COSMOS
Navigate the Compliance Universe

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.

What should relevant leaders understand about personal data?

Organizations often find that the inability to understand the full nature of the data elements held within their databases can make the transition from compliance-related thinking to ethics-driven data decisions challenging. Knowing where personal data are housed across the organization and understanding the data elements that the data set encompasses provide a relevant context to which ethics and values can be applied.

Many tools are available to help organizations identify and classify the data they hold. However, prior to making a tool purchase, organizations should complete a data discovery assessment by answering the following questions:

- Where are the data coming from?
- What are the various streams of data?
- What processes manipulate these data?
- Where do data live in the short and long terms?
- Who is the data steward?
- What training has been given to the data steward?
- Who requests access to the data, both internally and externally?
- Where do the data go outside of the organization?

In answering these and other questions, often the best place to start is with the data stewards (or application owners). Data stewards typically have a deep understanding of the data they maintain and sometimes have developed a data flow diagram that can answer many of these questions and significantly cut down on assessment time. In speaking with them, it is equally important to understand what type of training they might have had regarding their responsibility to secure, protect, and act ethically with the data. Unfortunately, these discussions often reveal that major gaps exist in training programs. While getting the answers to those questions can seem tedious and take a significant amount of time, it frequently reveals the complicated relationship organizations have with data and highlights some of those ethical concerns.

How can organizations reframe their thinking on personal data?

With the advent of the General Data Protection Regulation (GDPR) in May 2018, data subject rights (including, but not limited to, the rights to receive notice of data processing, correct or have personal data erased, and object to automated processing) moved front and center in all companies that do business in the European Union. Data subject rights come to life for individuals when they receive a privacy notice, describing for them what personal information might be collected, how these data will be used, how they will be shared, and where they will travel. The privacy notice companion is privacy consent, and the GDPR specifies that consent must be established affirmatively, in advance of data collection.

Approaching data collection from an ethics perspective, organizations can begin to think about data collected from an individual data subject as an asset that is on loan from the individual, not as something that is owned by the organization. The asset—the property of the individual—is being collected and used for a specific purpose, a purpose that is described ahead of time. The organization's use of the personal data is limited to what was described in the privacy notice and related privacy consent. Information cannot be used later for another purpose unless the individual data subject re-consents or the data are safely deidentified.

What do organizations need to focus on for strategy?

One concern that likely is top of mind when thinking about data ethics is the transfer of data to a third party for use in altruistic research, to promote a paid service, or for profit. While an entire book could be written on this subject alone, organizations should focus on and evaluate two areas as part of their data ethics strategy.

The first area involves the concepts of deidentification and minimum necessary, or providing the minimum necessary data for a business need. While these concepts usually are adopted when dealing with healthcare and diagnostic data to comply with various Health Insurance Portability and Accountability Act privacy regulations, organizations in all industries should consider deidentification and minimum necessary both when using data for internal testing and when providing the data to a third party.

Deidentification and minimum necessary can be difficult to accomplish based on the needs of the data set. For example, if a third party requests a data stream to mock process billing, it likely will need data elements that could tie back to the individual party. It is challenging to strip those data elements without losing the integrity of what is needed to fulfill a task. For instances in which pseudo-random replacements cannot be substituted, organizations should take the minimum necessary approach in which they follow a risk assessment process to fully understand and stringently challenge all data elements requested, thereby providing only what is absolutely necessary to fulfill the business need.

The second area organizations should consider as part of their data ethics strategy is performing due diligence risk assessments on any third (or fourth) parties to whom they might be transferring data. Organizations often perform due diligence risk assessments and evaluate privacy and security risks for any third parties they engage that will store, process, or house transferred data. However, two actions that are taken less frequently but that are recommended include:

- Performing risk assessments on all requestors of data regardless of whether the third party is providing a paid service.
- Performing risk assessments that include data ethics controls and seek to evaluate if the data organizations are loaning will be both secure and used in an ethical manner.

Again, keep the data subject in mind when creating these controls. Data provided by an individual should be treated as information "on loan" from the data subject.

