

Is your algorithm an ethical one?

The opportunities created by artificial intelligence require responsive and responsible leadership.

#Forensics #ForensicDataAnalytics #AI
ey.com/forensics

Of special interest to:

Legal counsel
Corporate security officers
Information security executives
Compliance executives
Risk management executives
Internal audit

■ ■ ■
The better the question. The better the answer.
The better the world works.

The EY logo consists of the letters 'EY' in a bold, white, sans-serif font. The 'E' and 'Y' are connected at the top. A yellow triangle is positioned above the 'Y'.

Building a better
working world

Introduction

Artificial intelligence (AI) has come to occupy center stage in the world of business: it is at the heart of digital transformation and business management.

In compliance management, AI has become the new front line of a company's ability to defend itself from external and internal threats. As such, it should be a central pillar in a company's risk management strategy.

AI is shaking compliance to the core. New methodologies to manage data, new ethical and moral questions far beyond the traditional scope of compliance, and new people to manage the issues and technologies – such is the impact of AI.

With the advent of AI as the new building block of a company's data architecture, companies will need to develop new processes to continue to innovate and drive their commercial leadership, while at the same time managing the evolving ethical and legal risks – risks which, if left ignored or unmanaged, can have a debilitating effect on a company's reputation and operational efficiency.

In this paper, we explore the "ethics of the algorithm" – some of the compliance risks that companies need to consider as they deepen their dive into digital transformation.

The dilemmas of data

At the root of AI is data. Data is a commodity that can be bought, sold, rented, hired, borrowed, stolen and disposed of. Never has the ownership of data been more valuable or more complex than now.

It is a truism of the age of information technology that the outputs of a computer program or IT process are only as good as the original inputs – at some point created by a human mind. To a certain extent, the life cycle of AI is similar. The quality of data outputs will reflect the quality of the data inputs. For example, if there is bias inherent in a programmer's mind when creating the algorithm that processes the data, that bias will be reflected in the final outputs – sometimes with devastating consequences.

The quantitative shift produced by the processing of larger volumes of data at ever faster speeds is fusing with a qualitative change: AI can discover new patterns that could never be visible to the human mind, and potentially missed even by relatively recent technological advances, such as data analytics.

Any use of data raises a multitude of questions: who owns the data, hosts it, collects it, "harvests" it and benefits from it? How can it be safely stored, exchanged, transferred and disposed of? To whom does data really belong and how is ownership transferred among stakeholders? Using AI can make these questions even more complex.

Furthermore, companies at the forefront of the AI revolution are operating in uncharted territory where the rules of the game are at best vague, and at worst nonexistent. And, the regulators are desperately trying to play "catch up." With knowledge concentrated in the hands of a small number of "high authorities" of technology, undisciplined AI – unconscious intelligence, one might call it – is a recipe for errors of judgment that can undermine and even destroy a company's reputation and brand.



The ethics of the algorithm

At the root of AI is the algorithm — the building block of information technology systems. Algorithms are nothing new to technology.

Recent examples of how companies have broken the law or had reputational setbacks due to loss of control of AI processes:

- ▶ In 2018, Cambridge Analytica was shown to have used data improperly obtained from Facebook to build voter profiles ([The New York Times, April 2018](#)).
- ▶ In the same year, Facebook also underwent a number of data security lapses and bugs, which allowed personal data to be made public without users' consent ([How 2018 became Facebook's worst year in privacy and security, January 2019](#)).
- ▶ In 2018, Reuters reported that Amazon had scrapped its AI-based recruitment tool because it discriminated against women. Other companies confirmed the limitations of AI technology in the human resources application ([Reuters, October 2018](#)).

Also available online:

- ▶ Uber: Self-drive disaster <https://www.nts.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf>
- ▶ World Cup 2018 AI Predictions – All Wrong <https://medium.com/futuristone/artificial-intelligence-failed-in-world-cup-2018-6af10602206a>

Merriam-Webster defines the algorithm as “a procedure for solving a mathematical problem in a finite number of steps that frequently involves repetition of an operation.” They have, after all, always been present in IT and have existed longer than IT has.

