EY
Building a better
working world

Why is the best digital strategy a human one?

We discuss how human ethics and machine logic can help drive the integrity agenda in the Technology, Media & Entertainment and Telecommunications sector.

#Forensic&IntegrityServices #TMT

ey.com/forensics

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

Introduction

Digital transformation is recognized as both a strategic opportunity and an emerging business risk.

New technologies and technology-enabled business models are evolving at a rapid pace as companies are finding new ways to collaborate, work and compete in the market with innovative solutions, increasingly transforming and disrupting the economy. Digital transformation has engendered new products, services and solutions – faster, and with more impact on the economy and society than ever before.

But the risks are also rising. 2018 was a watershed year as companies were accused – rightly or wrongly – of a wide range of misdemeanors, predominantly involving the use of data. As a result, employees demonstrated or resigned, investors put their investees on notice, and senior executives were invited to testify to congress and other legislative or regulatory authorities. Companies' approach to business culture, work environment, ethics and risk was subjected to detailed scrutiny by society.

While the challenges of digital transformation affect all industries, at the center of disruption is technology and data-led companies. With
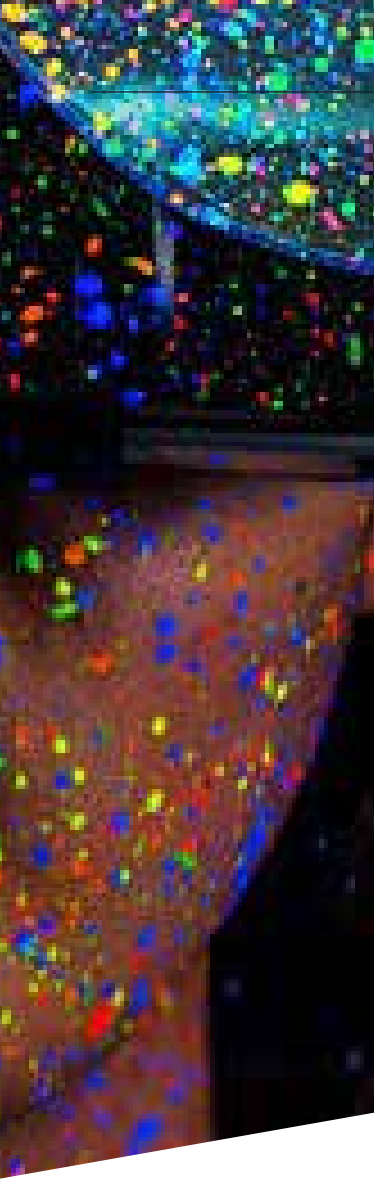
mobile phones, social networks and media, and exponentially increasing processing power, companies of the Technology, Media & Entertainment, Technology (TMT) sector are poised to introduce artificial intelligence (AI) and advanced technology solutions to all walks of life.

With the advent of AI, public concern at the prospect of organizations' compromising the security of personal data has reached a new level. As reported by the *Financial Times*, influential commentators such as George Soros are predicting "a web of totalitarian control the likes of which not even Aldous Huxley or George Orwell could have imagined".[1] It makes for a challenging regulatory and operating environment for the industry.

"TMT organizations play a special role in taking responsibility and managing the new ethical challenges facing companies, industry and society in the era of AI and technology-enabled business models," says Andreas Pyrcek, Partner and Global TMT Sector Leader, EY Forensic & Integrity Services. We look at the risks for the industry and how it can contribute constructively toward the development of a new digital agenda which balances innovation and responsibility, opportunity and risk, and entrepreneurship and restraint.

The importance of the TMT sector in a digital age

The TMT sector comprises a broad community of companies, most of which have either a direct or indirect relationship with end-consumers, often enabled by technical, analytical,

AI-driven or supplemented interfaces. Examples include telecommunication companies managing millions of consumer phone contracts, media and entertainment companies providing consumers with digitally provided media content, and technology companies selling goods and services directly to consumers — often replacing elements in the value chain, such as retail stores.

TMT companies have increasingly supplied their technical achievements to other sectors. Prominent examples include driverless cars for the automotive industry, hospitality and transportation platforms, surgical robotics and data analysis in pharmaceutical R&D in health care, and facial recognition technologies for government enforcement agencies. Indeed, the TMT sector is converging with many other industries.

What all companies in the sector have in common is a track record of unprecedented innovation and growth, enabling them to attract and retain some of the best scientific and engineering minds in the world. They also have succeeded in creating a strong financial and asset base for R&D; the ability to create and access the world's most advanced technology infrastructures; and to collect, analyze and monetize a vast proportion of private and public data. In short, the TMT sector is driving the technological revolution that the world is undergoing, and is playing a fundamental and significant role in shaping business and society in the years to come.

