CEP Magazine - October 2020

Shifting to the ethical mindset when making data decisions

By Pamela S. Hrubey, CCEP, CIPP/US, and Candice M. Moschell, CISSP

Pam S. Hrubey (pam.hrubey@crowe.com) is Managing Director and **Candice M. Moschell** (candice.moschell@crowe.com) is Senior Manager of Healthcare Cybersecurity at Crowe LLP in Indianapolis, Indiana, USA.

Handling personal data ethically is a relatively new concept that requires thinking differently about data privacy and security.[1] Decision-makers and leaders who shift from compliance-based to ethics-driven decisions can provide significant value to their organizations.

More than ever, organizations are using personal information to do business—sometimes without the owners' explicit consent. Maybe that use is an ad[2] that shows up during an unrelated web search, or maybe it appears as a solicitation[3] from an organization with whom the owner of the information desires no involvement. Over the past three to five years, data analytics and data mining to drive business decisions and smart advertising have dramatically increased[4] the potential for organizations to operate less transparently regarding their business use of personal information.

While the use of personal information in a nontransparent way might be on the rise, some companies also are starting to see a tangible benefit from investments they have made or are making in their privacy and data protection programs. Cisco's *Data Privacy Benchmark Study*,[5] released in January, describes a return on investment made into privacy-related programming, which demonstrates that most organizations are seeing a positive return on their privacy investments. Based on the results of this benchmark study and on extensive experience supporting clients across a variety of industries and leading in executive-level privacy practitioner roles, it is clear that taking a data ethics approach to collecting, processing, retaining, and destroying personal information can provide a similarly positive return on program-related investments.

Why do companies focus on privacy and data protection?

Fear of reputation damage or fines and penalties resulting from noncompliance are often at the root of business decisions relating to privacy and data protection. Compliance drives standards, policies, procedures, and best practices for data that in turn provide sound privacy and security practices to protect these data. Values and ethics, on the other hand, are based not on consequence but rather on what is viewed within and across the organization as what is right or wrong in the context of the business the organization is doing.

If someone sees another person drop their wallet, chances are they will stop the person to return it. That act is based on ethics rather than fear of consequences for not returning the wallet. Data ethics should be thought of in the same manner. In short, it's about doing the right thing. Organizations should be asking themselves hard questions about data subjects and the implicit use of their information as opposed to thinking of these data as raw material or thinking only about the compliance requirements of the data. Starting from a foundation of strong ethics, organizations can build programs and use data in a way that can result in attracting and retaining customers.