The New State of Data Privacy:
Q&A With Blake Hall, Founder & CEO of ID.me

We wished to better understand the "new state of data privacy" and specifically the roles, responsibilities, and investments of private companies ("privacy as a product") and the government in the consumer privacy space. Here, we interviewed Blake Hall, CEO and Founder at ID.me. You can follow him on Twitter @Blake_Hall.

Your company, ID.me, focuses on improving citizen access through portable identity proofing, streamlining inefficient processes while giving individuals control of their personal data. How do you think the landscape of the "new state of data privacy" currently looks with regard to the roles, responsibilities, and investments of private companies (like ID.me) in the consumer privacy space?

Consumer awareness and appetite for privacy centric technology continues to grow; regulators and policymakers are likewise paying increased attention to the way technology interfaces with citizens, their government, and the broader business landscape - as seen with the American Data Privacy and Protection Act (ADPPA) and proposed FTC rulemaking endeavors. Whether driven by consumer preference, business need, or regulatory changes, the new state of privacy will see consumers reclaim control over their data and their digital footprint, with companies that prioritize consumer privacy rights and protections gaining market share. This shift is already evidenced in the reallocation of advertiser adoption rate, and commensurate spend, in the online advertising space. In the portable identity proofing space, I believe that consumers, businesses, and government entities will all pivot away from legacy identity verification models that rely on data brokers and history in credit files, and the industry will move toward a more equitable and consumer-centric approach. ID.me has been, and continues to be, a leader in improving identity verification through the adoption of best-of-breed technologies, in combination with human-driven solutions, to provide consumers from all backgrounds with increased options for verifying their identity and controlling their personal data.

What do you think are the biggest motivators or drivers behind the innovative privacy product that is ID.me (e.g., increasing accessibility, maximizing efficiency, etc.)?

Increasing accessibility to digital services, which is inherently linked to efficiency gains, is the biggest motivator for consumers. Organizational customers demand that such gains are accomplished in a secure and privacy-enhancing way. ID.me excels across all of these dimensions. We provide individuals with a digital wallet that enables them to verify their identity and other credentials a single time and then re-use that verified data across websites. The concept of allowing an individual to verify their identity once, with ID.me, and then use their verified status across a growing network took hold and accelerated rapidly during the pandemic.

Where data is available to benchmark ID.me's performance against other vendors in the industry, ID.me has been proven to increase access rates for all users, and particularly for members of historically underserved communities including low income, the unbanked and those with limited credit profiles.

As reported by the Washington Post, ID.me nearly doubled the number of people able to create an IRS account. These access gains made it easier for 'more Americans- including low-income earners and minorities- to access their tax information'.

Beyond these results, we have also begun to study our impact on specific demographics. One underserved population we studied, which is primarily Spanish-language speakers and has ⅓ the median income of the overall US population, saw a 6x increase in access rates when compared to legacy solutions. We were able to achieve this outcome thanks to the strength of our algorithms, our video chat pathway, our Spanish language offerings, and our 24/7 customer support operation.

ID.me is a trusted technology partner to multiple government agencies, and your company enables them to provide secure online services to individuals using digital identity verification. How has ID.me helped (and how will it continue to help) government agencies address both newfound and age-old identity challenges, theft and fraud in the privacy landscape?

We are proud of our relationships with government agencies, and particularly our work to make digital services more accessible, equitable, and secure. As the dust settles on pandemic unemployment, five states have publicly come forward and credited ID.me with helping stop over

$238 billion in fraudulent payments. In at least one case, we enabled a government agency to re-open after fraudulent applications ground operations to a halt.

Our market-leading results in access and fraud prevention stem from more than a decade of innovation. ID.me evolved out of NIST grant funding where we had to demonstrate that we were privacy-enhancing, secure and resilient, interoperable, and cost-effective. We've been solving age-old identity challenges primarily by offering a model that puts users in control of their data - as opposed to the website where they registered or data broker aggregators. Historically, online identity verification has been dependent on data brokers that purchase troves of consumer data and build passive profiles on individuals, often without their awareness and consent. Many data brokers won't allow individuals to opt out of their service unless they're an elected official or can demonstrate substantial risk of physical harm. This old model treats someone's identity like an independently tradeable commodity rather than a personal asset belonging to an individual.

To solve this problem, ID.me built a consumer-centric model where a user presents identity evidence in accordance with government guidelines and gets to control when and with whom their data is shared. Privacy and consent are central to how we operate. And because of the strength of the NIST guidelines, we've found that we can put users in control of their data while also preventing fraud.

When it comes to newfound challenges, we're staying ahead of emerging threats. We've seen a rise in both prevalence and sophistication of social engineering, where a victim is manipulated by a fraudster into surrendering some of their personal information and online account ownership to the control of the fraudster. To counter this threat, we have developed a supervised machine learning fraud risk model that can identify victims of social engineering with a high level of accuracy and negligible false positives. This model is another example of how we deploy best-in-breed algorithms working in harmony with humans-in-the-loop.

What is "privacy-as-a-product" in your opinion? In your experience, is this a good space to invest in? Why or why not?

Privacy-as-a-product describes an individual's inherent right to control their own identity and to decide how, or if, their identity is shared in a particular content. Products that further individual control of data and informed consent operationalize these consumer centric principles. We all have different privacy preferences and values as consumers, and privacy-as-a-product recognizes that individuals alone can choose what is best for themselves as long as they are also provided with context that is clear and easy to understand.

Privacy-as-a-product represents a very real path forward in the digital economy for companies, allowing them to improve their approach to privacy and use of consumer data. ID.me is passionate about user control of data and privacy as a product, and we've found that relationships between brands and consumers grow stronger through transparency and choice.

What's the next stage of "privacy as a product"? Where is this space going, and what are the roles of big and small companies vs. the government or nonprofit bodies?

Consumers are waking up to the fact that they want to be in control of their data and know how it's being used. I think the next stage is all about transparency. Rather than making a consumer make a request to see a copy of the information that a data broker has on file for them, why can't a user simply log into an account and see it for themselves? Why can't they also monitor when and with whom it's being shared? Many consumers check their credit card statements for unusual transactions. Why shouldn't we be able to do the same with our personal information? As part of ID.me's commitment to privacy, transparency, and user control over data, our users can log into their account and see exactly who is receiving what data when. Consumers should expect this same level of transparency in more aspects of their digital lives.

From ID.me's perspective, the growth of our network and other digital wallets represent a paradigm shift where consumers are empowered at the expense of data brokers. Such a shift requires innovation and the adoption of a consumer centric network to wrest away market control, and we are working tirelessly to that end so individuals control their own data.

The United States could soon have a federal private statute. As a company that has worked to advance a new model for privacy and digital identity in which people retain direct control over their personal data, what principles do you think legislation like this should include?

ID.me supports federal privacy legislation. We believe the future of data security must be centralized around three pillars: user control of data, informed consent for data sharing, and data governance.

- *User control of data. Individuals should be empowered to control their own data. Consumers must have sole discretion over their data and where it's shared.*

- *Informed consent for data sharing. Credential service providers and other covered entities should be required to collect informed consent from individuals for the use of their data and should likewise provide options to revoke such consent for continued use.*

- *Data governance. Covered entities should provide a portal to show users where they have provided consent to share data – and allow them to revoke such access.*

This is the third Q&A in a series that DCI is publishing on the topic of Privacy Tech to better inform and engage policy and business stakeholders who are both influencing and influenced by these new dynamics in the privacy landscape.