The algorithm contains data or data sets and various instructions that produce a result. This, in turn, can be used as an input into another algorithm. AI is usually made up of strings of algorithms.

With computing power, sophistication and speeds reaching new heights, algorithms are capable of replicating human decision-making in a fraction of a second. If the observed human behaviors that dictate how an algorithm transforms input into output are flawed, it risks setting in motion processes in which outcomes may not be the ones we intended. With algorithms even able to create their own algorithms through “self-learning,” the risk of unforeseen and potentially harmful outcomes increases exponentially.

Algorithms aggregate, transfer, analyze, transform, share and create data, often without the controls, due diligence and attention to its origins and its destination that would habitually be applied to proprietary information stored or shared in more traditional forms. Whether through human error, bias, faulty design, poor-quality data

or malicious intent, the impact of getting an algorithm wrong and losing control of data can have a damaging effect on a company, on society and on social attitudes toward business and technology.

Traditionally, corporate executives made decisions based on data filtered through a familiar, and relatively transparent, hierarchy of expertise, intellectual exchange and debate. In tomorrow's company, the origin of the data and the assumptions underlying it, the scrutiny which it has undergone and how it has informed the top decision-makers are now concealed within the algorithm.

Constant, high-profile media coverage about improper use or misuse of data collected by companies is now the norm. Personal or proprietary data is passed to third parties, deliberately or by accident. There are hacks, leaks and security breaches. Sometimes these are for profit; on other occasions they are the fault of poor data security or sheer incompetence. Decisions come to light that display racial or gender bias. Data integrity, that fundamental underpinning of management integrity, seems to be uncontrollable.

The cost of ethical blindness

Companies (not only the technology companies that have produced the new technologies, but any company that uses them) are under scrutiny about how they manage their data.

Now the tough questions are being asked. How do companies manage data for their own benefit and growth while respecting individuals' fundamental civil rights to privacy or "to be forgotten"? How can they respect other companies' intellectual and data property? Will they

self-regulate? And if they will not, how can they be constrained? Governments everywhere are gearing up for a new wave of regulations, the likes of which we have not seen since the last financial crisis.

Here are several examples of legislation and regulations designed to control the use of data and safeguard its ethical use.

- ▶ [The General Data Protection Regulation \(GDPR\)](#) came into force in 2018 and regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU, and is a watershed in data privacy.
- ▶ The [California Consumer Privacy Act \(CCPA\)](#) passed into law in 2018 and comes into force on 1 January 2020. It represents one of the most sweeping acts of legislation enacted by a US state to bolster consumer privacy. The CCPA gives consumers the right to request access to and delete their personal information that a business has stored. They also have the right to opt out of a business selling their information.
- ▶ [New York State Department of Financial Services \(NYDFS\) Cybersecurity Resource Center](#) expands the definition of nonpublic information to all information, even if not personally identifiable, or financial information that "could cause a material adverse impact."
- ▶ Other countries have seen major developments in the implementation and enforcement of privacy and data security laws, such as Australia's Privacy Act, Japan's Personal Information Protection Act and China's Cybersecurity Law.
- ▶ The [UK government's Digital Charter](#), first published in 2018 and updated in April 2019, is a program to agree norms and rules for the online world and put them into practice, including the updating of laws and regulations.

For companies, these are challenges of a completely new order. New laws and guidelines that touch upon different aspects of data integrity are coming out at the regional, national and international levels faster than most companies can adjust. And, an increasing list of prosecutions or settlements show that this is no passing fad. As a result, a sharp-eyed focus on

legal compliance is the bare minimum investment a company should make.

But the bigger issues are that the law is often not clear, and the public is pushing for companies to have greater accountability to society. In the twilight zone, where the law is unclear, contradictory or even nonexistent, companies have to get

ahead of the curve to manage data responsibly. Negligence or ignorance may be punishable by law; ethical blindness will be punishable in the court of public opinion. The fallout from a case of ethical blindness can be just as damaging as a high-profile lawsuit in terms of brand and reputation damage, if not legal costs.

