Embracing A Consumer-Centric Paradigm Shift In Data Privacy

By **Kwamina Williford and Brian Goodrich** (August 12, 2021)

Kwamina Williford

Brian Goodrich

Imagine that you are seeking applicants for a job. You need to do a background check in order to evaluate the applicants' backgrounds. The extensive volume of data available and sources that may be tapped to assess an individual's character is vast.

But, instead of looking to receive sensitive personal information on a potential applicant indirectly from a third-party service, the applicant authorizes you to access a report that communicates the applicant's character and other background information.

No unverified personally identifiable information is shared, there is no need to hold that sensitive information, and the background information that forms the basis for the report is vetted by the applicant to ensure accuracy of information communicated. This approach is not only possible — it's plausible.

In the face of new market realities, this approach presents significant benefits to employers and entities that gather and evaluate individuals' credentials and background. In essence, the approach reroutes control over consumer data, placing it in the hands of the consumer.

This paradigm switch — with the consumer as the source of their own, authenticated identity — holds great promise for companies looking to navigate and streamline thorny issues associated with gathering, evaluating and using individuals' personally identifiable data.

It also may be the key to addressing the myriad concerns facing our society as it relates to consumer reporting. And it aligns with the direction that a proposed federal law may further push the market and the laws governing data privacy.

Legislative Backdrop and Changes Forced on the Market

Data privacy law stands on a precipice. In 2018, California became the first state to enact a comprehensive consumer privacy statute, the California Consumer Privacy Act. Then, on March 2 of this year, Virginia followed suit, passing the Virginia Consumer Data Protection Act.

Set to take effect in 2023, the law establishes rights for Virginia consumers to control how companies use consumers' personal data, and dictates how companies must protect consumer data in their possession and respond to consumers exercising their rights.

These bills, which follow the introduction of the European General Data Protection Regulation standards, as well as a fairly steady stream of high-profile data breaches, are the tip of the iceberg. Over 10 additional state legislatures are actively considering privacy bills.

There is a global awakening to the need for increased consumer control over consumer data. In March, on the heels of the Virginia privacy law, the new federal privacy bill — the Information Transparency and Personal Data Control Act — arrived on the scene.

The title of the federal bill itself conveys the upcoming paradigm shift and the need for a new approach. As it suggests, the bill aims both to set standards related to the control, storage and use of consumer data, and to provide consumers with rights to their data.

The federal legislation, and its state counterparts, come with a number of critical changes. If passed, the federal statute would allow consumers to access and correct their data. It would also require consumers to opt in to sharing sensitive personal information with companies, including financial data, biometric information, geolocation data, and citizenship and immigration status.

Data may only be used to the extent the consumer opts in — meaning that the uses would need to be clearly disclosed at the time the consumer provides their consent to the data usage.

The bill also requires companies to provide consumers with privacy policies in "plain English." It requires companies to disclose those policies to consumers upfront, including the purpose for the data sharing. Finally, the new statute would also require that companies must submit to privacy audits every two years from a neutral third party.

These changes will present compliance costs and risk. What this would mean for those that hire and evaluate candidates for jobs, housing or credit is that policies and procedures will need to be changed to ensure that informed and fulsome consumer consent is captured.

Disclosures and policies will be evaluated for user-friendliness, from the perspective of the "average" or "reasonable" consumer. For those utilizing traditional means of data collection and evaluation — i.e., background or consumer reports assembled by third parties from a multitude of data sources — these requirements may be onerous.

Yet, even more onerous may be the increased liability and pressure faced by those that use and store consumer data, in light of the impending waterfall of consumer data privacy legislation.

Embracing the Consumer-Centric Paradigm Shift

The law is changing. The market is changing. Embracing a consumer-centric paradigm sets your organization up to reduce its privacy and regulatory risk in connection with consumers' character evaluation in the following ways.

Reducing Risk Associated With Identify Theft

This risk is lessened because in this paradigm, the entity evaluating the consumer no longer receives a report compiled by a third party from various public and private sources. The report is instead coming from one source: the individual to whom it relates.

Further, the information will have been authenticated by a service engaged directly by the consumer. Solutions associated with this use case typically utilize secure platforms to present and share reports upon the consumer's request, reducing the risk of unauthorized disclosures of sensitive personally identifiable data.

Enhancing Accountability and Transparency

Lawmakers and regulators are seeking to enhance consumer control and transparency. In

the use case envisioned by this article, consumers have control over who can see their report, as well as the length of time for which those recipients have access to the report.

No longer is the consumer's identity constructed by third parties working behind the scenes, engaging in tactics like screen-scraping or other methodologies in which the consumer is not a participant or clearinghouse for his or her own data.

Increasing Accuracy

Consumers have the ability to review and question the accuracy of the information included in or affecting their report — before the report is provided to any third parties. This layer of review will help to insulate those entities using the report from claims that the information relied on to make a decision was inaccurate or improperly gathered and relied upon.

This model accomplishes the same goals as the consumer information dispute process mandated by the Fair Credit Reporting Act, or FCRA. But it does so upfront, minimizing business risk and disruption caused by inadvertent reliance on inaccurate information received from a third party.

While the consumer ensures the accuracy of the content shown in the report, the consumer should not be able to choose which types of background information appear on the report. Consumers would not be able to cull out accurate information simply because it does not put their character in a good light. In short, increased accuracy would not come at the cost of the organization's ability to meaningfully evaluate the applicant's character.

Minimizing Regulatory Risk

New legislation will not erase the FCRA, which includes some consumer protections related to data privacy. But the traditional character reporting model presents significant FCRA risk and compliance costs.

A benefit of embracing this consumer-centric approach is that such a model can sidestep thorny FCRA questions. Courts have yet to grapple with many of these issues. However, because the reports are provided directly to the consumer in the use case described in the introduction, such use would likely fall outside of the FCRA.

While prudent measures related to accuracy, transparency and security are and should be followed to best protect the consumer's interest, the model itself alleviates many of these concerns the FCRA was designed to address.

The deep angst from regulators related to the lack of transparency and standards for data processing is boiling over. Significant regulation and consequences are coming. These changes will impact who controls consumer data and set standards for data use.

Armed with the knowledge of how these changes can benefit them, organizations that engage in consumer character reporting or identity authentication should prepare for the foreseeable changes in data privacy law by considering alternate, consumer-centric approaches in order to get ahead of the curve.

Kwamina Thomas Williford is a partner and Brian J. Goodrich is an associate at Holland & Knight LLP.