DATA ETHICS PART II:
Handling Personal Data Responsibly

BDO

PART II:

Ensuring Proper Protections are in Place when Sharing or Selling Personal Information

The use of data analytics to monitor user behavior is a tried and true marketing methodology. Ethical use of data is more pressing as new privacy laws in the U.S. become effective, like California's Consumer Privacy Act (CCPA), Maine's Act to Protect the Privacy of Online Consumer Information, New York's Privacy Act, and Nevada's internet privacy amendment (SB220).

The first part of this series provided ethical guidance around data protection and privacy by outlining a four principle Data Ethics Framework:

- Clearly define the project and its benefits
- Use data proportionate to the project
- Develop a transparent program that holds the company accountable for the use of data
- Understand the limitations of the data

The second part of this series seeks to demonstrate how companies can use the Framework to ethically monitor behaviors, target individual users, and use geo-locations to target buyers while ensuring that consumers or individuals are not discriminated.

BUILDING A CULTURE WHERE DATA IS AN ASSET, NOT A LIABILITY

Data can be a company's greatest asset or biggest liability. Organizational planning often relies on big data to uncover, identify, and capitalize on trends and user behaviors. The ability to utilize employee, customer, and competitive electronic browsing and purchasing history enables businesses to become more competitive and to target select customers and geographies while increasing customer touchpoints. Data analytics has a proven value regarding market penetration, quality and delivery of goods and services, and customer satisfaction. Different market segments such as finance, retail, and healthcare may have different uses for the output of data analytics. However, the ability to glean specific information and utilize those results in a way that benefits the customer experience while supporting growth has become a cornerstone of enhanced decision making based on in-depth business intelligence, regardless of industry.

With the growth of big data there is a need for increased oversight and management of the data collection, storage, use, transfer, and destruction processes. Forthcoming and existing privacy regulations such as the E.U. General Data Protection Regulation (GDPR), CCPA, and other international and U.S. state regulations outline requirements for data management practices. Some key principles these regulations address include providing clear and transparent notice, collecting the minimum amount of data necessary, limiting the use of data for secondary purposes, and acquiring consent for data processing.

More important than any regulatory guidance is the ethical obligation each organization must instill in its employees to appropriately use big data. Driving this from a cultural perspective can help companies meet this obligation as they process, analyze, and utilize data to manage and grow their business.

Heightened awareness of how personal information is used and protected is top of mind due to the number of data breaches that have occurred over the last decade. It is no longer acceptable to leave data unprotected and without proper safeguards. Further, data privacy and security awareness and training is essential for an organization to ethically and responsibly handle personal, and potentially sensitive, information. The overall data privacy landscape, and more importantly the expectation of consumers and clients, is that each organization has a documented and implemented data governance program that includes proper consents, privacy notices, training, and data protection controls.

Established data privacy programs can co-exist with the need to perform data analytics while creating a culture of data protection. It is essential for organizations to understand how to do both without jeopardizing the trust of your employees, customers, and stakeholders. Below are guidelines to implement a data privacy program that considers the ethical use of data.

ETHICAL PRACTICES OF SHARING OR SELLING PERSONAL INFORMATION:

1. **Clearly define company's ability to share or sell personal information.**

   Prior to embarking on the sale or sharing of personal information, organizations should consider their ability to actually sell that data. New privacy laws vary from requiring explicit consent (i.e., opt-in), opt-out, or adequate notice before data is shared or sold. Each practice requires a specific analysis of requirements for opt-in, opt-out, or consent to be valid. For example, a clear and transparent notice should at least include:

   - What data is being collected (categories)
   - Where that data is being collected from (sources)
   - Why the data is being collected (purpose)
   - What types of third parties may receive the data (disclosure)
   - The specific data collected about the consumer (data elements).

   Defining and documenting projects that will result in the sharing or selling of data will allow an organization to analyze whether it can meet the minimum privacy requirements for the data subjects, consumers, or regions which will be affected. Additionally, it will allow for regulatory compliance analysis to occur. A best practice for documenting and analyzing project risk is through a Privacy Impact Assessment (PIA). The PIA should capture the benefits of the project while highlighting potential risks or negative consequences, such as inadequate security controls or bias results from automated processes when sharing data. Through the completion of a PIA an organization will be able to streamline data controls and management processes, better control risk and have a more thorough understanding of the data to be shared/sold, and the potential impacts to the organization in the event of an incident or breach.

2. **Develop a transparent method of sharing and selling personal information that holds the company accountable.**

   Organizations should develop standards, policies, and procedures that keep transparency and privacy requirements in mind to provide adequate guidance to employees developing new processes, products, or services that result in the selling or sharing of data with outside parties. To ensure your organization is accountable for protecting personal information, build accountability into employment agreements, training programs, awareness communications, and operating procedures.

   Additionally, ensure that data security, cybersecurity and other safeguards are considered prior to any data being shared or sold. For example, this can be accomplished by using encryption for data at rest and in transit, securing removable media, and implementing Data Loss Prevention solutions to limit the movement of data. Finally, create third party agreements that hold outside parties accountable through enforcement of IT audits, copies of audit and attestation (SOC2) reports, copies of penetration or vulnerability tests, or by establishing liability for the improper disclosure or use of information that you've sold or shared with them.

