Comments to the California Department of Justice

Proposed Regulations for the California Consumer Privacy Act (CCPA)

December 2019

The Better Identity Coalition appreciates the opportunity to provide comments to the California Department of Justice on the Proposed Regulations for the California Consumer Privacy Act (CCPA).

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 24 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, fintech, payments, and security.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at https://www.betteridentity.org/.

In the summer of 2018, we published "Better Identity in America: A Blueprint for Policymakers" – a document that outlined a comprehensive action plan for government to take to improve the state of digital identity in the U.S. Privacy is a significant focus: the Blueprint detailed new policies and initiatives that can help both government and industry deliver next-generation identity solutions that are not only more secure, but also better for privacy and customer experiences.

As a Coalition, we highlighted the concept of privacy as it relates to identity in our Policy Blueprint, noting:

> *The privacy implications of existing identity tools – specifically the ways in which the inadequacy of some identity systems has placed consumers at risk – have made clear that consumers need better identity solutions that empower them to decide what information they share, when they share it, and in what context.*
>
> *Accordingly, new identity proofing solutions should be crafted with a "privacy by design" approach. That means:*
>
> - *Privacy implications are considered up front at the start of the design cycle – and protections are embedded in the solution architecture*
> - *Identity data is shared only when consumers request it*
> - *Identity data that is shared is only used for the purposes specified*
> - *Consumers can request release of information about themselves at a granular level – allowing them to choose to share or validate only certain attributes about themselves without sharing all their identifying data*

Our Policy Blueprint also highlighted the challenges the country faces when it comes to digital identity, particularly when it comes to the ways attackers have caught up with many legacy identity security tools used for both authentication and identity verification.

With regard to authentication, we noted:

> *There is no such thing as a "strong" password or "secret" SSN in 2018 and America should stop trying to pretend otherwise. The country needs to move to stronger forms of authentication, based on multiple factors that are not vulnerable to these common attacks.*

With regard to identity verification, we highlighted how attackers have caught up with commonly-used knowledge-based tools, noting:

> *Adversaries have caught up with the systems America has used for remote identity proofing and verification. Many of these systems were developed to fill the "identity gap" in the U.S. caused by the lack of any formal national identity system – for example, Knowledge-Based Verification (KBV) systems that attempt to verify identity online by asking an applicant several questions that, in theory, only he or she should be able to answer. Now that adversaries, through multiple breaches, have obtained enough data to defeat many KBV systems; the answers that were once secret are now commonly known. Next-generation solutions are needed that are not only more resilient, but also more convenient for consumers.*
>
> *While these solutions were helpful for several years, they also became targets of attack for adversaries. Their goal has been simple: steal identity data in order to aggregate and analyze it – and then turn it against systems that used knowledge of personal data as a means of protection.*
>
> *A number of Better Identity Coalition members also have seen stepped-up attacks on these knowledge-based systems and learned that merely answering the questions correctly cannot guarantee authenticity; one financial institution commented that if someone correctly answers a knowledge-based quiz too quickly, it is a signal that they might be dealing with an attack from a "bot" rather than a real human being.*

As we detail in the sections below, the shortcomings of many commonly used identity verification and authentication tools create challenges with certain aspects of privacy legislation and regulation.

Better Identity is essential to improving privacy and data security

In a world where commerce is increasingly digital, well-designed identity solutions are becoming increasingly important in achieving good privacy outcomes.

- Identity is far and away the most commonly exploited attack vector in cyberspace; 81% of 2016 breaches leveraged compromised credentials to get into systems. Strong identity solutions help protect consumers' data and guard against identity theft.

- Strong identity solutions are also needed to enable consumers to securely authorize third parties to access their personal data at a granular level (allowing an organization to access some, but not all of their data, and potentially for a limited time period), as well as grant

delegated access rights (when, for example, a consumer needs to authorize a third party access certain data on their behalf).

- New legal mandates to grant consumers the right to know, correct or delete their data depend on the existence of well-designed, robust, digital identity systems.

  In practical terms, delivery of these new rights is largely dependent on the ability of the organization holding that data to easily know whether the person demanding access to that data is actually who he or she claims to be. In order to deliver access, correction and deletion, organizations must be able to:

  1) Validate the identity of a consumer making a request to access or correct their information,

  2) Securely authenticate them into the system – while keeping others out, and

  3) Connect them to their information

When properly designed, Identity becomes the "great enabler" of better privacy. But without robust, secure and resilient digital identity systems, any new legal requirement for organizations to deliver access, correction and deletion is likely to inadvertently create a new attack vector for hackers and other adversaries to exploit in their race to steal personal data.

