

Biometric Information Privacy Laws and the Privacy Paradox: A Q&A with Simon Blanchard

Simon Blanchard and **Elizabeth Milsark** — 6 MIN READ

States are increasingly wary of the collection and use of biometric data. In this interview, we explore what marketing research can tell us about consumers' attitudes and expectations regarding data privacy.

Many of the laws governing biometric information passed over the last several years aim to protect consumers who entrust companies with their information in exchange for enhanced services or improved user experience. The regulatory burden these laws impose can be substantial. But it often remains unclear to what extent consumers value the privacy of their information, and how they balance the worth of using the at-issue technology as compared to the risks of their data being compromised – for example, in a data breach.

Analysis Group Vice President **Elizabeth Milsark** explored these issues with academic affiliate **Simon Blanchard**, Dean's Professor at the Georgetown University McDonough School of Business. An expert on consumer behavior and marketing, Professor Blanchard focuses much of his research on users' interaction with technology. He and Ms. Milsark discussed the "privacy paradox" inherent in many of these interactions, and what empirical marketing research can tell us about how consumers balance competing values.

Looking at the landscape of biometric information privacy laws in the US, what strikes you as especially salient from a consumer behavior and marketing research perspective?

One issue is the large and pervasive gap between what consumers say about the importance of privacy and how they actually behave when using digital services, social media, and other online platforms. Many consumers say they are very concerned about how companies use their personal data. Yet these same consumers are frequently the ones who use applications and services that are known to collect extensive personal data – and sometimes even accept terms of service and privacy policies without reading them.

In academic literature, this phenomenon is known as the "privacy paradox." It seems to me that much of the state legislation in this area is aimed at tackling this apparent paradox by regulating the way that companies – especially technology companies – collect, store, and use these data, to account for the potential misalignment between consumer attitudes and behaviors.



> *What's important to recognize … is that what drives consumers to trade off uncertain future risks for immediate present benefits is dependent on both the context and users' expectations. This is a matter that is eminently well suited to empirical investigation."*
>
> SIMON BLANCHARD

Give us a sense of how these concerns might play out in real life.

Let's take a hypothetical example. Suppose that a hypothetical consumer electronics company called AquaPhone offers an optional feature called FingerID on its smartphones. By opting into FingerID, consumers can use their fingerprint to quickly and securely unlock their devices. However, to do so, it is necessary for AquaPhone to collect, store, and use a detailed fingerprint. For users who choose to enable the FingerID feature, AquaPhone provides screens (i.e., a feature sign-up flow) that explain what data are being collected. Of course, it also provides a comprehensive terms-of-service document detailing how users' information is collected, stored, and used.

Why is it that so many consumers say they are concerned about privacy and the risks of losing control of their personal data, and yet still enable services that collect this information?

You can see this dynamic in the hypothetical AquaPhone example. On the one hand, consumers are providing their personal information (a fingerprint) to AquaPhone – something that consumers often report that they want to protect. On the other hand, consumers who complete the opt-in sign-up process for FingerID learn about the context-specific benefits of providing their fingerprints, such as not having to remember a password, time saved from typing, and

enhanced security. The consumers who have opted in to the hypothetical FingerID process are suggesting that the perceived benefits of the sign-in process outweigh the potential concerns with sharing their personal information.

That's an example of the privacy paradox.

Exactly: Consumers express concerns about the privacy and safety of their data yet entrust companies with their use anyway. That raises the question of why. Do they understand the risks and benefits and simply believe the benefits outweigh the risks? Do they not fully understand the risks, and therefore underweight them?

What's important to recognize about this scenario is that what drives consumers to trade off uncertain future risks for immediate present benefits is dependent on both the context and users' expectations. This is a matter that is eminently well suited to empirical investigation.

How have you used empirical methods to study tradeoffs?

In my own research, I have studied consumers' evaluation of and tradeoffs between risks and benefits and how these perceived tradeoffs influence consumer preferences for various products and services. For example, in one study, my coauthor and I conducted a field experiment aimed at understanding how consumers of different ages react to messages encouraging them to purchase life insurance. We found that young adults, in particular, respond differently to messaging that frames life insurance as a product providing present gains versus avoiding future risks. This exploration revealed how the temporal framing of messages can significantly influence consumer behavior.

What kinds of tools and methods are best suited to exploring these types of questions in the context of biometric information and data privacy?

A number of empirical tools can be relevant in the context of biometric information privacy. Experimental surveys, when executed carefully, are especially useful because they can help us determine whether and to what extent consumers understand and weigh the benefits and tradeoffs of providing their data and, thus, contextualize the concerns raised by parties to litigation or by the government in investigations.

First, in some instances, surveys testing consumer understanding can be used to evaluate whether and to what extent consumers have misconceptions about the data being collected or stored, or how those data are used. These questions can be relevant to determining whether consumers have sufficient information regarding how data are collected and used and whether the collection and use of these data are being adequately disclosed. Archival research of company documents and analyses conducted in the ordinary course of business can also be relevant to this inquiry.

Second, surveys testing consumer behavior and decision making can also be relevant to understanding whether and to what extent the alleged gaps in disclosures or understanding have an impact on consumer behavior. Results from these surveys can shed light on whether consumers would have made different decisions – such as not opting in to a service or not using a service as often – in the face of more information or clearer disclosures.

Finally, surveys testing consumer purchase drivers or consumer attitudes about a product or service's functionality can be applied to evaluate the priorities and perceived benefits consumers associate with the functionality facilitated through the sharing of biometric information. Such research can be important to understand potential unintended consequences of implementing proposed relief sought by plaintiffs. In fact, such research can help one determine if some consumers may be harmed, on balance, from barring or limiting the use of at-issue features, functions, products, or services, and the potential for raising the costs of accessing products or services. Evaluations of consumer decision making using academic frameworks such as the consumer buying process can also be relevant to this inquiry.

So, how is this kind of information relevant to biometric privacy litigation? What questions could an expert opine on in that context?

Because of the privacy paradox, directly asking survey respondents whether they care that their data are being collected can be very misleading if one doesn't properly contextualize the tradeoffs and potential benefits of the data collection. Experts in these litigation matters can help provide this context.

Using rigorously designed surveys and other research tools, consumer behavior and marketing experts can opine on, for example, what consumers understood themselves to be doing when they agreed to a set of terms for a service, and whether the decision they made was well informed. They can also help elucidate why such consumers made the choices they did and whether they would make different decisions in the face of additional revised disclosures. All of these can help factfinders navigate these complex matters. ▪