Facing the Risks: Biometric Data

Malk Insights — January 2024

Key Takeaways

- Not only has the collection and use of biometric data outpaced regulatory and ethical frameworks in recent years, emerging use cases for this data have the potential to inflict significant social harm.
- These risks include those related to privacy, including unauthorized access, misuse, consent, and transparency, as well as higher-level ethics concerns around the potential suppression of civil liberties through mass surveillance or discriminatory outcomes.
- When investing in such data collection technology, GPs can not only carefully consider these risks, but also adopt best practices to ensure robust data governance and regulatory compliance, as well as monitor end-use to prevent adverse outcomes to both businesses and individuals.

Biometrics: The New Frontier of Data Collection

Facial recognition, fingerprint scanning, voice identification—these increasingly ubiquitous emerging technologies are considered biometrics, or data related to unique physical, biological, or behavioral traits, characteristics, or measurements. In recent years, biometric data collection has become more publicly visible and heavily scrutinized, reputationally and financially impacting companies leveraging such technology.

In 2023, for example, the Transportation Security Administration (TSA) integrated facial recognition technology into the screening process across select airports in the U.S., leading to concerns among privacy advocates around the TSA's biometric data retention procedures. Notably, technology leveraged by the TSA is sourced solely from one private equity-owned company. In response to controversy, the bipartisan Travel Privacy Protection Act was introduced which argued that travelers were not made adequately aware that they could opt out of the facial recognition program, and that the TSA should be required to not only obtain congressional authorization to use the technology and delete related biometric data, but also be banned from expanding the program further. Importantly, both senators and privacy advocates have cited the potential for racial discrimination to be exacerbated by the technology, as well as the overarching concern that biometric data could fall into the hands of unauthorized third-parties, including private companies or malicious actors.

This debate around the TSA's use of facial recognition technology is just one example within the larger discussion around biometric data collection and its potential consequences. Use cases for biometric data can range from the seemingly innocuous, such as heart rate monitoring on wearable fitness devices or prescription verification and patient identification, to potentially insidious, including facial recognition in public spaces, surveillance by police forces, or using biometrics for deceptive marketing tactics. Innocuous or not, however, it is crucial for investors to navigate this new frontier of data collection ethically and with a sensitivity for privacy,

understanding the inherent risks associated with biometrics, best practices among companies, and even when to reconsider investing.

Privacy Risks of Biometrics

The risks related to collecting biometric data largely fall into two categories: privacy and ethics. Privacy concerns on biometrics are centered around the potential for unauthorized access and misuse, both of which are exacerbated by the sensitive nature of biometric data. Importantly, biometric data is inherently unique to the individual, making it a powerful identifier, and in most cases are irreplaceable unlike a password or PIN. In addition to applications such as facial or voice recognition, biometric data collection also includes information like genetic data, which not only reveals sensitive data about the individual, but also about their relatives. Further, while some biometric data types can be anonymized or de-identified (albeit less effectively than with non-biometric data), it is not always possible to do so with genetic information. As such, the severity of a privacy incident is heightened considerably when biometric data is involved.

For example, Biostar 2, a biometric security system developed by South Korean company Suprema and used in the security systems of commercial buildings globally, experienced a data breach in which unsecured biometric data, including fingerprint and facial recognition data, was found in a publicly accessible database. The cache included nearly 30 million records and allowed hackers to access any building secured using Biostar 2, as well as platforms integrated with the program, including security systems used by organizations such as governments, banks, and the UK's Metropolitan Police service. Consequently, the company experienced both negative press as well as inquiries by the Information Commissioner's Office, the UK's data regulator.

Further, there are significant risks related to consent and transparency when it comes to biometric data, as well as potential noncompliance with evolving regulations. Much of the negative press related to biometrics concerns the seemingly opaque manner in which data is collected, processed, and stored. In particular, individuals may not fully understand the implications of providing biometric data, or whether it may be collected for a specific or secondary purpose, such as profiling or other surveillance. Instagram, for example, was subject to a class action lawsuit alleging the company violated the Illinois Biometric Privacy Act (BIPA)—the U.S.'s only law governing biometrics, albeit at the state-level—by failing to obtain informed consent around a facial recognition feature launched in 2015, resulting in a significant settlement of $68.5M in 2023. Further, Clearview AI, a venture-backed facial recognition company, faced public and legal scrutiny related to its sale of biometric data to not only private entities, but also police forces nationwide without the consent of individuals. In response, both New Jersey and Illinois state governments have placed bans on the technology, and Clearview AI has been required to comply with a series of BIPA-aligned restrictions. These examples are two of many and demonstrate that the implementation of biometric data collection mechanisms without the necessary concern for transparency can have serious impacts on businesses.

