

Follow-Up Questions from Economic Affairs Interim Committee 67th Montana Legislature

March 25, 2022

HJ48 Study on Facial Recognition Technology Follow-up Questions for ID.me

1) ID.me stated that “ID.me does not share data with advertisers absent consent, through an opt-in process, from the individual to whom such data pertains. ID.me never sells data to advertisers.”

- a) **ID.me does not technically sell data to advertisers but are you saying that, with opt-in consent, ID.me does *share* data with advertisers?** → No, ID.me does not share any data with advertisers. ID.me only shares data with a commercial entity after receiving explicit consent from an appropriately authenticated user who reviews each data element requested and authorizes release. This is always managed on a case by case basis e.g. helping a military Veteran prove their service to get a free ticket to a concert from a non-profit organization like Vet Tix without needing to upload their DD 214 (and their SSN) to a commercial organization. This consent would only apply to sharing military service status with Vet Tix specifically. Interactions with commercial organizations are completely separate from any public sector interaction.

ID.me makes plainly evident in section 2 of our Privacy Policy that there is no relationship between government programs and marketing: “if you are using ID.me Services in connection with legal identity verification for a state or federal government agency we will not use any [p]ersonal [i]nformation provided as part of your verification for any type of marketing or promotional purposes.”

In other words, our stance is that each individual has the right to control their own data and to share it as they see fit. By default, users are opted-out of everything. If they wish to opt-in to something, then that is their prerogative.

- i) **If so, what data is shared with/supplied to/otherwise furnished to those third parties?** → As stated above, ID.me does not share our users’ information with advertisers, only with our partners as directed by a given user. Users engaging ID.me in connection with legal identity verification for a state or federal government agency are not provided with the opportunity to verify and enroll in Group Verification, or to opt-in to receiving marketing communications from ID.me, during the verification process.
- ii) **Can this data then be used for targeted advertising to ID.me users?** → N/A.
- b) **What does ID.me consider to be consent?** → An application first registers with ID.me and will define an access policy for a given service. ID.me reviews the policy and ensures the requested data attributes are reasonably associated with the context of the interaction. When a user attempts to access a program, they must be appropriately authenticated based on risk. After appropriate authentication, users go to a consent screen and review each specific data field

the application requests from them. The Allow and Deny buttons are equally sized. A user grants consent to a specific organization and authorizes the specific data fields shown after they click the Allow button. Users are prompted to consent for each new partner with whom they direct ID.me to verify their identity and share their data. More information on this process is found in the answer to question 1.e. Users can [revoke consent](#) for the further sharing of their data at any time in their account settings.

A consent screen for a NIST 800-63 authentication policy for Montana is below:

ID.me + Montana Department of LABOR & INDUSTRY

AUTHORIZE MT DLI

We've verified your identity!

Before we send you back to MT DLI, we need your permission to share your verified identity information.

Please note that only information obtained from the verification process will be shared.

MT DLI will receive:

- First Name
- Last Name
- Full SSN
- Phone
- City
- Postal Code
- Middle Name
- Email
- Birth Date
- Street
- State

Allow

Deny

You can remove this access at any time by changing your ID.me account settings.

[What is ID.me?](#) | [Terms of Service](#) | [Privacy Policy](#)

- c) **What does the opt-in process consist of?** → ID.me makes plainly evident in section 2 of our Privacy Policy that there is no relationship between government programs and marketing: “if you are using ID.me Services in connection with legal identity verification for a state or federal government agency we will not use any [p]ersonal [i]nformation provided as part of your verification for any type of marketing or promotional purposes.” Users engaging ID.me in connection with legal identity verification for a state or federal government agency are not provided with the opportunity to verify and enroll in Group Verification, or to opt-in to receiving marketing communications from ID.me, during the verification process.
- d) **By simply creating an account with ID.me, does ID.me consider that to be consent?** → No, account creation does not equate to consent for ID.me to automatically share user information with our partners. Where a user elects to verify their identity with a partner using ID.me, they are prompted to provide a

just-in-time consent that details the data elements ID.me will share directly with the partner. In order to effectuate consent, users must manually click the “Allow” button at the end of the ID.me process flow to pass their data to the Montana DLI. Question 1.e has more details on the “Allow” consent process.

