March 27, 2023

Via Electronic Mail (regulations@cppa.ca.gov)

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: PR 02-2023

The Computer & Communications Industry Association ("CCIA")[1] is pleased to respond to the California Privacy Protection Agency (the "Agency" or "CPPA") Invitation for Preliminary Comments on Proposed Rulemaking (the "Rules") that will implement the California Privacy Rights Act of 2020 (the "CPRA").

I. INTRODUCTION

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. The Association supports and appreciates the Agency's efforts to adopt and implement privacy regulations that will guide businesses and protect consumers. These comments focus on the topics and questions for public comments regarding Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking.

To give businesses clear standards and meet consumer expectations, California should seek to harmonize its approach with other state laws. Virginia, Colorado, and Connecticut have all adopted privacy laws that incorporate automated decisionmaking opt-outs limited to "decisions that produce legal or similarly significant effects" and the forthcoming rules should be consistent with this emerging norm. Interoperability of state laws allows consumers to benefit

[1] CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

from consistent protections and avoids a complex patchwork of privacy laws that disproportionately impacts the compliance efforts of small and medium sized businesses.

II. CYBERSECURITY AUDITS

A. Question 2.

The National Institute of Standards and Technology continues to provide a forward-looking approach to cybersecurity as it develops its Cybersecurity Framework (CSF) 2.0, building upon the success of its CSF 1.0.[2]

B. Question 3.

Some existing laws allow businesses to submit an annual self-certification that the required audit has occurred – such as the New York Department of Financial Services.[3] The Agency should adopt a similar regulation, permitting organizations to submit annual self-certifications to the Agency. Moreover, if the processing that creates a significant risk (as eventually defined by the final Rules) is already the subject of another audit (such as the Payment Card Industry Data Security Standard (PCI-DSS) or Sarbanes-Oxley Act of 2002), then the existing audit should suffice for the CPRA regulations.

The Agency should allow businesses the option, as an alternative, not as the sole requirement, to submit proof of certification such as PCI, NIST, or International Organization for Standardization (ISO) that demonstrates their compliance with this requirement.

Businesses may already perform certain industry standard audits and reports. For example, the storage of payment cards on file is regulated in the industry by the PCI-DSS standards, and merchants are required to recertify every year. In those circumstances, businesses should be able to re-use such audits and certifications rather than duplicate their efforts, which

---

[2] Cybersecurity Framework, *Updating the NIST Cybersecurity Framework – Journey To CSF 2.0*, NIST (March 1, 2023), https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.
[3] NYDFS Cybersecurity Regulation, 23 N.Y. Comp. Codes R. & Regs. Tit. 23 § 500 (2017).

would unduly add to the cost and burden of compliance. Businesses should be permitted to use certifications and audits related to cybersecurity from service providers to help meet their requirements to conduct cybersecurity audits and provide risk assessments.

C. Question 4.

CCIA recommends that the Agency should allow companies to rely on reasonable industry standards. To ensure that audits are independent, companies should also be permitted to rely on internal bodies that have safeguards to ensure that they are thorough and independent.

D. Question 5.

The Agency should clearly define what type of processing creates a significant risk, preferably by limiting the types of personal information to which the cybersecurity audit requirement applies. Other sector-specific laws that require similar audits are limited to specific types of personal information such as payment data (as in the NYDFS Cybersecurity Regulation). For large businesses, conducting such an audit for lower-risk personal information that does not require such audits under other laws would create a significant expense with little benefit to consumers.

Many businesses already have self-audit mechanisms and other internal standards and protocols based on appropriate industry standards.[4] Further, larger businesses have internal teams that exist solely to conduct audits, often separate from the first-line teams that are actually implementing security controls. Such an audit can be conducted by auditors internal or external to the covered entity and its affiliates. These teams are designed to be thorough and independent. CCIA recommends that businesses should be able to leverage those existing processes to meet CPRA requirements.