Ethics Risks of Biometrics

On the other hand, biometric data collection poses ethics risks based on how such data is leveraged by the end-user. Notably, certain applications, such as the use of biometrics in public spaces (both in person and online) can be considered biometric mass surveillance, as this process of turning human biology into data is indiscriminate, large-scale, and without the control or knowledge of affected individuals. While there is no explicit ban on this kind of mass surveillance in the U.S., the recently passed EU AI Act has implemented safeguards to protect individuals against profiling, though there remain exceptions for certain law enforcement activities. That said, there is no law which completely prohibits biometric mass surveillance in the EU, either. Even if the data is subject to deletion, individuals can perceive this surveillance to be a form of social control,

leading to a 'chilling effect' in which people are disincentivized from participating in public life out of fear of being watched at all times.

These ethics risks are compounded, however, when the publicly collected data is utilized for harmful purposes such as profiling or recognition without individuals' knowledge or expressed consent. Prominently, MSG Entertainment, owner of Madison Square Garden and Radio City Music Hall, experienced significant backlash when several news outlets reported that the arena was utilizing facial recognition to inform an exclusion list composed of lawyers representing people suing the company. In addition to the risks of mistreating paying customers, civil liberties groups warned that this application of technology could discourage people from accessing the legal system, raising the question of whether anybody would take legal action against a company that would retaliate in this way. Importantly, if customers can be banned from sport or concert venues through biometric profiling, other businesses may follow suit and use biometrics as a means to subvert the legal process, thereby suppressing individual civil liberties.

Ethics concerns related to biometrics additionally include the potential for discriminatory outcomes resulting from factors such as algorithmic bias due to a lack of representative data in training or underrepresentation due to unequal access to technology, both of which can result in varying accuracy rates across demographic groups. Studies by the National Institute of Standards and Technology (NIST), for example, have found that facial recognition is more likely to misidentify Asian and African American people. Taken a step further, the application of biased biometric data technology, particularly in law enforcement, can contribute to discriminatory outcomes through heightened risk of profiling or the targeting of specific demographic groups. These biases can lead to disproportionate surveillance, and consequently, disproportionate law enforcement actions, particularly against people of color. FaceFirst, a private equity-owned facial recognition company whose technology is utilized by national retailers, was subject to scrutiny in 2020 after it was found to have regularly misidentified shoppers across 200 Rite Aid stores over eight years. Specifically, the technology led to false matches that disproportionately identified people of color as shoplifters or mistakenly matched individuals of color—Rite Aid eventually ended its relationship with FaceFirst, highlighting the business impacts for investors backing technology that is not deployed with adequate ethics considerations.

Managing Biometrics Business Risks

Despite the widespread use and significant risks associated with biometric data, there is no comprehensive law in the U.S. that addresses its protection—in addition to BIPA, businesses must take a piecemeal approach across regulations by relying on relevant provisions from different privacy laws, including but not limited to the California Privacy Rights Act, the EU's General Data Protection Regulation and AI Act, as well as various state-level privacy regulations that may or may not address biometrics. To not only safeguard data and protect individuals but also navigate this evolving regulatory landscape, investors targeting businesses that collect biometric data should ensure that such companies are implementing data privacy and ethics and compliance practices that are on par with the most stringent industry standards (e.g., ISO 30107, ISO 19794, NIST Biometric Evaluations).

Robust privacy practices may include technical controls such as encryption, multi-factor authentication, or tokenization, or may include operational processes like personnel trainings, access controls, or codified policies related to biometric data collection, storage, and use. On the user-facing side, businesses should ensure that the underlying data used to train algorithms reliant on biometric information is representative of those who will be subject to the technology in order to prevent discriminatory outcomes. Companies must additionally make it a practice to ensure customers are adequately and transparently informed of if, how, and why their biometric data is being collected, including any secondary uses that may not be as apparent. As businesses across

industries—whether it be entertainment, security, or retail—continue to collect and leverage biometric data, it will be increasingly crucial for discerning investors to be able to identify not only risks, but also best practices related to biometrics. Malk is well positioned to serve as a partner in supporting both investors and management teams seeking to better understand and manage the unique risks associated with biometrics beginning in diligence and through exit.

Authors

Rae Edmunds
Senior Associate
e: redmunds@malk.com

Christina Tedeschi
Project Manager
e: ctedeschi@malk.com

About Malk Partners

Malk Partners is the preeminent advisor to private market investors for creating and protecting value through environmental, social, and governance ("ESG") management and impact investing. Founded in 2009, Malk Partners advises many of the world's leading alternatives managers investing across private equity, growth equity, venture capital, and private credit by helping them define ESG goals, achieve ESG results, and guide their portfolio companies in driving value creation and mitigating risks. The firm is headquartered in La Jolla, California with a second office located in New York. For more information about Malk Partners, please visit www.malk.com.