COSMOS
Navigate the Compliance Universe

ethikos Volume 33, Number 9. September 01, 2019
How can compliance support an ethical framework for artificial intelligence (AI)?

By Patrick Wellens, CFE, CIA, CCEP-I, CRMA

Patrick Wellens (patrickwellens@hotmail.com) is currently working as a Global Compliance Business Partner for one of the divisions of a multinational pharma company in Zurich, Switzerland.

In the digital age, more and more companies are using artificial intelligence (AI) to look for new business opportunities, get better insight into data, automate repetitive processes, and/or reduce costs. By looking at some real-life scenarios, such as the use of facial recognition in military technology and using AI in recruitment processes, autonomous vehicles, and the Microsoft chatbot "Tay," it becomes clear that apart from the many benefits of the new technologies, there are also some challenges. In this article, I will briefly mention the principles of an ethical framework for AI and focus on how ethics and compliance (E&C) departments can contribute to the creation and implementation of such ethical standards at their companies.

Ethical principles in the development and delivery of AI

Throughout last year, several institutions (e.g., the World Economic Forum, Partnership on AI, a high-level expert group on AI set by the European Commission[1]) and several countries (e.g., the Personal Data Protection Commission in Singapore, Commonwealth Scientific and Research Organization in Australia, and the United Kingdom House of Lords Select Committee on Artificial Intelligence) have created an ethical framework for the development and delivery of AI.

A number of principles were defined specifically:

- **Generates net-benefits**: The AI system must generate benefits for people that are greater than the costs;
- **Human oversight:** In situations where the risk that fundamental rights will be ultimately affected, a fundamental rights impact assessment should take place. Human oversight helps ensure that AI does not undermine human autonomy or cause adverse effects;
- **Technical robustness and safety**: AI should be protected against vulnerabilities that can allow it to be exploited by adversaries (i.e., hacking) and should have a recovery plan in case of incidents;
- **Privacy and data governance**: AI systems must guarantee privacy/data protection through the entire life cycle. Given that the quality and integrity of data is paramount for the performance of AI systems, data protocols (e.g., who can access what data under what circumstances) should exist and be maintained;
- **Accountability**: People and organizations responsible for the creation and implementation of AI algorithms should be identifiable and accountable for the effects of that algorithm, even if adverse impacts are unintended;
- **Non-discrimination and fairness**: In order to build trustworthy AI systems, they should be designed to minimize—and even better, to eliminate—social bias by consulting all stakeholders who may be directly/indirectly affected by the AI system; and

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

- **Transparency:** To allow for traceability and to increase transparency in all data sets, AI system decisions should be documented and easily explainable to various stakeholders (e.g., layperson, researchers, and/or regulators). Furthermore, AI systems must be identifiable and should not represent themselves as humans to users.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.