[4] *See,* NIST, *Assessment & Auditing Resources*, Cybersecurity Framework, (Oct. 7, 2022) https://www.nist.gov/cyberframework/assessment-auditing-resources

CCIA strongly urges that the final Rules do not require businesses to use third-party auditors as the burden and expense would be overly disproportionate to any downstream consumer benefit, and the result would likely be increased consumer costs. Notably, third-party audits may also present a security risk, as they may expose a business's confidential security practices and (depending on the nature of the audit) potentially also underlying data to one or more third parties.

III. RISK ASSESSMENTS

Risk assessments should seek parity with other states. With states increasingly incorporating requirements around risk assessments, these obligations must be streamlined to avoid businesses having to conduct multiple assessments for substantially similar processing activities. California could look to obligations such as those in Virginia and Connecticut to shape this requirement and avoid unnecessarily duplicative compliance burdens.

A. Question 3.

Question 3(d) asks, what processing does not present a significant risk to consumers' privacy or security.

From a privacy risk perspective, risk assessments should be limited to processing that presents a heightened risk of harm to a consumer. Risk assessments should be consistent with other states like VA and CT.

From a security risk perspective, risk assessments should be limited to the processing of data that, if compromised, is likely to result in real, concrete harm(s) to individuals. Examples may include identity theft or fraud, extortion, or physical injury from the disclosure of intimate or other objectively sensitive personal details such as one's sexual orientation.

However, the processing of personal information in any context for fraud prevention, anti-money laundering processes, screening, or otherwise to comply with legal obligations should be exempted from the scope of this definition/regulation. These activities protect

consumers' privacy and security and enable organizations to keep such activities confidential to prevent bad actors from gaining insight into the organizations' internal systems. The use of data tools and mitigation measures, such as pseudonymizing or encrypting the relevant data, can meaningfully reduce the risk with processing.

B. Question 4.

Question 4(a) explores the benefits and drawbacks of considering the data protection impact assessment (DPIA) content requirements under the General Data Protection Regulation and the Colorado Privacy Act.

A DPIA should be detailed enough for the business and the regulator to appreciate the risk, however, it should not be overly prescriptive or specific. This balanced approach would allow businesses to retain flexibility and scale existing processes, in particular where a wide variety of factors may apply.

The Agency could consider a similar approach to the one outlined in the EU's Article 29 Data Protection Working Group Report on the Guidelines for DPIAs.[5] The report describes that a "DPIA is not mandatory for every processing operation", but rather only when the process is "likely to result in a high risk to the rights and freedoms of natural persons." Furthermore, the "GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. […] However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them."

Ultimately, the DPIA should be viewed as a documentation requirement and not a substantive mandate that the company must mitigate or fix any identified risk. The DPIA should also be limited to the actual processing of data – it should not be used as a proxy to require a risk

[5] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, (Oct. 13, 2017), https://ec.europa.eu/newsroom/article29/items/611236.

assessment of the feature itself as distinct from any processing of data that occurs as part of that feature. Finally, the Agency should permit a single risk assessment to cover multiple related types of data processing activities.

C. Question 5.

The Rules should recognize that risk assessments are an increasingly common requirement under U.S. and international privacy and data protection laws. To promote interoperability and minimize burdens to covered businesses, CCIA recommends that the regulations specify that the Agency will accept risk assessments that were originally conducted under a comparable legal requirement.

Privacy obligations and risk balancing should be consistent across jurisdictions relating to the same requirements. The Association suggests the Rules align with any data impact or risk assessments required under other similar laws, such as the Colorado Privacy Act and Virginia Consumer Data Protection Act. However, CCIA cautions against adopting in full any future regulatory guidance under other laws, including the GDPR. EU case law is evolving in unpredictable ways, and California should develop guardrails that would ensure that any future obligations on California businesses are appropriately balanced against any potential burden. A consistent standard across jurisdictions would allow businesses to continue to build robust systems to protect consumers' information. These systems will benefit from clear guidelines that allow businesses to innovate and develop their data protection assessments and properly assess their cybersecurity risks.

D. Question 6.

Regarding Question 6(a), as a threshold matter, the Agency should clarify that its function under the statute to provide "a public report summarizing the risk assessments filed with the agency" refers to the risk assessments identified in 1798.185(15)(b). The statute appears to mistakenly refer to 1798.185(15)(a), which concerns cybersecurity audits.