The risks of inadequate identity verification solutions were detailed this summer in a presentation at the Blackhat conference entitled *GDPArrrrr: Using Privacy Laws to Steal Identities,*[1] which detailed how an adversary could exploit GDPR's new "Right of Access" to gain unauthorized access to a consumer's data. As we detail below, we are concerned that the proposed regulations to implement CCPA may open up similar attack vectors in California.

Note that CCPA is a law where our members, given their diversity, may have a diversity of views. For this reason, our comments on the proposed regulations are limited to those areas that touch on identity.

We offer the following comments on the proposed regulations:

1. **The proposal in §999.313 (c)(7) and §999.324 that companies should rely on passwords to verify the identities of consumers asking to see their personal data is likely to put consumers at risk.**

   Passwords offer very little security. More than nine billion accounts and 555,278,657 distinct real-world passwords have been compromised, according to the HaveIBeenPwned.com

[1] https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf

website.[2] If possession of a password is all that is needed to get a company to release a consumer's data (per the proposed CCPA regulations), Californians should be prepared for criminals and hackers to exploit millions of already-compromised accounts and passwords to access their personal data.

The issue is that the proposed CCPA regulations would make compromised passwords more valuable: whereas today a compromised password allows a criminal to access the account associated with that password, the proposed CCPA regulations would expand what a criminal can do with a compromised password – allowing that criminal to not only access the account, but also demand that a company share all of the information associated with that account.

Given that many companies have customer data that is not readily available through their standard, customer-facing account portals, this will have the impact of increasing the risk to consumers associated with compromised passwords.

Use of Multi-Factor Authentication (MFA) is the best way to mitigate the threats associated with passwords. At the Federal level, the government recognized that release of personal information with nothing but a password created serious risks; Executive Order 13681, issued by President Barack Obama on October 17, 2014, stated *"All agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication, and an effective identity proofing process, as appropriate."*[3]

California should look to establish a similar baseline of consumer protection by embracing this Federal standard.

Specifically, California should require that consumer requests for data be validated against Authentication Assurance Level 2 (AAL2), as defined by NIST in its Digital Identity Guidelines.[4] AAL2 details multiple ways that accounts can be protected with MFA, using a combination of knowledge-based (i.e. passwords), inherence-based (i.e., biometrics) and possession-based (i.e. security keys or certificates on a laptop or mobile phone). The Guidelines also make clear that some MFA tools like SMS should not be used, given that attackers have figured out several ways to compromise MFA codes delivered over SMS.

Establishing NIST AAL2 as the standard for identity verification would align California with a well-accepted national standard that sets a meaningful bar for security and would provide clarity to

[2] For more details, visit www.HaveIBeenPwned.com. This is a free service that aggregates stolen usernames and passwords from major, publicly known breaches and offers a service to notify individuals if their password or data was stolen in a breach. The service also runs a "Pwned Passwords" service that supports the NIST recommendation that user-provided passwords be checked against existing breaches.
[3] See Section 3 of https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions
[4] See NIST Digital Identity Guidelines – Authentication and Lifecycle Management at https://pages.nist.gov/800-63-3/sp800-63b.html

businesses looking for firm guidance on how authenticate consumers requesting access to their data.

2. **Suggestions in §999.324 that companies mitigate the threat of compromised passwords through use of security analytics tools are sound – but other parts of CCPA may allow consumers to opt out of having companies use these tools to protect their accounts.**

   The proposed regulations seem to recognize the vulnerabilities associate with passwords, suggesting that companies should be looking to mitigate the threat of compromised passwords by using security analytics tools to detect *"If a business suspects fraudulent or malicious activity on or from the password-protected account."* (per §999.324 (b)).

   We were pleased to see this. At a time when identity is far and away the most commonly exploited attack vector in cyberspace, security analytics solutions are one of the best tools industry has to help guard against these kinds of attacks and prevent fraud. Many Chief Information Security Officers (CISOs) look to the use of these products as a best practice and are increasingly deploying them alongside traditional "strong authentication" products to protect against breaches.

   But use of security analytics tools requires data – and CCPA itself is vague as to whether consumers (or fraudsters posing as consumers) could request their data not be used for security and fraud prevention.

   As backdrop, Europe's General Data Protection Regulation (GDPR) did a decent job here: while it limits the collection of data in many circumstances, it also highlights that when it comes to protecting security and preventing fraud, there are cases where an entity may have a "legitimate interest" in processing personal data – including in cases where such data can be used to deliver and develop secure authentication or verification capabilities and technologies. This "carve out" has allowed the use of data-based security and consumer protection solutions to flourish.