In conclusion

How can companies take more ownership and responsibility for their data? How can they make sure that the algorithms that underlie the myriad processes that go into a business decision are under control? How can they be certain that there is human oversight over the system? How can they protect themselves from AI risk?

First, companies need to make sure that they are legally protected. The legal framework in which companies operate may be in flux, but companies can still structure their contractual relationships so that employees, clients and third-party business partners are all “signed up” to safeguard information that is proprietary or subject to privacy rules.

For example, companies need to have well-defined contractual requirements governing the use of data by third parties. They also need to gain transparency into how third parties access, use and store data, as well as their internal control measures, to minimize the risks of data breach and noncompliance. In this, major companies play a quasi-regulatory role in their supply chains.

Second, the data management, information tracking and security systems need to be highly sophisticated. Algorithm monitoring and auditing systems and advanced data analytics are required to understand where a unit of data is coming from, where it is going and how it will be processed between these two points. In the past, functions such as internal audit would have been sufficient to analyze data and to track financial flows and monitor internal

controls. Today, when there is so much data being processed at such speeds, AI needs to be devised and developed to audit and monitor AI already in use.

Third, companies need to invest in human resources. All employees, and especially company leadership, need to be aware of how AI affects both the business and stakeholders. IT processes traditionally have been within the remit of the CIO and the IT team. Today, it is necessary for all employees to be aware of how AI will affect their part of the business, and to understand the legal and reputational consequence of failure to understand the risks of AI. No longer should the IT function be the domain of a small group of highly specialized professionals.

Furthermore, the traditional silos in companies need to be broken up. In the future, individual managers will need to be multifunctional, equally at ease with key elements of the Legal function and the IT function. Cross-pollination of ideas across functions and throughout the whole company is the best way for companies to manage AI risk and take advantage of AI opportunities. We can forecast a transformation in compliance departments as data compliance is replaced by ethical values at all levels of the company.

Above all, humans need to supervise and control the process. In the age of AI, this is a big ask of a company's senior executives, but this is what is required and demanded of them. The ambition to succeed in managing AI will be achieved only by companies' ambition to recruit the caliber of team to make this happen.

Fourth, companies need to open themselves up to influences in the market. Companies are not islands. In an area of human endeavor that is so new and has such broad social repercussions, no single company will get it right on its own. Companies will find strategies in dialogue with others. There are a number of interesting platforms (see page 7 on right) in which these issues are being actively discussed from the point of view of business and society. By pooling resources and brain power, companies are likely to find technological and managerial applications faster and more efficiently.

Multi-stakeholder platforms discussing ethics and technology.

There has been an escalation of platforms and organizations set up to address the ethical challenges inherent in rapid technological developments, including AI. The following is just a sample:

- ▶ [AI Now Institute](#) is a research institute at New York University that examines the social implications of artificial intelligence.
- ▶ The [Algorithmic Justice League](#) is an advocacy group whose mission is to highlight algorithmic bias and develop practices for accountability during the design, development and deployment of coded systems.
- ▶ The [Center for Technology Innovation](#) at the Brookings Institution focuses on delivering research that affects public debate and policymaking in the arena of technology innovation.
- ▶ [The Centre for Data Ethics](#) is a UK government initiative to connect policymakers, industry, civil society and the public to develop the right governance regime for data-driven technologies.
- ▶ The [EU High-Level Expert Group on Artificial Intelligence](#) supports the implementation of the European Strategy on Artificial Intelligence, including the elaboration of recommendations on ethical, legal and societal issues related to AI.
- ▶ The [Partnership on AI](#) advances the understanding of AI technologies, including machine perception, learning and automated reasoning for the benefit of people and society.

Author



Todd Marlin

Global and Americas Forensic
Technology & Innovation Leader,
Ernst & Young LLP



The views reflected in this article are those of the author and do not necessarily reflect the views of the global EY organization or its member firms.

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

© 2019 EYGM Limited.
All Rights Reserved.

EYG no. 004912-19Gb1
WR #1910-3285942
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