"

TMT organizations play a special role in taking responsibility and managing the new ethical challenges facing companies, industry and society in the era of AI- and technology-enabled business models.

Andreas Pyrcek

Partner, Ernst & Young GmbH, EY Global TMT Sector Leader, Forensic & Integrity Services

---

[1] "George Soros takes aim at 'mafia states' and social media," *Financial Times*, ft.com/content/b4717b08-021a-11e8-9650-9c0ad2d7c5b5.

Digital dilemmas of Globalization 4.0

Any revolution of this scale will inevitably pose challenges to society. Previous technological revolutions, such as the advent of the steam engine, new sources of energy, innovative methods of transport and scientific developments, led to significant economic growth, wealth and disruptive social forces in equal measure.

The Fourth Industrial Revolution, or "Globalization 4.0" as the World Economic Forum has called it,[2] which we are living through now and which is being driven by the TMT sector, is no exception. Along with reducing poverty in the developing world and making public and private services and communications accessible to a mass global audience, the digital revolution has raised a multitude of questions regarding employment, equitable distribution of wealth, citizens' rights, accountability, fairness, transparency, privacy and safety. These matters are often raised by impacted customers, providers, regulators and the public at large.

Just as in previous industrial revolutions, controversy has never been too far from the industry which leads with the introduction of the new disruptive technologies: the displacement of the high street by e-commerce, the automation of manufacturing industries and consequent laying-off of the blue-collar labor force in advanced economies, and transfer of customer service and the new tech centers to low-cost countries. Among the negative side-effects of what was generally an extraordinary story of global growth include social

upheaval, unemployment, indebtedness and income differentials. It could not all be laid at the foot of the TMT sector — each application of the technology had its social consequences in its respective sector — but the technology was always at the forefront of the changes.

The abuse and misuse of data

What distinguishes the TMT sector is the fact that it operates in a regulatory vacuum. The technological development, and therefore, the social disruption are taking place at such a breakneck speed, that governments are sometimes struggling to keep up.

One of the direct consequences of this, and companies' increasing dependence on data, is the rapid rise of cybercrime. Data theft, identity theft, hacking, malware and viruses have all become commonplace and is one of the biggest perceived risks for modern-day business. In the EY *Global Fraud Survey 2018*, 51% of respondents from the industry placed cyber attack as the greatest risk to their business, equal to the macroeconomic environment.[2]

The World Economic Forum's *Global Risk Report 2019* concurs: cyber attacks, data fraud or theft, and critical information infrastructure breakdown are all listed among the top adverse consequences of technological advances.[3]

For all its technological prowess, the industry is being challenged to protect itself and its dependents — governments, companies and other organizations across the world — to defend themselves from the new criminals. If governments remain one

step behind in terms of regulation, the criminals will be one step ahead, in terms of cybercrime. It has not all been bad news — without the revelations of WikiLeaks, the Panama Papers and the Paradise Papers, much corruption would remain firmly under wraps. However, the digital economy has enabled a whole new class of crime which is not so easy to control.

[2] EY Global Fraud Survey 2018.

[3] "The Global Risks Report 2019," *World Economic Forum*, weforum.org/reports/the-global-risks-report-2019/.