Concerning (a)(i), risk assessments should highlight the most significant privacy risks associated with the processing activity in question and the steps being taken to address and mitigate that risk. Companies should not be required to divulge commercially sensitive information or sensitive security information, including details on technical safeguards that would allow a bad actor to compromise the company's security practices.

For (a)(ii), the Agency should not overly prescribe the format in which the business must submit the risk assessment. Businesses may prepare and record assessments in different ways and in response to different jurisdictions, so they should retain the flexibility to submit the assessment without needing to alter the format or content to match California-specific requirements. An example of an overly-prescriptive format would be if the Agency mandated that a business submit the required information via a webform with answer bubbles that needed to be manually populated.

With respect to (a)(iii), the regulations should not require organizations to repeatedly conduct or submit risk assessments for processing activities that have not materially changed and that pose no new or heightened risks. Such a requirement would be operationally burdensome, particularly for small and medium-sized businesses, and could incentivize businesses to treat risk assessments as a mere 'check-the-box' compliance exercise. Therefore, the Agency's regulations should specify that businesses are only required to "regularly submit" assessments for new or materially changed processing practices that present a significant risk. If the Agency requires periodic updates absent any change, then such updates should not occur more frequently than once every three years.

E. Question 8.

Regarding the guidance for conducting risk assessments and weighing the benefits of processing against potential risks, the Agency should describe that the factors relevant to this balancing may include:

- Technical and organizational measures and safeguards implemented by the business to mitigate privacy and security risks;
- The reasonable expectations of consumers;
- The context of the processing concerning the relationship between the business and consumers.

The regulations should also include protections to ensure that businesses have the necessary confidence to use risk assessments to fully document and assess processing practices, and are not incentivized to treat their assessments as a defensive measure against potential future litigation. Therefore, in addition to the important carve out for trade secrets, the regulations should clarify that risk assessments conducted under the CPRA are confidential and exempt from public inspection and copying under the California Public Records Act and that submitting an assessment to the agency does not constitute a waiver of any attorney-client privilege or work-product protection. The Agency should also not be permitted to use the submitted assessment as evidence of wrongdoing or used to penalize the business for weighing the risks in a way with which the Agency disagrees.

IV. AUTOMATED DECISIONMAKING

Any regulation of automated decisionmaking technology must be grounded in an understanding of how personalization provides people with informative and relevant content, helping them achieve their goals. Personalization – through advertising, ranked search results, or tailored content recommendations – allows people to navigate through the vast amount of information online and connect with the content most relevant to them. When people find new music on their favorite streaming service or discover an interesting article in a news application, they are likely seeing personalized recommendations. Personalization benefits the entire internet ecosystem, from helping charities and non-profit organizations better reach the audience most interested in their offerings, to enabling individuals to connect and share interests to create online

communities and social movements. Personalization is essential to the core value of the internet, and without it, online services would be far less efficient, and possibly even unusable.

A. Question 1.

The Agency should keep in mind that automation is a subset of decisionmaking – and so existing laws (such as anti-discrimination frameworks) that govern how a company makes decisions generally would also apply to such automated systems.

Regarding laws targeted solely to automated decisionmaking, companies in the United States are subject to several existing, or enacted but not yet effective, privacy laws that already impose substantial obligations with respect to the consumer right to opt out of automated decisionmaking. This includes the CO, CT, and VA state privacy laws. Critically, each of these laws is limited to high-risk decisions, described as those which have "legal or similarly significant effects," and in the case of CT, target "solely" automated decisions.

To ensure interoperability with those laws and to strike the right balance between protecting consumers while enabling access to important technology, the Agency should likewise confirm through rulemaking that the profiling opt-out: (i) applies only to decisions with *legal or similarly significant effects* (ii) is limited to solely or fully automated decisions, and (iii) applies only after an automated decision is made.

