FRAUD AND EMERGING TECH

Data ethics and governance with COVID-19 considerations

By Robert Pérez
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Data ethics and governance</td>
<td>2</td>
</tr>
<tr>
<td>Key ethics principles</td>
<td>2</td>
</tr>
<tr>
<td>Governance considerations</td>
<td>2</td>
</tr>
<tr>
<td>Influence on fraud</td>
<td>3</td>
</tr>
<tr>
<td>Balancing fraud detection and privacy</td>
<td>3</td>
</tr>
<tr>
<td>COVID-19 disruptions</td>
<td>4</td>
</tr>
<tr>
<td>Civil liberties in a new context</td>
<td>4</td>
</tr>
<tr>
<td>Social distancing and contact tracing</td>
<td>4</td>
</tr>
<tr>
<td>Relief package fraud</td>
<td>4</td>
</tr>
<tr>
<td>Risks and key considerations</td>
<td>5</td>
</tr>
<tr>
<td>Strengthening privacy awareness</td>
<td>5</td>
</tr>
<tr>
<td>Resources</td>
<td>6</td>
</tr>
<tr>
<td>Data ethics and governance</td>
<td>6</td>
</tr>
</tbody>
</table>
INTRODUCTION

Technological advances designed to collect data more efficiently and effectively are driving extraordinary business innovation and disruption. The advent of the Internet of Things (IoT), artificial intelligence (AI), robotics process automation (RPA), and 5G technology make it possible to amass and use enormous amounts of data — and how those data are leveraged, shared, protected, and potentially misused is raising serious and urgent questions about data ethics and governance.

These issues have permeated our society at an alarming scale and can impact anyone from those who use a smartphone to the billions of users who rely on Google, Facebook, Amazon, and the like in their daily lives. Now, as a result of the COVID-19 pandemic, technology is being developed at an even faster pace with potentially broader implications. More than ever, companies must address complex privacy issues and limit potential biases in the collection and creation of data.

This post, part of an emerging technology series from the Anti-Fraud Collaboration, explores the implications of data ethics and governance in the fight against financial reporting fraud and within the context of the current COVID-19 crisis.
DATA ETHICS AND GOVERNANCE

New concepts in a rapidly changing field

Key ethics principles

The exponential growth in the quantity of data that can be collected has spawned a new area of study, data ethics, which is fundamentally different from information ethics. The latter, which has a well-established history and precedents, focuses on ethical considerations involving intellectual property (e.g., patents, trademarks, copyrights, and trade secrets). In contrast, data ethics examines concepts of right and wrong in relation to the collection and dissemination of both structured and unstructured data, particularly as these actions relate to personal information. Although the study of data ethics is relatively new, these key principles have emerged to help oversee data collection, usage, and governance:

- **Ownership.** Individuals own their personal data.
- **Transparency.** Individuals should have transparent access to the algorithm used to generate aggregate data sets if their personal data are used.
- **Consent.** Use of personal data requires informed and expressed consent related to how personal data are shared and with whom, when, and for what purpose.
- **Privacy.** All reasonable effort needs to be made to preserve privacy if data transactions occur.
- **Currency.** Individuals should be aware of financial transactions resulting from the use of their personal data and the scale of those transactions.
- **Openness.** Aggregate data sets should be freely available.

But even these basic principles are undergoing modifications in the current environment of constant data collection and manipulation. For example, privacy is a possessive concept for which personal information is consciously and intentionally shared, and the process is becoming more transactional and collective as more information is exchanged for access to services and online interactions. These changes and others are examined in Deloitte’s provocative article, Managing Data Ethics: A Process-Based Approach for CDOs, authored by Christopher Wilson.

Governance considerations

An integral part of any discussion about data ethics must include how data, once collected by data brokers, are governed. Important data governance considerations include how data are used, stored, disposed of, and protected. In an era of relentless cyberattacks — during which the risk and frequency has been further elevated due to the COVID-19 crisis — protection of private information is critical.
INFLUENCE ON FRAUD
Role of data ethics and governance

Balancing fraud detection and privacy

**Accessibility to data** — and the technology to examine data continually — can greatly enhance fraud detection and deterrence efforts. Indeed, organizations that implement proactive data monitoring detect frauds 33% faster and experience losses that are 33% lower than organizations that do not, according to the Association of Certified Fraud Examiner’s (ACFE) 2020 Report to the Nations.

Discussions about ethical use and governance of data must evolve into how fraud investigation and information monitoring should be weighed against protecting personal data. In addition, fraud investigators should consider the privacy implications and guarantees associated with data they use in their investigations.

For example, fraud investigations often include digging into the personal backgrounds of suspected fraudsters, which some investigators describe as following digital footprints to uncover the truth. New data privacy regulations such as the European Union’s Global Data Protection Regulation and the California Consumer Privacy Act could limit access to such important data. These regulations, and a slew of others around the world, are not designed to make it harder to detect fraud; however, they are designed to protect fundamental privacy rights.

The traditional concepts of protecting data embraced by fraud investigators are most clearly articulated in Article Six of the ACFE Code of Professional Ethics: “An ACFE Member shall not reveal any confidential information obtained during a professional engagement without proper authorization.”