51%
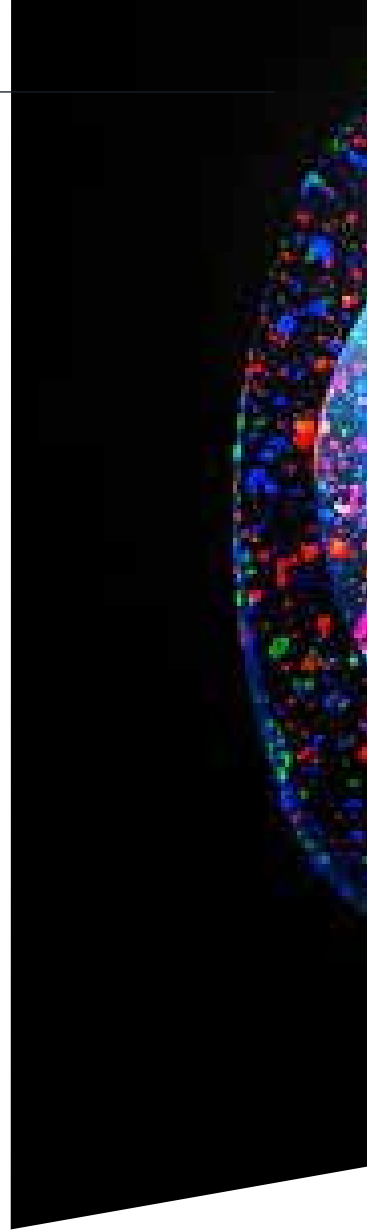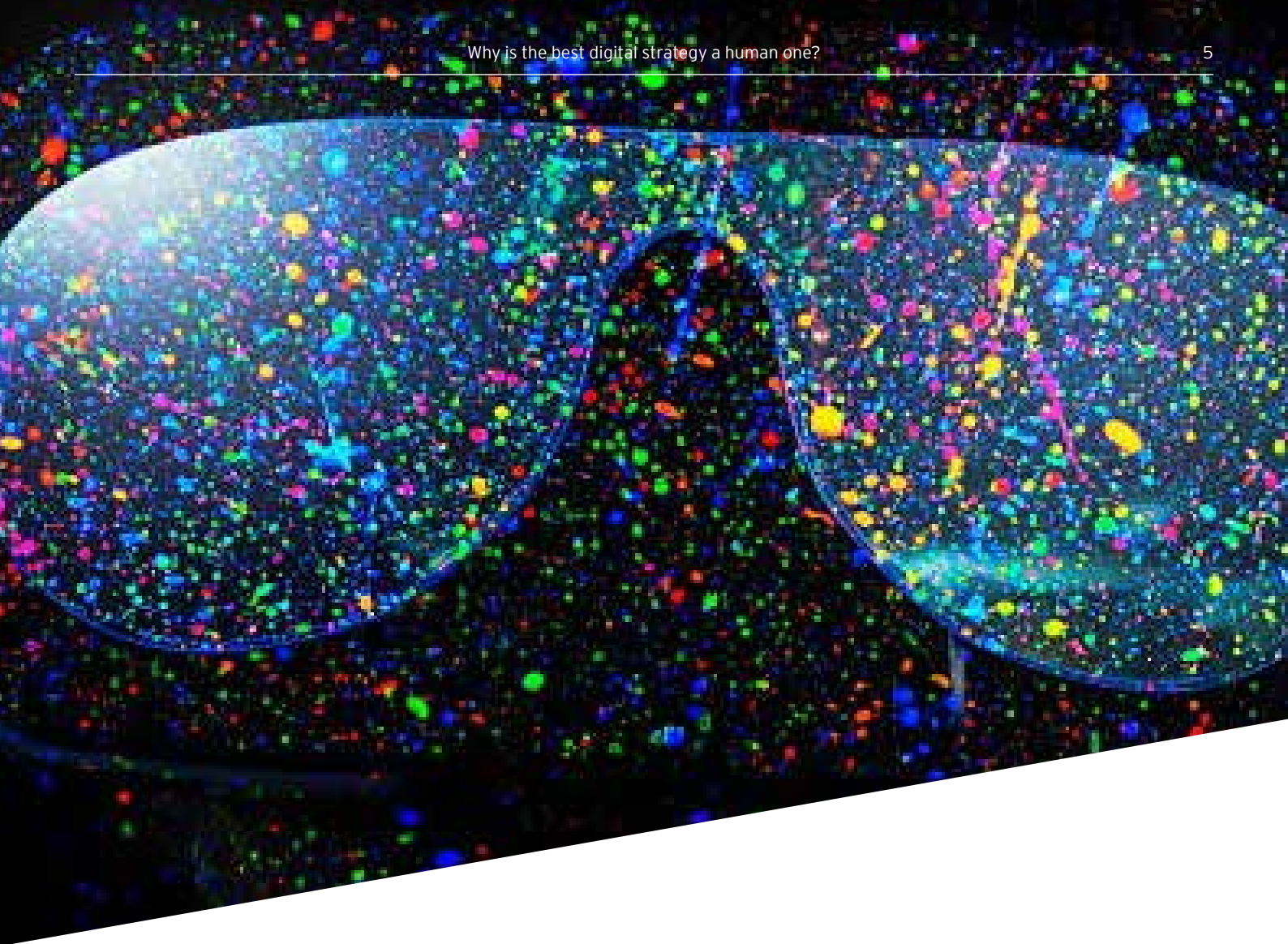
of respondents from the industry placed cyber attack as the greatest risk to their business, equal to the macroeconomic environment

In fact, 2018 saw the beginnings of a more robust approach to data regulation on the part of governments. In 2019, the first technology giants were hit with a record fine for breaching the EU's General Data Protection Regulation (GDPR). The €50 million fine issued by French regulator Commission nationale de l'informatique et des libertés (CNIL) was triggered by complaints relating to how technology firms handled people's data. And in 2018, an investigation was started into Cambridge Analytica, which used the data collected from social media about users' preferences and tastes to trace psychological patterns and target the users with personalized advertising.

For all the benefits it has brought to society, the digital economy raises serious and unresolved questions about the security and safeguarding of personal information, sensitive and secret data, and intellectual property. We are in an age where the line between private and public property has become blurred.

AI – the new ethical challenge

> "
>
> Compliance organizations have always been great in managing external regulatory risks — but understanding, preventing and responding to the emerging risks of the digital transformation is a rapidly growing challenge that requires a complete new approach and skill set.