Significant and High-Risk Decisions. The Agency should not regulate the use of low-risk automated decisionmaking technology, such as spell check, GPS systems, databases, spreadsheets, or transcription services. Requiring businesses to provide opt-outs for such low-risk technology could slow down their activities substantially, while not providing a meaningful benefit to consumers, who should expect that business activities are performed using well-accepted, widely used technology. Regulators should focus on high-risk use cases, such as using technology to make final decisions regarding access to housing, medical benefits, or other critical services without appropriate human involvement. For example, under the Virginia

Consumer Data Protection Act, the consumer's right to opt out of profiling is restricted to "[d]ecisions that produce legal or similarly significant effects concerning a consumer." This is defined as "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water."

Fully-Automated Decisions. This limitation avoids creating an unreasonable obligation on businesses, without impacting the right of a consumer to have their decisions assessed by a human.

Final Decisions. Businesses in every industry sector use automated systems to improve their competitiveness and enhance their products and services, including routine and low-risk applications such as filtering and spell-check. The use of such systems and algorithms has enabled small businesses to effectively market their products to the right consumers at affordable prices and allows for better customer experience and cheaper prices.[6] Furthermore, such automated systems have helped small businesses improve their efficiency and productivity, increase accuracy and reduced errors, and better collaboration and communication.[7] CCIA is concerned that a blanket approach to automated decisions would impose excessive costs and delays upon businesses in return for minimal consumer benefit, with an increased cost being more likely.

Mandating that companies must provide the option of human involvement even before any decision is made creates a huge burden on companies, which might not be able to support a

[6] Alessandra Alari, *As consumer decision-making gets more complex, automation helps to simplify*, Think with Google (Aug. 2021), https://www.thinkwithgoogle.com/intl/en-gb/marketing-strategies/search/consumer-decision-making-automation/.
[7] Shopify Staff, *How Workflow Automation Can Streamline Your Business*, Shopify (Feb. 24, 2023), https://www.shopify.com/blog/workflow-automation.

similar number of requests without incurring unreasonable expenses. For example, individuals receive faster access to services if businesses can quickly identify low-fraud risks. This is only possible at scale through the use of either simple algorithms – such as to approve the transaction with no prior fraud flags – or more complex algorithms including ones using machine learning. Then, for the smaller set of fraud risk cases, businesses can use a manual review to make final decisions, for example, akin to an appeals process. In these situations, if non-final decisions – like those cases flagged only by algorithms for further human review – are regulated, then consumers will receive slower access to services, and will incur higher costs from increased, and unnecessary, manual review.

While such a pre-decisional requirement will result in higher costs and slower service times, it would not provide consumers with any benefits beyond those that a post-decisional opt-out would provide. For instance, if individuals apply for a loan and have a positive outcome on the first automated decision, which might take just a few seconds to be issued, they likely will not want or need to opt-out and request review (but they would retain the right to). Even if they have a negative outcome (again, which they might know in just a few seconds), they will still be able to exercise the right to contest that decision and have a human making a new decision. If laws force companies to have the opt-out even before a decision is made, the experience could take several days, without any actual gain/benefit for customers, because the decision will be issued by the same person that already had access in the first scenario.

B. Question 2.

Generally, companies do not have requirements, frameworks, or best practices that address access/opt-outs related to low-risk, everyday technology, even those that arguably make automated decisions. Access or opt-out rights for these types of automated decisions would slow down business substantially with no benefit to consumers. For example, businesses do not typically give consumers the right to opt-out of using optical character recognition on PDF

documents containing that consumer's personal information. Additionally, businesses do not give consumers the right to opt-out of having their information stored in an internal database that automatically sorts information alphabetically, and instead demand handwritten records be stored and sorted manually. Regulations should not dictate how businesses use or do not use everyday, low-risk technology.

However, to the extent that artificial intelligence (AI)/ machine learning (ML) is used in high-risk automated decisionmaking, that is an area where there are robust requirements, frameworks, and best practices that are continually being developed and deployed. In recent years there has been a proliferation of AI/ML international standards, such as those created by the International Organization for Standardization (ISO) and NIST. In January 2023, NIST released an Artificial Intelligence Risk Management Framework, a set of guidance for organizations designing, developing, deploying or using AI systems to help manage risk. Among many other measures, this framework discusses transparency, human oversight, and appealing system outcomes. Moreover, the NIST AI Playbook helps organizations navigate and incorporate the frameworks' considerations, such as trustworthiness in the design, development, deployment, and use of AI systems.