But discussions about data ethics turn that concept on its head. What are the ethical implications of using fraud investigation techniques to get around or “break” anonymized data sets? The well-established *mosaic effect* — the practice of bringing together disparate data sets to glean new insights — can be used to discover individuals or their actions from anonymized data sets. Such ethical conundrums should be discussed when organizations establish protocols and policies on the use of RPA and AI to monitor data sets.
COVID-19 DISRUPTIONS

Data governance considerations related to COVID-19

Civil liberties in a new context

The COVID-19 pandemic is creating once-in-a-lifetime economic and social disruptions that are manifesting themselves in myriad ways. The data ethics and governance dynamics are just as varied.

For example, limitations on certain civil liberties have been installed for the greater good. They include aspects from the private sector, where mandatory telecommuting is now the norm, to the public sector, where governments are imposing social distancing rules, curfews, and prohibitions on public gatherings.

Social distancing and contact tracing

Efforts to enforce isolation rubrics raise additional data ethics and governance questions. For example, in Bellevue, Washington, residents were encouraged to report violations of the state’s stay-at-home orders, which are tracked in the myBellevue app. This application identifies hotspots where gatherings have been reported.

Nationally, support is growing for assembling and analyzing data on collective movements to test the effectiveness of social distancing. For example, private companies such as Google or Facebook could turn over location information to government agencies. However, it is highly unlikely that pandemic scenarios were considered in standard information-sharing agreements.

As another example, Google and Apple have recently teamed up to develop a COVID-19 contact-tracing application that informs smartphone users whether they have been in contact with someone who has tested positive for the virus. Such data sharing is not a new practice — medical researchers have used data from cell phones pinging nearby towers to predict the spread of malaria in Kenya — but such efforts should consider ethical implications of consent as well as how the data are aggregated and anonymized.

Relief package fraud

The recently approved $2.2 trillion US CARES Act is just one of dozens of COVID-19-related monetary relief packages approved worldwide. How that money ultimately is disbursed — and the related collection of data to manage such a monumental undertaking — also has data ethics and governance implications. The urgency to get relief into the hands of individuals and businesses creates significant opportunities for financial fraud.
RISKS AND KEY CONSIDERATIONS
Data monitoring and analysis

Strengthening privacy awareness

Proactive data monitoring and analysis are among the most common anti-fraud controls, according to the ACFE’s 2020 Report to the Nations. Data ethics and governance clearly affect the ethical use of data by fraud examiners, internal auditors, and financial professionals, but these measures do not have to pose a significant risk as long as those conducting an investigation are aware of privacy issues and the limitations and potential biases in data sets.

The previously cited Deloitte article by Christopher Wilson offers a list of potential vulnerabilities and questions about data collection by public agencies. It also provides a solid foundation for fraud examiners, internal auditors, and financial professionals to consider when evaluating data sets in their investigations:

- **Project planning and design.** How were various aspects of the data collected? Was the right amount collected? In the case of a breach, what data protection strategies and controls were deployed?

- **Data collection and consent.** Who owns the data, and who should give permissions and consent? Do any methodological issues affect the reliability of the data? How can consent be obtained for alternate use of the same data?

- **Data analysis.** Do the data have any biases or gaps? Does other information exist that would contradict the data or the conclusions drawn?

- **Data maintenance.** Does the level of data security match the potential threats to the data?

- **Data sharing and publication.** Do the data contain sensitive information? Are there explicit ethical standards in data-sharing agreements?

- **Data use, reuse, and destruction.** Are there any ethical issues in connection with how the data were originally collected? Has the context changed since then in a way that requires regaining consent of data subjects? Are there data ownership or licensing issues to be considered?

The overwhelming use of data has challenged many organizations’ approaches to their data lifecycle management and safeguard protocols. While balancing today’s ever-increasing need for more data creation, collection, and sharing, companies should double down on their data ethics and governance practices to balance society’s fast-paced needs and ethical foundations.
RESOURCES

Data ethics and governance

- Deloitte: Data Governance for Next-Generation Platforms
- Deloitte: Managing Data Ethics: A Process-Based Approach for CDOs
- Deloitte: Treat Your Data Like the Superpower That It Is: Making the Case for Data Governance
- EY: 10 Things You Need to Know about Rich Data and Reporting
- EY: How Do You Teach AI the Value of Trust?
- EY: Is Your Algorithm an Ethical One?
- FEI: Data Governance: The New Frontier for the Board
- FEI: Financial Executives are Going All in on Data
- The IIA: Data Ethics, Where Does Internal Audit Fit?
- KPMG: Data Governance: Driving Value in Healthcare
- KPMG: Ethical Use of Customer Data in a Digital Economy
- KPMG: Guardians of Trust: Who is Responsible for Trusted Analytics in a Digital Age?
- NACD: NACD Director's Handbook on Cyber-Risk Oversight
- NACD: Risk Changes the Data Governance Game
- NACD: Why Data Governance Should Be Part of Your Boardroom Conversations
- PwC: Consumers Trust Your Tech Even Less than You Think
- PwC: Data Trust Pacesetters Show How to Create and Protect Value from Data
- PwC: Data-Use Governance: Monetizing Data While Respecting Privacy

The founding organizations of the Anti-Fraud Collaboration are developing a wide range of resources to help members of the financial reporting supply chain respond to COVID-19. Learn more at our resource centers:

- CAQ: COVID-19 Resource Collection
- FEI: COVID-19 Dashboard
- The IIA: COVID-19 Resources Exchange
- NACD: COVID-19 Resource Center
About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession’s most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association’s global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

Copyright © 2020 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact copyright@theiia.org.

May 2020