Andreas Pyrcek
Partner, Ernst & Young GmbH and
EY Global TMT Sector Leader,
Forensic & Integrity Services

AI investment has been increasing exponentially. According to IDC, AI spending will grow to US$52.2 billion in 2021 and achieve a compound annual growth rate (CAGR) of 46.2% over the 2016-21 forecast period.[4] The recent introduction of AI poses exceptional opportunities – but also new risks to business and society, and especially to the companies in the TMT sector which are at the forefront of this new technological development.

At the root of public concern is the perception that there are limits to the ability of machines to resolve problems of fairness, bias and discrimination. For example, there are real and great opportunities in leveraging AI – but also perceived dangers and anticipated risks in algorithms that are created with no control, awareness or an ethical framework in place

Bias arises because of attitudes among humans. But what happens if the bias is created by the new generation of "intelligent machines"? Can robots make ethical judgements? Can they empathize? Can they feel what is right and wrong? Can AI have human-like or emotional intelligence? In short, and most importantly for the industry, should AI be allowed to operate without emotional intelligence?

Bias affects many walks of life, especially where humans and machines converge. In recent years, specific applications of AI have raised the issues of racial bias in algorithms. Relatively harmless applications, such as the use of bots for customer service can be managed by a human supervisor who can "intervene" when things go wrong. Tracking and matching movement of people, their email and voice communications, and other private activities can potentially constitute an infringement of people's rights. And experiments with autonomous vehicles have raised questions of safety and ethical judgement in leaving such complex operations as driving to a machine.

Fundamental questions have arisen on the impact of social media on society, especially, vulnerable groups like children. The uncontrolled and inestimable impact of addiction to social media and mobile phones, and the presence of harmful or dangerous content has become a major concern. Underlying these info-culture debates is an implicit criticism of the role of algorithms supporting a business model which regards facetime and click-through rates as essential components of advertising revenues.
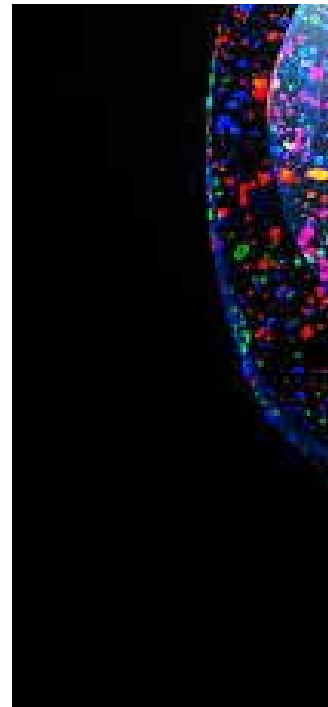
[4] "Worldwide Spending on Cognitive and Artificial Intelligence Systems Will Grow to $19.1 Billion in 2018, According to New IDC Spending Guide," *IDC*, idc.com/getdoc.jsp?containerId=prUS43662418.
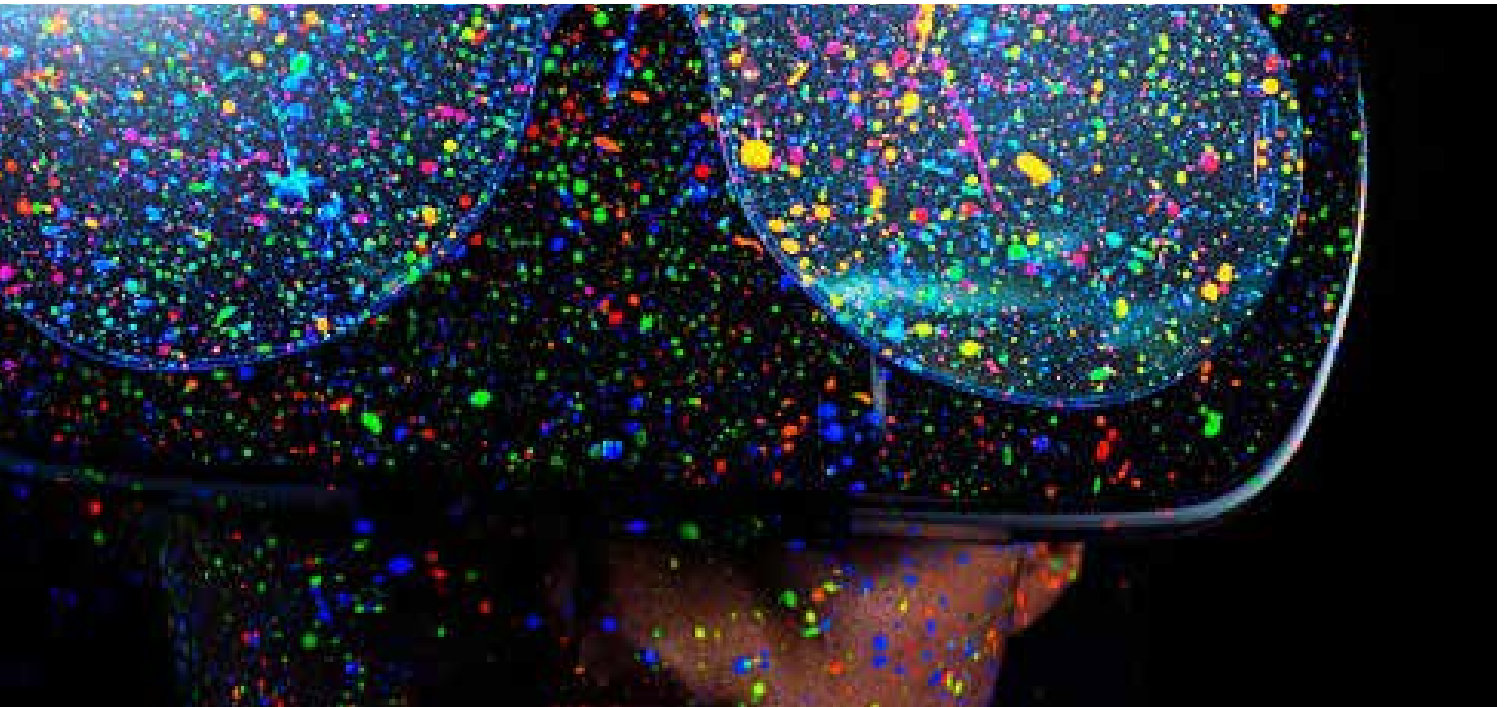
The concerns will grow even greater in the new generation of immersive technologies which are about to reach the consumer. For example, what are the design option and algorithms that are modeled for virtual reality (VR) and augmented reality (AR)? New ethical challenges arise from issues of access, privacy and consent. There's also the issue of virtual crimes, social desensitization and in-game trauma.[5] The use of AI to create realistic – but entirely fictitious – videos bring the threat of fake news and its existing unethical impact on society to a whole new level.

