October 2018

The Intersection of Privacy and Security

An article by Pamela S. Hrubey
As cybercriminals and their tools become increasingly sophisticated, so must the approach to thinking strategically about information security and privacy. Information technology (IT) professionals and ordinary individuals alike must stay one step ahead of the game when it comes to protecting information assets, whether proprietary company information or personal data. However, these efforts often result in a struggle to balance security practices against data protection, especially when considering the rights of data subjects.

**Foundation of data protection**

Whether a company is dealing with privacy concerns of its employees and customers or with vast amounts of personal data from big data-related operations, personal data is the foundational concern of the information strategy that a company builds. Moreover, protection of that personal data is the core point at which privacy and security interests intersect. A comprehensive data protection strategy must consider the integration of best practices to both security and privacy. Data integrity, retention, and availability are part of the overall data protection goal for an organization, and as such, they are tied directly to individuals’ rights as data subjects. Data-dependent organizations that want to succeed in this changing environment must understand that protecting personal data is nonnegotiable and bring security and privacy professionals together for the common goal.
What does privacy mean?
Often defined as “the right to be let alone,” the concept of privacy has changed in the modern data-driven era, and it can be increasingly difficult to maintain. New technologies such as the internet of things (IoT) reveal vast privacy concerns that businesses and individuals never before imagined. Internet-connected security cameras, smart cable boxes, and smartwatches have redefined what privacy entails. For example, recent pushback from the U.S. military demonstrates the unintended consequences of the IoT when analysts discovered that enemies can potentially identify troop locations via GPS-based data from wearable technologies such as fitness trackers worn by military personnel.

Thanks to technological advancements, individuals and organizations are more interconnected than ever, and, as such, the concept of privacy is evolving. Data-based personal privacy has become less a matter of invisibility and more a matter of the type of data collected, who has access to it, how data will be used, and how long it will be stored. Simply put, personal data is now understood to belong to an individual, not to an organization. In addition, with regulations such as the General Data Protection Regulation, organizations increasingly understand that they essentially borrow this personal data for a specific business purpose and must use it within parameters to which the data subject agreed to in advance.

Business and operational impact of privacy concerns
As individuals become more aware of how organizations collect, store, and secure personal data, they are also getting smarter about how they want their data protected. Increasingly, individuals are choosing to share their data only with companies that develop and abide by data protection-related best practices. The privacy concerns and focus on individuals’ rights with regard to data has spearheaded a drive for stronger protections. High-profile data breaches, such as social media sites collecting and sharing personally identifiable information with research consortiums and other companies, are stark reminders of why users are concerned and how information can potentially be shared without users’ knowledge or consent.

Employers, too, must align their operational needs to data protection principles. Take, for example, employees using personal mobile computing devices on company networks. Companies require employees to sign acceptable use policies (which can limit personal privacy rights for the device), sync to stored personal images and videos, and include a right-to-wipe agreement in case of a lost or stolen device. Whenever employees connect personal mobile devices to company networks, they expose the company to a measure of vulnerability and, at the same time, they accept limited rights to privacy in order to protect that company’s data.
Achieving balance
Privacy cannot exist without security, but security can exist without privacy – not an ideal situation for anyone concerned. With the continued advance of technology, organizations and individuals must continue to increase awareness and knowledge of data protection, data threats, and the steps required to ensure security and privacy while still maintaining effective business practices and relatable social media interactions. The way to develop a resilient privacy and data protection program is to combine privacy- and security-related thinking into a common approach that makes it easier for employees in all organizational levels to do the right thing. As we continue to move forward in the data-driven world, we must view ourselves as data subjects and strive to attain an agile balance between security and privacy interests.

Learn more
Pam Hrubey
Managing Director
+1 317 208 1904
pam.hrubey@crowe.com