   In contrast, CCPA has more ambiguous language that may allow consumers to opt out of having their data used to protect against malicious, deceptive, fraudulent, or illegal activity.[5] This ambiguity is already inhibiting the deployment of security analytics tools that can guard against

[5] Specifically, §1798.120 discusses a consumer's right to opt out of the sale of their personal information – but does not create any exception for ""*[d]etecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity."* It is unknown whether these omissions were deliberate or a drafting error – the inclusion of a security and fraud prevention exception in other parts of CCPA leads one to believe it was the latter. Many attorneys and companies, however, have interpreted this clause to mean that there is nothing that would prevent a consumer (or someone posing as one) from demanding that a company refrain from collecting or using personal information in to protect against fraud, or – in the case of security vendors – from selling products that make use of that information to help other companies protect themselves.

the kind of password-based attacks the proposed regulations seem to anticipate, placing consumers at risk.

Given the ambiguities of CCPA, the best thing the California Department of Justice could do here would be to clarify the final regulations to state:

1) Businesses should, wherever feasible, be using security analytics tools to detect suspect fraudulent or malicious activity on or from password-protected accounts, and

2) Businesses should be free to use data in security analytics tools to assure security and prevent fraud, provided that they are not collecting information for "security" and then turning around and using it for other purposes.[6]

This clarification would address a much-needed area of concern in CCPA, and would be consistent with language in the CCPA definitions section (§1798.140(d)(2)) which states that: "*Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity"* is a "business purpose."

3. **The proposed process for companies to verify consumer identity in situations where the consumer does not have a password-protected account is based on an obsolete "knowledge-based" approach that will put consumers and businesses at risk.**

As drafted, §999.325 of the regulations call for companies that require a "high degree of certainty" on identity verification to rely on *"matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer."*

There are two problems with this approach:

a) The National Institute of Standards and Technology (NIST) has specifically cautioned against use of Knowledge-Based Authentication (KBA). Per NIST guidance[7]:

Knowledge-based authentication (KBA), sometimes referred to as "security questions," is no longer recognized as an acceptable authenticator by SP 800-63. This was formerly permitted and referred to as a "pre-registered knowledge token" in SP 800-63-2 and earlier editions. The ease with which an attacker can discover the answers to many KBA questions, and relatively small number of possible choices for

[6] Note that Facebook earlier this year was revealed to have been collecting phone numbers under the auspices of "security" only to also be using the data for marketing purposes. See https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/. We believe this sort of behavior should be banned.
[7] See https://pages.nist.gov/800-63-FAQ/

many of them, cause KBA to have an unacceptably high risk of successful use by an attacker.

California would thus be establishing a regulation calling for an approach to identity verification that conflicts with national standards.

b) This proposed process is not based on any standard, nor is there any way to measure its efficacy.

The threshold of what is *"reliable for the purpose of verifying the consumer"* leaves a great deal open to interpretation – and creates multiple opportunities for impersonation and error.

The challenges businesses and governments have faced in determining what data elements are *"reliable for the purpose of verifying the consumer"* have existed for years, with little resolution. Companies have struggled to find data sets that are 1) unique to a user, 2) secret (and thus meaningful), and 3) easy enough to remember that they are usable as a security tool.

These challenges are so acute that security researchers years ago created a flowchart to parody them, with the use case of trying to establish whether noted MC Rob Base – of legendary hip-hop duo Rob Base and DJ EZ Rock – is in fact who he claims to be.

As noted in Figure 1, an identity verification process can be constructed for Rob Base with four distinct elements, based on the opening verse of the 1988 hit "It Takes Two."[8]

The four pieces of personal information depicted in Figure 1 meet criteria 1 and 3 – they are unique to the user (at least in aggregate) and easy enough for the user to remember. However, they are <u>not</u> secrets – and thus not useful for security purposes.

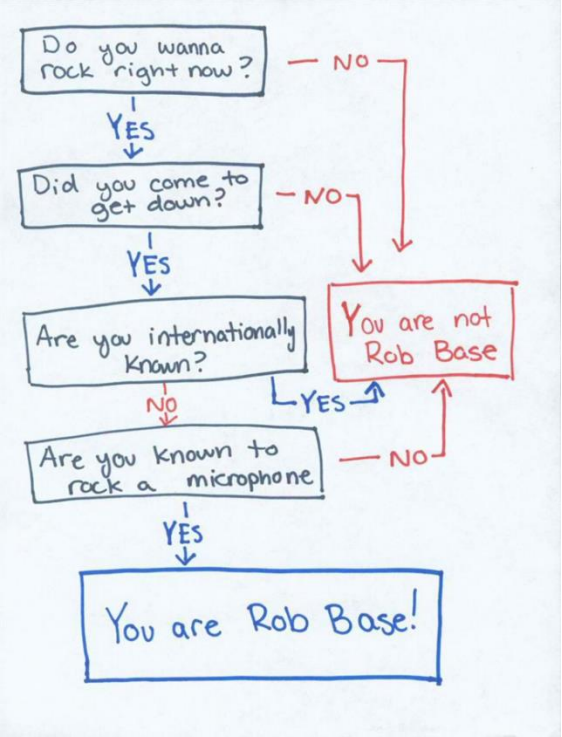

Figure 1: *"Are You Rob Base?"*

Moreover, even if the data points were secrets, the idea is that they are "shared secrets" known by both the consumer and a business. The last ten years have demonstrated that most security solutions based on