The biggest concern to have emerged in the last year is the use of AI in surveillance and tracking applications, especially when these are used by governments in a non-transparent way. The examples include use of AI-enabled technologies for immigrant screening purposes.[6]

The reaction from society, the markets and indeed from within the industry has been significant. As reported in the *New York Times*, one company's investors became active in their determination to prevent facial recognition technology from being abused. According to them: "such government surveillance infrastructure technology may not only pose a privacy threat to customers and other stakeholders across the country, but may also raise substantial risks for our company, negatively impacting our company's stock valuation and increasing financial risk for shareholders."[7]

There are more AI developments to come. The AI Now Institute, a research institute dedicated to understanding the social implications of AI, points to affect recognition and automated decision systems (ADS).

Affect recognition is a subset of facial recognition, which aims to interpret faces to automatically detect inner emotional states or even hidden intentions. And, ADS can seek to aid or replace various decision-making processes and policy determinations across government domains, including criminal justice, child welfare, education and immigration.[8] Largescale quantum computing may render obsolete the tools that form the basis of current digital cryptography, further opening secret or proprietary information to cyber criminals.[9]

[5] "VR and AR: The Ethical Challenges Ahead," *Educause*, er.educause.edu/blogs/2018/4/vr-and-ar-the-ethical-challenges-ahead.

[6] "The role of corporations in addressing AI's ethical dilemmas," *Brookings*, brookings.edu/research/how-to-address-ai-ethical-dilemmas/.

[7] *The New York Times*, nytimes.com/2018/06/19/

[8] *AI Now Report 2018*, ainowinstitute.org/AI_Now_2018_Report.pdf

[9] *"The Global Risks Report 2019,"* *World Economic Forum*, weforum.org/reports/the-global-risks-report-2019/

How can the industry meet the challenges posed by society?

As the AI Now Institute has pointed out, at the core of the digital dilemma debates in 2018 are questions of accountability: who is responsible when AI systems harm us? How do we understand these harms, and how do we remedy them? Where are the points of intervention, and what additional research and regulation is needed to ensure those interventions are effective?[10]

As Todd Marlin, EY Partner and Global Leader for Forensic Data Analytics & Financial Services Forensic Technology says: "We are on the brink of a "perfect storm," where AI, cybersecurity and privacy issues are converging. Organizations need to understand this increasingly complex legal and compliance environment, where existing risks intertwine and new risks keep emerging. For the industry and its companies, it is critical to get ahead of the storm." From this we can conclude that It is clearly a responsibility of the industry to address these issues and, with other stakeholders, to find solutions that will enable the industry and society to develop along a path of mutual benefit and trust.