Importantly, technology companies remained focused on the responsible use of AI/ML. Some examples include Meta's five pillars of Responsible AI, AWS' guide on the Responsible Use of Machine Learning, and Google's Responsible AI practices. For example, AWS' guide provides considerations and recommendations for responsibly developing and using ML systems across three major phases of their lifecycles: design and development; deployment; and ongoing use. Lastly, where useful and meaningful to mitigate risk, companies have provided information or guidance on technology that may be related to automated decisions.

C. Question 3.

Regarding Question 3(a), CCIA urges policymakers to focus on automated decisionmaking systems that produce legal or similarly significant effects. Accordingly, automated decisionmaking should be defined as "final decisions that are made solely/fully with AI/ML technology with legal or similarly significant effects on an individual," and AI/ML technology should be defined as: "the use of machine learning and related technologies that use data to train algorithms and predictive models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, natural language processing, and speech recognition."

Regarding Question 3(c), as part of GDPR compliance, companies already allow EU customers to request a review of certain fully automated decisions. Companies can extend that process to U.S. customers as appropriate.

D. Question 4.

Businesses of all sizes and in nearly every industry sector use ADM to improve their competitiveness and enhance their product and service offerings, such as through the use of daily, low-risk applications like spellcheck and tabulations. For instance, algorithms may be used to recommend a book or song or allow a small business to market its products to the right consumers at affordable prices.

Regarding AI/ML, the adoption of AI across industries is widespread and growing. A 2021 McKinsey and Company study found that 56% of business leaders across the globe now report using AI in at least one business function.[8] The report highlights that the most common AI use cases are low-risk, involving service-operations optimization, AI-based enhancement of products, and contact-center automation.

E. Question 5.

[8] Report, *The State of AI in 2022—And A Half Decade in Review*, McKinsey (Dec. 6, 2022), https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review#/.

Automated technology has significant benefits to both businesses and consumers, including enhanced accuracy and consistency, safer and more innovative products, scalability, cost savings, and increased efficiency. Accordingly, regulators should be very mindful about providing consumers with a right to opt-out of automated activities, as it could severely hamper businesses' and other consumers' ability to realize those advantages.

CCIA recommends the Agency provide businesses and organizations guardrails rather than broad opt-out rights. Specifically, if high-risk business offerings are essential or critical, and it is not reasonable for consumers to consider other options, businesses should have the ability to demonstrate the existence of operational guardrails instead of providing for an opt-out. Depending on the specifics of the use case, appropriate guardrails could include things like significant, rigorous testing; system monitoring, corroboration of results, or even a complaint process if reasonable.

Automation can serve as the offered service or product – often automation may be core to certain high-risk service offerings, making opt-outs infeasible. For example, an in-car safety system that automatically senses a crash and immediately connects a driver with assistance should not be required to provide a consumer with some sort of manual process that conducts the same task – that would defeat the purpose of the automated service. In these instances, businesses should have the ability to demonstrate the existence of operational guardrails that protect California consumers' interests instead of providing for an opt-out.

Automation may also be essential to products that involve less significant effects, while still providing high value with minimal risk to consumers. Examples include:

- calendars that provide you with updated travel times based on traffic patterns from your current location;
- voice services that improve understanding and performance based on interaction history (e.g., when you ask to "play Rush," you mean the band, not the pundit);
- robots that learn what your stairs look like so they do not fall.

Firms should not have to design objectively worse, and potentially even dangerous, versions of their products and services merely to give customers a right to opt-out of ADM. To avoid unnecessary interruption to consumer enjoyment of these products and services, CCIA recommends the Agency should follow the approach of other U.S. state privacy laws and limit the profiling opt-out to automation that has legal or similarly significant effects on an individual.

Opt-out option may also create significant risks. The regulations should recognize that some uses of automated decision-making that produce legal or similarly significant effects may be highly beneficial to consumers – and if turned off, creates the risk of potential harm. The statute did not intend for consumers to be able to opt-out of these uses. For example:

- a health-care system that uses an individual's address to select the closest ambulance dispatch location;
- a bank that uses income or account balance to assess available credit; or
- fraud detection and related activities in making financial or insurance decisions.