'We don't delete anything'

Another concern when thinking about data ethics is data retention. For most organizations, data retention is an established, documented policy. But in reality, this policy tends to reflect a "we don't delete anything" mentality, which poses significant risk, liability, and data ethics implications. While laws and regulations provide rules on the minimum length of time to retain data, they do not provide specific guidance on the maximum length of time data can be held, which leaves organizations questioning when it's safe and ethical to delete data. Said another way, organizations sometimes struggle to operationalize regulatory requirements stating that data should be kept for no longer than necessary for the processing-related purpose.

Organizations should ask two questions when thinking about data retention. The first is, "Have we met our legal obligation?" This question is what drives most organizations' data-retention policies. When answering this question, organizations should make sure to confer with compliance or legal counsel, as, based on the data elements involved, legal requirements will vary.

The second question organizations should ask is, “Do we need these data any longer to fulfill the purpose for which we originally captured them?” This question involves an element of judgment about necessity and transfers an ethical dilemma to the person answering the question. However, as with creating data ethics controls, this question should be answered with the data subject in mind, through the lens of borrowed data, and with the depth of knowledge gained from understating the business need for the data. If organizations recognize that the data were collected only to support a specific time frame, such as processing a claim for service provided for one visit, then these data are no longer needed to support their original purpose. While the data most certainly could be retained longer and used for data analytics, the organization would be operating outside the bounds of what the data subject likely understood in the original agreement.

How can organizations transition to handling data ethically?

Handling personal data ethically is a concept that might be new to some organizations, and by no means are organizations de facto unethical by not having approached privacy from an ethical perspective. Taking an ethical approach to security and data privacy requires thinking differently. The following 10 questions can help organizations decide what approach to addressing privacy and data protection–related concerns is best for the business and for the customers, employees, stakeholders, and third parties with whom they conduct business.

1. Is the organization asking individual data subjects to give up control of their personal information in exchange for use of a free service?
2. Does the organization clearly describe for individual data subjects how the exchange of their personal information could affect them?
3. Do the data subjects that share personal information with the organization trust the organization’s ability to keep their personal information safe from breach, misuse, or alteration?
4. Does the organization clearly describe for data subjects how their personal information is used in consent-related language, avoiding highly technical language and using words that are readily understandable?
5. Does the organization clearly describe for data subjects with whom it will share their personal information (third and fourth parties)?
6. Does the organization test to see if data subjects understand the privacy notice provided to them?
7. Does the organization get clear and unambiguous consent from data subjects who submit their personal information?
8. Does the organization limit the use of personal information to what was described in the privacy notice and privacy consent?
9. Does the organization report to data subjects any potential breach of their personal information and provide appropriate protections for them when a breach is confirmed?
10. Do business leaders across the organization understand that the personal data held are not owned by the organization?

What does the future hold?

While ethics-driven data collection models might be new, decision-makers that approach collecting, processing, retaining, and destroying personal information using a data ethics lens can provide significant value to the organization. By evaluating and assessing their current data strategies, business leaders can make more informed decisions about how to address privacy and data protection–related concerns in the future.

Takeaways

- Organizations are moving from a compliance-driven model of privacy and data protection to an ethical decision-based model with the data subject at the center.
- Understanding the personal data collected and maintained by the organization supports an ethical decision-based privacy and data protection program model.
- Organizations should consider personal data collected from an individual as an asset "on loan" from the data subject, not as something owned by the organization.
- Sharing personal data with third parties can have a detrimental impact on the individual data subject if not carefully managed.
- Answering some key questions can help organizations begin the transition to an ethical data decision-based approach to privacy and data protection.

[1] Pamela S. Hrubey, "The Intersection of Privacy and Security," Crowe LLP, November 1, 2018, https://bit.ly/34gca0k.
[2] Wharton School of Business, "How Will Targeted Ads Fare in an Era of Data Protection?" University of Pennsylvania, June 22, 2018, https://whr.tn/325t53b.
[3] Jaclyn Peiser, "Women Get an Unwanted Surprise by Mail: You're Pregnant! (They're Not.)," *The New York Times*, October 25, 2019, https://nyti.ms/328qO7b.
[4] Insight Center Collection, "Data-Driven Marketing: The Science of storytelling and brand performance," *Harvard Business Review* (May–June 2018), https://bit.ly/2Yj0ar8.
[5] Cisco, *2020 Data Privacy Benchmark Study*, January 2020, https://bit.ly/3aGHbMi.