SentryCard: Addressing Privacy Concerns

The protection of biometric data is of paramount importance. Any breach exposing this ultra-sensitive personal data poses significant risks and liabilities to the organization as well as to the affected person.

In order to keep organizations accountable, several U.S. States have passed legislation regarding the collection, storage and use of biometric data. Internationally, the E.U.'s General Data Protection Rights (GDPR) legislation, along with the rules in the UK and India provide a strong stance on biometric data protection and the associated liabilities.

The potential liabilities for the mishandling of biometric data are considerable. Under Illinois' Biometric Information Privacy Act (BIPA) penalties range from $1,000 to $5,000 per violation, per employee, until remedied. Internationally, under GDPR, penalties could total up to 4% of a company's revenue or 20 million euros (whichever is greater).

> "Utilizing the SentryCard will demonstrate to regulators your commitment to protecting your employee's sensitive biometric information."
>
> David Ross
> Chief Privacy Officer
> GreyCastle Security

Sentry Enterprises is committed to having a Data Processing Agreement (DPA) in place with each of its resellers by mid-2021.

KEY PRIVACY ATTRIBUTES: The SentryCard eliminates most of the risks associated with using biometric authentication by removing all human access to the biometric data.

1. **DECENTRALIZED:** Biometric data is enrolled, stored and matched solely within the SentryCard platform, never touching an external database or server. With SentryCard there is no large "honeypot" of biometric data for hackers to pursue.
2. **UNIQUE:** Each SentryCard generates its own unique inaccessible encryption key used to protect the biometric data stored within the card.
3. **NON-TRANSFERABLE:** The SentryCard is a single-use solution. Once a person's biometrics are enrolled only that person can ever use the credential.
4. **CONTROLLED:** Once issued, the holder maintains control of their biometric data, stored securely within the credential.
5. **IRRETRIEVABLE:** Enrollment of the holder's biometrics are one-way and irreversible once set. The credential's only output is an affirmative or negative authentication.

SENTRY