Failure to take an active role in the digital dilemma debates could have serious repercussions. These include increased regulation by governments, reduced revenues as advertisers refuse to be associated with channels and information which are perceived to be harmful, lower visitor rates as the public grows more skeptical about social media and more aware of its dangers, reduced investment as the new generation of consumers and investors, tech-savvy but socially conscious, turn their attention toward products and services that genuinely "do no harm". In his annual letter to CEOs Larry Fink, CEO of Blackrock, the world's largest investor wrote: "Companies that fulfill their purpose and responsibilities to stakeholders reap rewards over the long-term. Companies that ignore them stumble and fail. This dynamic is becoming increasingly apparent as the public holds companies to more exacting standards. And it will continue to accelerate as millennials – who today represent 35% of the workforce – express new expectations of the companies they work for, buy from and invest in."[11]

The companies in the industry seem to have understood that the TMT sector will play a key role, and even become a role model, in how AI is pursued around the globe. Society's acceptance level will be strongly influenced by how ethically AI is being developed and how it interacts with impacted stakeholders. Employees and management working in the field of engineering and programming are starting to see data

"

We are on the brink of a "perfect storm," where AI, cybersecurity and privacy issues are converging. Organizations need to understand this increasingly complex legal and compliance environment, where existing risks intertwine, and new risks keep emerging. For the industry and its companies, it is critical to get ahead of the storm.

Todd Marlin
Partner, Ernst & Young LLP,
EY Global Leader, Forensic Data Analytics &
Financial Services Forensic Technology

[10] *AI Now Report 2018*, ainowinstitute.org/AI_Now_2018_Report.pdf
[11] *"Larry Fink's 2019 letter to CEOs: Purpose & Profit," BlackRock*, blackrock.com/corporate/investor-relations/larry-fink-ceo-letter.

security, algorithms and AI decision-making in a broader social and ethical context. The EY *Fraud Survey* series shows how ethics is becoming a critical priority for management. According to the EY *EMEIA Fraud Survey 2017*, 40% of respondents from the industry "heard senior management communicate frequently regarding the importance of maintaining high ethical standards" over the previous two years.[12] In the EY Global Fraud Survey 2018, 98% of respondents from the industry felt that it was fairly or very

important "to be able to demonstrate that your organization operates with integrity."

As a result of this new social consciousness, there are considerable efforts in the industry to find technological solutions. For example, data analytics and cybersecurity technologies are already providing better protection for companies and individuals. The issue of bias, despite its inherently subjective nature, will also have some technological solutions.

For example, one company which is developing cloud-based software will provide transparent views to customers on how their algorithms are making decisions and the factors underlying them.[13]

Clearly, much needs to be done beyond technology: engagement in a public discourse with stakeholders, from governments to consumers, has become critical. There are mainly two aims for such engagement by companies. Firstly, for finding

---

12 EY *EMEIA Fraud Survey 2017*

13 BBC news technology, *BBC News*, bbc.co.uk/news/technology-45561955.

"

Companies that fulfill their purpose and responsibilities to stakeholders reap rewards over the long-term. Companies that ignore them stumble and fail. This dynamic is becoming increasingly apparent as the public holds companies to more exacting standards. And it will continue to accelerate as millennials — who today represent 35% of the workforce — express new expectations of the companies they work for, buy from and invest in.

Larry Fink
CEO, Blackrock

real solutions to apparently intractable problems with the help of wide stakeholder engagement – a kind of crowdsourcing of ideas from people belonging to different sectors and professions, such as ethicists, behavioral scientists, philosophers and others. Secondly, for rebuilding their reputations, so as to remove possible obstacles to growth, such as regulation, walk-outs or other civic actions. Executives of TMT companies interviewed for the EY *Global Fraud Survey 2018* placed customer and public perception as the top benefits of demonstrating integrity, higher than successful business performance and shareholder perception. It is no wonder that companies in the industry have gone on an active campaign to engage and communicate with the wider community on digital dilemmas.

Over the last year, we see companies in the sector taking a far more proactive role in public fora and dialogues with organizations such as the influential *World Economic Forum*. Indeed, at Davos in January 2019, topics included "A New Architecture for Cyber-Cooperation" discussing how the public and private sectors should collaborate in new and innovative ways to counter the challenge of cyber attacks; "A New Kind of Learning?" on what values, behaviors and skills must be taught to the new generation in the era of AI; "Compassion through Computation: Fighting Algorithmic Bias"; and "Governing Data in Our Daily Lives" on how ethics and norms should ensure that data-driven decisions are not perpetuating biases and prejudice. Many of the TMT's top leadership were present and actively participating.[14]

Companies have also taken active measures in terms of governance and management to provide guidance and direction to their employees, investors, customers and consumers. For example, many leading TMT companies have adopted ethical codes, which have also served as guidelines for the industry.