- e) **Describe the specific workflow associated with getting consent and/or opting-in.** →
- i) **Consent:** After the user successfully verifies their identity with ID.me, they must provide consent in order to share their information and verify their identity with a partner, for example Montana DLI. If the user does not click “Allow”, the partner - in this case Montana DLI - does not receive any information. Included below is the consent screen that Montana DLI claimants see on their final step in the ID.me verification flow.
 - ii) **Opting-in (share data for advertising):** N/A. As stated above, ID.me does not share our user’s information with advertisers, only with our partners as directed by the user. Users engaging ID.me in connection with legal identity verification for a state or federal government agency are not provided with the opportunity to verify and enroll in Group Verification, or to opt-in to receiving marketing communications from ID.me, during the verification process.

Note the text on the screen: “Before we send you back to MT DLI, we need your permission to share your verified identity information. Please note that only information obtained from the verification process will be shared.”

- f) **What percentage of user profiles currently have their data shared for advertising/marketing purposes?** → N/A. As stated above, ID.me does not share our user’s information with advertisers, only with our partners as directed by the user. Users engaging ID.me in connection with legal identity verification for a state or federal government agency are not provided with the opportunity to verify and enroll in Group Verification, or to opt-in to receiving marketing communications from ID.me, during the verification process.
- g) **How many users have proactively opted-out of sharing their data for advertising/marketing purposes?** → N/A. As stated above, ID.me does not share our user’s information with advertisers, only with our partners as directed by the user. Users engaging ID.me in connection with legal identity verification for a state or federal government agency are not provided with the opportunity to verify and enroll in Group Verification, or to opt-in to receiving marketing communications from ID.me, during the verification process.

It’s important to note that for non Public Sector integrations, users do not opt-out of marketing emails from ID.me, they must **opt-in**.

- i) In Montana specifically: N/A.
- ii) In total: N/A.

- 2) **Earlier this month, ID.me stated that they would create a process whereby users could delete their selfie. Specifically, “...all ID.me users will be able to**

delete their selfie or photo at account.ID.me beginning on March 1.” In written response to questions on February 9th, ID.me stated “The subject contract with Montana was performed in accordance with NIST Special Publication 800-63-2, Electronic Authentication Guideline, which required a retention period of seven years and six months.”

- a) **Does this mean that Montana citizens will NOT be able to delete their biometric information?** → No. All ID.me users who submitted a selfie and consented to the collection of biometric information may now direct ID.me to delete such data as of March 1, 2022 through our [Privacy Rights Center](#).
- b) **How can ID.me abide by federal guidelines that require retention for 7 1/2 years while simultaneously permitting users to delete their selfies?** → ID.me had historically complied with the data retention period specified in the National Institute of Standards and Technology (NIST) 800-63-2 guidelines, which recommended a record of the registration, history, and status of each credential shall be maintained for a period of seven years and six months beyond the expiration or revocation (whichever is later) of the credential. NIST 800-63-2 was superseded by NIST 800-63-3, however the updated version (63-3) does not state a recommended data retention period; as a result, ID.me continued to align our retention policy to the most recent NIST 800-63 normative requirement.

On March 14, 2022 ID.me updated our retention period, shortening the term to 3 years as disclosed in our updated [Privacy Policy](#). ID.me is required to retain certain data provided in course of verification in order to adhere to our compliance obligations, including our Kantara Trust Mark for compliance with NIST 800-63-3.

- 3) **Is facial recognition the only form of biometrics that ID.me collects from its users?** → Yes. Facial recognition, using facial geometry derived from the selfie provided by a user, is the only type of biometric information collected and processed by ID.me. ID.me is an identity verification company, not a facial recognition or biometric information company.

The use of biometric information to conduct identity verification is promoted by NIST 800-63-3 as a viable option for remote verification, however it is not the only pathway for remote verification offered by ID.me that aligns with NIST guidelines. A partner may elect to offer an alternate pathway to verification through ID.me where a user is not required to submit a selfie or consent to the collection of biometric information. The alternate pathway offers users the option to join a recorded video chat with a Trusted Referee (TR) agent to present the necessary evidence for physical comparison. ID.me believes that technology combined with humans is the best approach.

- a) If you collect other forms of biometrics, what does that include? → N/A
- b) For what purpose are those biometrics collected? → N/A
- c) What are the corresponding retention policies on those biometrics? → N/A

4) What other companies do you partner with to deliver your services?

- ID.me integrates data from authoritative data sources to confirm whether the data provided matches an identity on record. These data sources include: Experian, TeleSign, Prove, National Plan & Provider Enumeration System (NPPES), National Student Clearinghouse, and TransUnion.
- For document and biometric verification, including assessing the authenticity of a credential or comparison of a credential photo to a selfie, ID.me partners with Paravision, iProov, and AuthenticID.
- For assessing digital risk on mobile devices, ID.me partners with Prove, TeleSign, and FingerprintJS.
- For behavior analysis, ID.me partners with Fraud.net