To protect California consumers' interests without burdening beneficial uses, the regulations should tailor the scope of "legal or similarly significant effects" to the harms regulators seek to protect against. And as noted above, the regulations should permit operational guardrails rather than requiring an opt-out.

F. Question 7.

Businesses should be allowed to use race, ethnicity and other demographic data with the user's consent for the narrow purpose of evaluating and preventing bias. Restricting the use of this data will unnecessarily inhibit progress in this field to achieve fairness and possibly reintroduce the failures of "fairness-through-unawareness."[9]

[9] Fairness through unawareness assumes that if one is unaware of protected attributes, like gender or race, while making decisions or omits it from the model, the decisions will be fair. This approach has been shown to not be effective in many cases. *See* Giandomenico Cornacchia, et al, *Auditing Fairness Under Awareness Through Counterfactual Reasoning*, 60 Info. Processing & Management 2 (2023), https://doi.org/10.1016/j.ipm.2022.103224.

CCIA also urges the Agency to consider a safe harbor for businesses that are trying to prevent bias. It is not possible to prevent bias without measuring the algorithm's impact on different user groups, including minority groups.

G. Question 8.

Yes. Given the vast use cases for automated decisionmaking technology and profiling, the Agency should largely defer to sector-specific regulatory schemes to address any concerns about the use of this technology. For example, the risks, concerns, and benefits pf using an AI translation service differ significantly from developing and using self-driving cars, which also differ significantly from the use of AI medical software. From a policy and regulatory perspective, each of these areas is best addressed through a specific examination of the sector in question. To the extent the Agency does promulgate rules in this space, it should consider the parameters set out in the aforementioned response to Question 3.1

Yet some use cases raise additional concerns about permitting an opt-out right even for high-risk service offerings. For example, an in-car safety system that automatically senses a crash and immediately connects a driver with assistance shouldn't be required to provide a consumer with some sort of manual process that conducts the same task – that would defeat the purpose of the automated service.

Finally, the Agency should recognize the ADM benefits of reducing the need for human review, in particular where such review may lead to human error in processing, risk of improper disclosure, review, or dissemination of consumer personal data, and bias.

To protect California consumers' interests without burdening beneficial uses, the regulations should tailor the scope of "legal or similarly significant effects" to the harms regulators seek to protect against (such as the provision or denial of lending services or housing). Regarding employee and business to business data, the profiling opt-out should exclude automation involving individual data in the employment or and commercial contexts.

Concerning the employment context, there are developing state and local laws that already specifically target the use of these technologies in the workplace, so California should let that regulatory activity run its course. Moreover, those laws are being tailored to the nuances of an employment context and, recognizing the potential unreasonableness of requiring specific opt-outs for every instance of automated decision-making, are mainly focused on transparency and human review. Lastly, any decision in the employment context arguably could have a "legal or similarly significant effect," including innocuous ADM-like task allocation that is intended to enable efficiency and scale.

H. Question 9.

Companies are still at an early stage in the development of automated decisionmaking system transparency tools. Rather than prescriptive and granular transparency requirements that do not necessarily provide consumers with meaningful disclosures, the rules should provide businesses with the flexibility to figure out what tools are most effective. Platforms must be given the ability to innovate with their transparency tools and provide information that is meaningful to people. CCIA is concerned that such prescriptive requirements will unnecessarily constrain this innovation.

Businesses should be able to fulfill consumer access requests by providing a general explanation of technology functionality, rather than information on specific decisions made. Businesses should be able to provide this information via a publicly available disclosure on their webpage.

In order to provide "meaningful" information about the logic involved in a decision, businesses should be permitted to describe the general criteria or categories of inputs used in reaching a decision. For example, if a rental company considers certain personal information when evaluating a housing application, those categories of information could be described. A more detailed description of any complex algorithms involved in automated decisionmaking will

not provide the average consumer with "meaningful" information on the logic involved in the processing. In addition, providing a detailed explanation of the algorithms involved runs the risk of imposing obligations that conflict with the intellectual property, trade secret, and other legal rights of the business in question. With respect to fraud or security decision-making, disclosures could instruct fraudsters or bad actors on circumventing the system.