Finally, a plethora of organizations has emerged – including universities, think-tanks, and non-government organizations (NGOs) – to study the issue. They are bringing together leaders of the industry, former employees, government officials and academics from different disciplines in a serious collaborative effort.[15] These play a critical role in building the cross-sector partnerships and "crowdsourcing of ideas" mentioned earlier. The TMT sector can join, inform, support and fund these useful initiatives, and indeed is beginning to do so.

---

[14] "World Economic Forum Annual Meeting," *World Economic Forum*, weforum.org/events/world-economic-forum-annual-meeting/programme.

[15] In researching this paper, we consulted materials produced by the AI Now Institute, the Algorithmic Justice League, the Brookings Institutions' Center for technology Innovation, the Partnership on AI, the Foundation for Responsible Robotics.

How can companies manage the risks of digital transformation?

Clearly, the industry is on a new trajectory. But individual companies within the industry are likely to find themselves confronting some of these digital dilemmas as they embark or continue on their journey of digital transformation. We offer here some initial recommendations about what companies can do to manage the risks and opportunities of this rapidly changing market.

And also, compliance programs are maturing on the basis of the challenges of the digital era: keeping up with the speed of innovation is challenging for the compliance officer, as business risks, procedures and ways of working are changing rapidly. And this has a significant impact on the skill set needed by the compliance officer and how they interact with key stakeholders within the organization to prevent, detect and respond to fraud.

As a starting point, companies should manage fraud and compliance risks beyond clear policies and procedures. Rule-based compliance programs are transforming to behavioral-based approaches: adopting an Integrity Agenda helps in the new era, underpinned by a digital integrity strategy, which puts the agenda into practice at all levels of the company.

The Integrity Agenda helps companies bridge the gap between intentions and behaviors. It is a framework for success built on a core set of elements that align an individual's actions with an organization's objectives. To develop the agenda, companies should focus their efforts on four elements: assessing the corporate culture, controls and governance from an integrity perspective, and leveraging new technologies to provide better data insights.

A clear Integrity Agenda that is based on communication, leadership commitment, strong training and

The Integrity Agenda has four foundational elements that align an individual's actions with an organisation's objectives. The core challenge is influencing behaviour over diverse and dispersed employees and third parties amid intense competitive pressures and rapid technological change.

Culture

Measurable effectiveness

Governance

Data insights

Controls
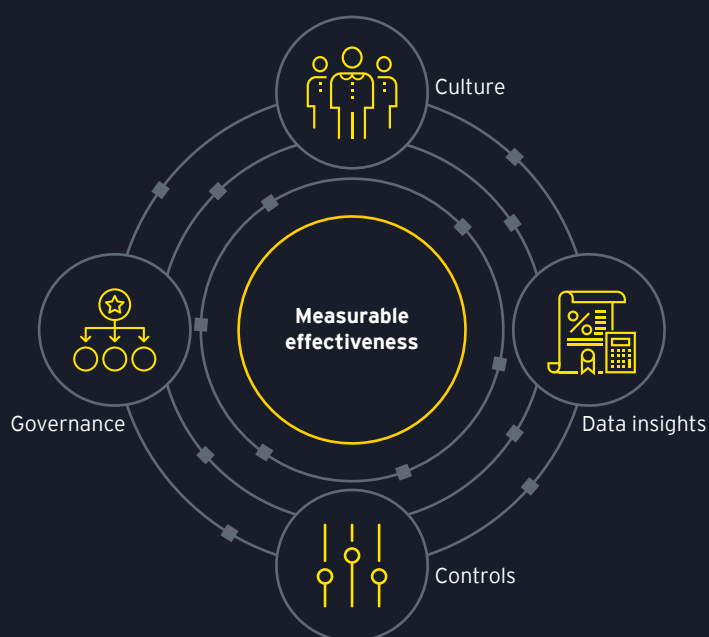
interaction, as well as technology-based procedures, can address the challenges posed by customers and society by enabling the entire workforce to be more aware of the ethical risks which the company is confronting. A well-thought-out Integrity Agenda enables successful companies to stay true to their missions, keep their promises, respect laws and ethical norms, and foster public trust in the free enterprise system.

They can manage the agenda by designing and establishing a digital integrity strategy. This is a business model which combines a vision for AI technological development with foresight into its social and ethical impact. Creating and managing a digital integrity strategy will allow companies to innovate while remaining sensitive to external and internal pressures.

The digital integrity strategy enables the company, from the CEO to every member of the team, to consider the broader ramifications of their technical, scientific and financial decisions. At the root of the strategy are a number of simple and inter-related questions – each requiring highly complex answers – which need to be asked, on an ongoing basis, about the relationship between AI and the underlying data sets at each stage of the R&D, production and marketing process:

▸ **Purpose:** What is the purpose of applying AI to the data?

▸ **Application:** Where does the data come from, to whom does it belong and how will it be used?