[8] See https://www.youtube.com/watch?v=phOW-CZJWT0

"shared secrets" are doomed to fail, as a secret possessed by two parties tends not to stay a secret for long. Attackers have caught up with these solutions. The examples provided in the "illustrative scenarios" in §999.325 are examples of so-called "secrets" that are not reliable for security purposes.

In summary, while it takes two to make a thing go right, California setting a threshold of three data elements to prove identity is going to go wrong. The "Are You Rob Base" approach to identity verification should not be enshrined in California regulations.

We note that § 999.325 of the draft regulations do call for a consumer to provide a "signed declaration under penalty of perjury" alongside their assertion that they are "who they claim to be" – but we do not believe this will help. If a criminal is trying to impersonate someone to steal their data, it is unlikely that they will be worried about a perjury charge at a time when they are already breaking the law.

While we believe this proposed approach to identity verification is problematic, there are two steps that California could take to improve them – better protecting consumers and businesses alike.

1. Rather than call for businesses to "match 3 pieces of data" – a non-standard approach that will open California consumers and businesses to increased identity fraud – California should instead require that consumer requests for data be validated against Identity Assurance Level 2 (IAL2), as defined by NIST in its Digital Identity Guidelines.[9] Establishing NIST IAL2 as the standard for identity verification would align California with a well-accepted national standard that sets a meaningful bar for security, and provide clarity to businesses looking for firm guidance on how to validate the identities of consumers requesting access to their data.

   An added benefit of aligning California regulations with this NIST standard is that doing so will prevent the minimum bar from being tied to a static standard or technology, as the NIST standard is updated every few years to reflect both new technology advances, as well as evolution of threats against identity solutions. Thus, as new methods to achieve IAL2 compliance are devised, the California regulation will automatically support their adoption – rather than being tied to any particular technology or methodology. Threat is always evolving, and a regulation that calls for a specific technology or approach may, in fact, put consumers at risk when adversaries catch up to what was acceptable at the time the rule was written.

[9] See NIST Digital Identity Guidelines - Enrollment and Identity Proofing Requirements at https://pages.nist.gov/800-63-3/sp800-63a.html

2. Participate in the Driver's License Data Verification service (DLDV).[10] DLDV is of the best tools in the market for remote identity verification – created and supported by more than 40 states to help commercial entities validate driver's license and state ID card information to verify identity and combat identity fraud. Government is the only entity that authoritatively confers identity; government is thus in the best position to verify the identities that it issues.

   Note that DLDV is designed up front to protect privacy: states do not share or reveal personal information through DLDV, they only provide a "Yes/No" answer as to whether identity data provided to open a new account matches what the state has on record, and only with a consumer's consent. This consent-based approach enhances privacy and protects against the unauthorized disclosure of Californians' information.

   California is one of a handful of states that do not yet participate in DLDV – this means that California businesses are at a disadvantage when it comes to authenticating identity relative to 40 other states. At a time when California businesses are being asked to take on new identity verification obligations that exceed those imposed on businesses in other states, the least the state could do would be to allow California businesses the ability to validate identities against DLDV.

4. **Other items**

In addition to the points above, there are a number of other aspects of the proposed regulations where specific provisions or wording are problematic. These include:

- § 999.313 (Responding to Requests to Know and Requests to Delete). Subsection (d) of this section states:

  For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.

  As written, this would require businesses to convert an unverifiable request to delete into an unverifiable request to opt-out. If an identity cannot be verified, it may be a sign of fraud. Given this, why should it be treated as an authoritative request that binds a business to take action?

- § 999.324 (Verification for Password-Protected Accounts). This section would require that a business *"require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data."* While we have concerns about the ways in which password-protected accounts may be exploited under this section, if someone has

[10] The DLDV is owned and operated by the American Association of Motor Vehicle Administrators. See: https://www.aamva.org/DLDV/

already authenticated into their account, it is not clear what security value can be gained by requiring someone to authenticate again before a deletion.

We greatly appreciate your offices' willingness to consider our comments and suggestions and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at info@betteridentity.org.