Any regulation should also ensure that businesses are protected from disclosing proprietary information, such as that which is subject to intellectual property or trade secret protection, in response to consumer access requests.

I. Question 10.

The right to opt-out should be limited to automated decisions that pose the greatest risk. Online services routinely make several automated decisions to provide the services that people sign up for – automated recommendations enable personalization, which is the basis for a wide array of free and paid online services.

CCIA is concerned any rule implementing a blanket opt-out right of automated decisionmaking technology and profiling would significantly undermine companies' ability to provide personalized services to all users, regardless of whether they have opted-out. Rather, the focus should be on profiling based on automated decisions rather than the technologies used to derive those decisions. Profiling is simply data collected and processed about an individual. Businesses use the data they collect to provide consumers with richer, more engaging experiences.

The rules should avoid blanket restrictions on profiling and instead focus on how the data is collected, secured, and used. Profiling can enable numerous consumer and societal benefits such as helping:

- consumers find the TV shows and movies that they want to see out of the thousands of options available on a streaming service;
- nonprofit community organizations find volunteers who live nearby;

- small businesses compete against large incumbents without spending tens of thousands of dollars on traditional advertising.

Although, like much of what makes the internet valuable, some automated decisions involve risks such as those relating to individuals' privacy and data security. However, this possibility should not result in uncompromising rules that take control away from the consumer.

The GDPR strikes the right balance between ensuring consumers have access to reasonable controls and enabling beneficial uses of automated systems by limiting regulation to those that pose the greatest risks, specifically solely automated systems that produce "legal or similarly significant effects." In the US, privacy laws in Virginia, Colorado, and Connecticut incorporate a similar limiting principle, where the right to opt-out is limited to "profiling in furtherance of decisions that produce legal or similarly significant effects." These provisions are appropriately focused on decisions of significance to an individual's employment, financial status, health care, and California's opt-out right should mirror this approach.

An effective balancing of interests gives consumers control over how their data is used without creating all-or-nothing choices that are inconsistent with consumers' expectations. The best way to do that is by tailoring the opt-out around the highest-risk decisions. An opt-out that severely limits – or altogether eliminates – the ability to employ all automated decisionmaking will make it far less efficient, and in some cases impossible, for people to find what interests them or unlock the content most relevant to them (especially if they don't know what they are looking for).

A broad opt-out right could also have a significant impact on efforts to protect the safety and integrity of online platforms. It would not only harm the effectiveness of automated decisionmaking in protecting the safety of users (e.g., the removal of spam or other violative content), but also the ability to defend against security threats and other integrity risks posed by

bad actors. Rather, consumers should be offered a meaningful choice that respects their autonomy and allows them to make clear, understandable decisions about how their data is used.

Regulations should distinguish between the role of automated decision technology developers – companies that design and develop the technology – from deployers – companies that deploy the technology out in the world and with consumers. Regulations should clarify that developers do not have any standalone obligations about consumer access requests or opt-outs, but only an obligation to provide "reasonable" assistance to deployers, which could, among other things, be provided in the form of generally available documentation.

Any regulations around automated decisionmaking need necessary exceptions to access and opt-out to avoid abuse – as is already the case in CO, CT, and VA – that include to:

- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action.
- Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by authorities.
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may be illegal.
- Provide a product or service a consumer requested or perform a contract with the consumer.
- Take immediate steps to protect an interest that is essential for the life of the consumer or another natural person, if the processing cannot be manifestly based on another legal basis.
- Process personal data for reasons of public interest in the area of public health, subject to certain conditions.
- Conduct internal research.
- Fix technical errors.
- Perform internal operations that are consistent with the consumer's expectations.

V. CONCLUSION

CCIA and its members thank the Agency for this opportunity to provide input on how to balance the next set of Rules in ways that protect consumers, are feasible to implement, and retain flexibility for personalization and innovation.

Respectfully submitted,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
amaranon@ccianet.org

March 27, 2023