3. Use data proportionate to accomplish the project.

Best practices that help organizations to collect and process data that is necessary include: (1) data minimization; and, (2) purpose limitation. Data minimization is the practice by which an organization limits the collection of personal information to that data that is directly relevant and necessary to accomplish a specific purpose . Purpose limitation, on the other hand, requires two elements, (1) data must be collected for specific, explicit and legitimate purposes only (purpose specification); and, (2) data must not be further processed in a way that is incompatible with those purposes (compatible use) .

By limiting the amount of data that is collected or processed, organizations can reduce risk while enhancing public trust. Data elements that are not beneficial to the project but that are nonetheless shared and/or sold may result in an organization violating its own notice and/or privacy obligations.

Organizations must review their privacy notices and consents on a routine basis and should perform an analysis against the content of those documents when obtaining, managing, and sharing/selling data. Aligning data management practices with company policies, notices and consents is critical when properly managing data and keeping operational practices in line with stated data privacy practices. Deviations from stated policy and actual business practices may result in reputational and financial impacts and penalties including potential sanctions by government regulators that may prevent the business from engaging in certain data collection practices going forward.

Other methods that can assist an organization with ethically processing data include pseudonymization or anonymization. Pseudonymization replaces specific information that could identify an individual with artificial information (pseudonyms), while anonymization is the process of either encrypting or removing personal information, so individuals remain anonymous. It's an important distinction because pseudonymization can be completely restored to its original state whereas anonymization is irreversibly altered. Depending on the way the organization intends to use personal information it is important to determine whether pseudonymization or anonymization is appropriate. If data does not have to be tied to an individual, then the project should strongly consider using pseudonymization, but keep in mind that pseudonymization can be reversed so depending upon where data ends up it may not be a viable option. This has the added benefit of reducing risk, limiting potential discrimination, and may reduce the applicability of privacy laws and/or regulations.

Discriminatory practices, whether on purpose or inadvertent, can be enabled or exacerbated by data analytics practices. When collecting vast amounts of personal information it becomes possible to segment out specific groups of individuals and tailor marketing and other business practices towards identified subsets of those whom your company has obtained data. For example, you may run a targeted marketing campaign aimed at those individuals in a certain geographic area whose income is greater than a specific dollar amount. While this may seem to be a reasonable marketing tactic, there may be some bias or other interpretation that can be taken from the business practice that may negatively impact your organization. As such, it is important to account for not only the approach to data analytics usage, but also to be aware of how it is viewed and/or interpreted, and how through a properly established data management program your organization can account for potential discriminatory data management practices.

4. Limit the use of personal information for the purpose for which it was collected.

Data should not be used in a way that is different or out of line with its intended use described during the initial collection of data. Data may be limited in how it can be used if the notice provided at the time did not contemplate or provide adequate notice of the secondary use. If the use of the data is incompatible with the originally intended purpose, then the organization should revise its notice. The new notice should provide clear details on how the approach was designed and how the collected data is now being used.

Additionally, the organization may be required to seek new consent for existing data it has collected from consumers if that data is to be used in a way that was not addressed within the original consent. For example, if you have collected personal information for a specific purpose, i.e., customer order, billing or healthcare information, that data should be used for the purposes that have been stated within the notice or consent. It would be a violation of your operational policies and privacy regulations to collect such information and use it for purposes other than outlined in the notice and original consent. Regulations like GDPR prohibit the use of collected information for purposes other than those compatible with the original purpose of collection.

Data collection and analysis should never be used for predatory or other nefarious reasons. Organizations should remember that regulations such as GDPR and CCPA preclude organizations from targeting specific segments of the population or collecting certain types of data without explicit consent. Examples include collecting data on minors (children) and the sensitive/protected categories for secondary purposes. Data collection methods should be documented, reviewed, and approved by the appropriate individuals within organizations to ensure that violations are not occurring, and that the highest ethical data handling standards are being met.

CONCLUSION

It is possible for companies to ethically monitor behavior and target specific market segments utilizing the Data Ethics Framework by implementing a data privacy program that includes:

- A culture focused on data management and protection with top-down support
- Tailored and accurate privacy notices and consent forms
- Collection practices that align with the organization's data management policies
- Collecting only the data needed for specific purposes
- Properly training employees on data privacy obligations
- A complete understanding of why your organization is collecting data, where that data is stored, how it is managed/shared and ultimately deleted when no longer required to be kept for operational or regulatory purposes.

In this way Data Privacy can be a business enabler while protecting the public's trust in an organization.

CONTACT

CHRIS JURS
Director, Governance, Risk & Compliance Practice
212-515-2557
cjurs@bdo.com

ANDREW TOBEL
Manager, Governance, Risk & Compliance Practice
732-734-3032
atobel@bdo.com

SANGEET RAJAN
Managing Director, Governance, Risk & Compliance Practice
415-490-3001
srajan@bdo.com

KAREN SCHULER
Principal, Governance, Risk & Compliance Practice Co-Leader
301-354-2581
kschuler@bdo.com

GREG SCHU
Partner, Governance, Risk & Compliance Practice Co-Leader
612-367-3045
gschu@bdo.com