ACTIVE CYPHER

Are You Violating Privacy Laws and Don't Know It?

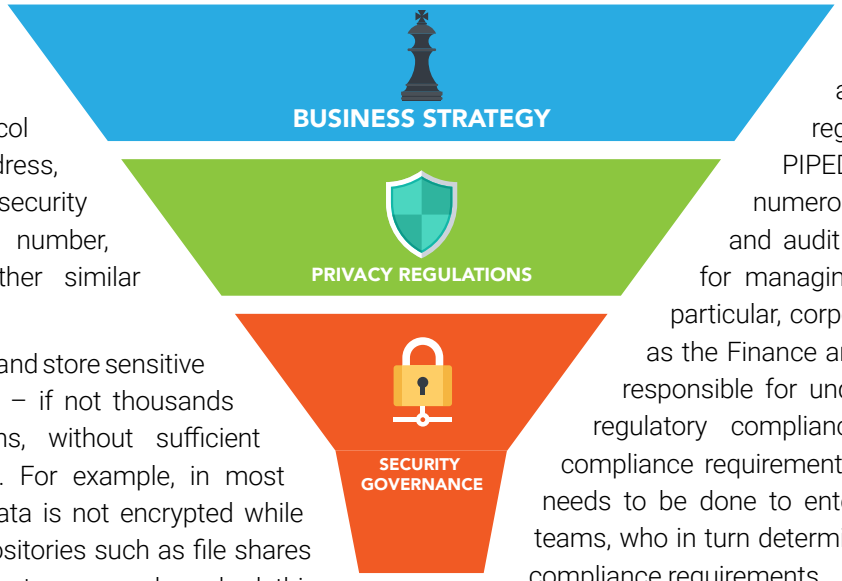
Privacy is a complex matter for corporations, institutions and society. Organizational policies, governance, law, compliance, company products and services, operational infrastructure, standards, technology, consumer trust and branding all play a role. In addressing privacy many organizations have elected varied approaches and tools contingent upon industry, regulatory and cultural contexts; establishing corporate privacy officers, privacy councils, technologies and tools - but are still learning what to do about privacy. A litany of privacy protection regulations have emerged over the past two decades, including the following:

- **HIPAA** – the Health Information Portability and Accountability Act establishes U.S. national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.
- **PCI** – the Payment Card Industry Data Security Standard (PCI DSS) was created to increase controls around cardholder data to reduce credit card fraud and applies to companies of any size that accept credit card payments.
- **PIPEDA** - the Personal Information Protection and Electronic Documents Act (PIPEDA) is the Canadian federal privacy law for private-sector organizations to regulate the way private-sector organizations handle the personal information in a commercial activity.
- **CCPA** - California Consumer Privacy Act (CCPA), passed in 2018 is a bill that enhances privacy rights and consumer protection for residents of California. CCPA is modeled closely after the 'grand-daddy of all privacy laws', GDPR.
- **GDPR**- General Data Protection Regulation (GDPR), which governs the processing of personal data of EU citizens.

The privacy regulations listed above are but a few of the myriad laws that require proactive compliance in order to protect the personal identifiable information (PII) data of customers, employees, contractors and business partners around the globe. Some are industry-specific, such as HIPAA within Healthcare, but they mostly apply to all industries. Using GDPR, one of the most recent and perhaps far-reaching privacy regulations of all as a signpost, many organizations may collect personal information as part of operating functions and are now subject to GDPR compliance – whether the organization is based in EU, the U.S. or elsewhere in the ordinary course of its business.

As an example, GDPR defines two types of PII data: personal information, such as would be commonly found on business cards; and sensitive personal information, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, etc. CCPA defines personal information as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household such

as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.



Many companies process and store sensitive PII, available to hundreds – if not thousands of enterprise applications, without sufficient data encryption in place. For example, in most corporate systems this data is not encrypted while 'at rest' (i.e., stored in repositories such as file shares and databases). If such systems were breached, this identity data would be easily exposed and exploited. And make no mistake – this data is pure gold to criminals as well as rogue nation-states.

Take this further, daily business operations for most enterprises today commonly involve the use of cloud-based applications and services to distribute and share corporate data that includes PII. The use of these off- premise, co-tenanted services typically results in unstructured personal information being disseminated in environments that are not controlled to the same extent as on-premise systems. In many cases, accountability for controlling access is a shared responsibility between the enterprise and its cloud providers, but existing contracts are highly unlikely to provide clear lines of demarcation with respect to those shared responsibilities - particularly in light of GDPR or CCPA requirements. Off-premise environments are particularly vulnerable to sensitive information being moved outside of normal IT controls, whether accidentally or maliciously. There is a high likelihood that many enterprises' current SaaS providers lack the necessary controls, monitoring, and audit capabilities that would be required for that enterprise to comply with GDPR or CCPA.

In order to sufficiently protect the use of an individual's data, regulations such as GDPR, PIPEDA and CCPA expect numerous governance, control and audit schemes to be in effect for managing access to PII data. In particular, corporate business units such as the Finance and Legal departments are responsible for understanding and ensuring regulatory compliance. These groups feed compliance requirements – in the form of 'what' needs to be done to enterprise Security and Risk teams, who in turn determine 'how' best to meet the compliance requirements.

One of the most fundamental capabilities associated with how to protect data in general and PII in particular - is through encryption. The current regulatory compliance and intellectual property protection requirements are now front-and-center for nearly all enterprises. The demand for a simple to use yet exceedingly secure encryption solution such as Active Cypher will increase as traditional enterprise barriers disappear and virtual barriers enabled via end-to-end file encryption become the norm.

That said, competitors in the user-centric file encryption market have not been able to develop such low-overhead and simple-to-deploy solutions. As a result, many enterprises have not deployed file encryption because of the extensive, costly and error-prone administrative overhead required to deploy these competitors' solutions. As the traditional enterprise security barriers continue to morph into perimeter-less, zero trust models, the elegance and effectiveness of Active Cypher's file encryption solution becomes the best way augment your Azure AD-centric environment with fully integrated file encryption that spans both on-premise and cloud-centric environments.