Use Case: Intrinsically Protecting User Data

Although the majority of enterprise businesses have deployed concentric or perimeter-based security architectures using a combination of detection, protection and transportation technologies, the results are good, but fall short after witnessing the numerous and recent corporate data breaches in the news and the loss of billions of user's records. In many cases, human error played the largest role from misconfiguration, fraudulent scams, stolen mobile devices, and even intentional security violation. However, the real issue is that the data that "directly or indirectly" identifies an individual is typically not protected or encrypted in the event of an unauthorized breach. This has prompted regulators' concern about data security and the threat of hacking as well as the need to protect sensitive consumer and corporate financial data.

The European Union first blazed the trail to protect consumer personal information when the General Data Protection Regulation (EU) 2016/679 or "GDPR" became law on May 25, 2018. The United States quickly followed suit, as each State began rolling out their own regulations. In March of 2018, all 50 U.S. states enacted breach notification laws that require businesses to notify consumers if their personal information is compromised. California lawmakers enacted the California Consumer Privacy Act of 2018 or the "CCPA" June 28, 2018. Others included Alabama with SB 318, Arizona with HB 2145, Colorado with HB 1128, Iowa with HF 2354, Louisiana with Act Number 382, Nebraska with LB 757, Oregon with SB 1551, South Carolina with H4655, South Dakota with SB Number 62, Vermont with H. 764, Virginia with HB 183 and many others followed. California has already made several amendments, in October 2019 and in November 2020 the California Privacy Rights Act, which amends and expands the CCPA.

Many of these data protection acts also stipulate that consumers have the right to be forgotten and to request that any data a company has on them be deleted. There are some limits on what data a business can retain for legal, compliance, and business reasons, but a solution must be in place to timely delete all other information about a consumer.

Deploying Bonafeyed's ***Cy4Secure*** technology encrypts consumer personal data, in real-time and the data remains protected when accessed by authorized users within an enterprise's network, or outside by 3rd party partners or mobile devices. In addition, the consumer datasets when placed on backend Business Enterprise systems or in the cloud for collaboration or archival storage remains natively secured. However, when encrypted data is lost, stolen, abandoned, or forgotten, it becomes demonetized ensuring cybercriminals or internal non-authorized users only obtain unintelligible data and permanently inaccessible once the cipher keys to access the data are deleted or retired, which exceeds data protection legislation.

The frequency of breaches also arises from focusing on perimeter security and not on protecting the data itself. Data that remains in the "clear" is vulnerable. Bonafeyed can secure individual data elements, such that any loss of data whether by a mega breach or down to an end-user's mobile device is mitigated. Traditional security products are just one part of the solution. Since cybercriminals have found quick ways to monetized stolen data, without directly securing and protecting the data, these massive breaches and data exploits will continue to occur.

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.