. verification of authenticity of travel documents);
* administration of justice and democratic processes (e.g. applying the law to a concrete set of facts).

3. a. The Agency should use the ICO definition because it’s the most concise:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>

For related terms, I also recommend <https://publications.jrc.ec.europa.eu/repository/handle/JRC126426> which provides an “operational**definition”** consisting of an iterative method providing a concise taxonomy and list of keywords that characterise the core domains of the AI research field.

3. d. e. f. I recommend the Agency analyze how its own regulations on ADM would or would not apply to use cases in the EU, in light of the other conflicting US laws which could circumvent these protections. Existing GDPR case law, and associated privacy risks can be found in the following report, <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf>.

For example, one consumer complaint I filed with the California Office of Attorney General applies directly to case law, *3.3 Credit Scoring*, which *is justified on “contractual necessity” only if it relies on relevant information*. I was denied access to my business banking account due to their use of an identity provider which is a credit rating agency exempt from the CCPA, is a registered data broker, and also has a history of data breaches involving my compromised answers to security questions pertaining to another individual which I have no right to correct. In my case there was no automated decisionmaking using machine-learning or artificial intelligence algorithms: just me and my US passport standing in front of the bank branch manager who opened my account but could not authenticate me for online-banking because of a simple “automated process” consisting of a flawed lookup table maintained by an untrustworthy identity provider exempt from the CCPA.

Closing Comment

I want to thank the CPPA for providing this opportunity to participate in its rulemaking process through these public comments. For brevity’s sake, my Appendices are attached (if possible) to this submission, and published in my PrivacyPortfolio for peer review and collaboration with my professional colleagues.

Like laws and audits, my own assumptions and proposals need to be tested. Therefore, as a follow-up to this public comment I will be conducting these tests on my personal vendors and sending my findings to my vendors and the appropriate enforcement agencies and publishing the results of my experiment in my public data catalog.

As a California Consumer who exercises my own rights, I hope that the CPPA succeeds in providing independent assurance to all stakeholders that critical assets and citizen data are protected, which is the stated goal of Mandatory Independent Security Assessments of California Agencies.

Sincerely,

Craig Erickson, a California Consumer