▸ **Criticality:** What are the social and ethical implications of applying AI to the data? Are there any other viable solutions?

This approach will enable companies to manage situations where a new technology has led to the risk of an ethical dilemma. As we have highlighted, many of the technological outcomes and their social and ethical impact cannot realistically be foreseen. A digital integrity strategy based on these three approaches allows the company, over time, to be flexible in balancing innovation and ethics. In so doing, the business model can bridge the twin pillars of profit and purpose that constitute long-term business success, as described by Blackrock's Larry Fink.[16]

A company's digital integrity strategy will, in practice, be constructed from many different and complex building blocks, and will be specific to each company. For example, creating a digital integrity strategy will require a fresh look at the basic tenets of internal control in the age of AI – due diligence, audit, accountability and transparency will all need to be looked at anew.

The conclusions drawn about the function, structure and operational processes of the company will go far beyond the IT function of a company. The digital transformation will most likely involve close multifunctional collaboration, between parts of the company that traditionally were quite far apart, such as IT, human resources (HR), legal and compliance. Many functions will also need to acquire new skills to meet new demands of the market; and there might be a need for new structures and new functions. For example, companies that are investing in AI should consider the appointment of a digital integrity leader – a C-suite executive who is capable of combining technical know-how and business insights, as well as knowledge of legal and compliance risks into a cohesive vision for the organization.

We are in effect talking about a wholesale change in corporate culture driven by the introduction of AI. Ultimately, AI should be considered a discipline, not just a tool for technological advance.

Here are a few examples of key steps in building a digital integrity strategy, classified according to the guidelines of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control framework:[17]

Control environment:
▸ Define the company's business model, purpose and its social objectives, including the role and positioning of AI

▸ Create a code of ethics which lays out principles, processes and guidelines for handling the ethical aspects of digital development

▸ Appoint a digital integrity leader who will interact with the technical and business teams to ensure that all ethical implication of technological innovation is being fully considered, and will be instrumental in implementing an ethical corporate culture

Purpose

Digital Integrity Strategy

Criticality

Application

---
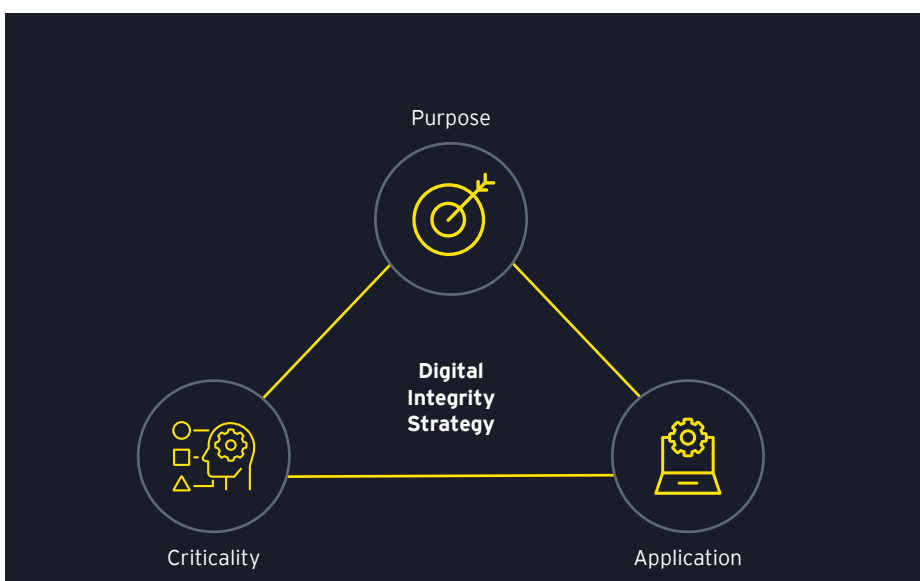
16 "Larry Fink's 2019 letter to CEOs: Purpose & Profit," BlackRock, blackrock.com/corporate/investor-relations/larry-fink-ceo-letter.

17 COSO, coso.org/Pages/default.aspx.

Risk assessment:

‣ Conduct a risk assessment and compliance performance assessment to constantly evaluate the role and purpose of digital technologies, and advanced solutions such as AI and their implications for key stakeholders, such as employees, customers, consumers and government

‣ Establish external oversight and advisory bodies to ensure that due attention is paid to ethical challenges – this could include employee representation on the board of directors, external ethics advisory boards, and the implementation of independent monitoring and transparency efforts[18]

‣ Support and contribute financially to a third-party think tank or NGO that is doing useful research into ethics in the sector

Procedures and control activities:

‣ Implement at all levels of the company, the corporate strategy that balances the financial goals with ethical outcomes

‣ Embed the digital integrity strategy into the business plan through financial and nonfinancial incentives

‣ Hire a diverse workforce from a variety of cultural or educational backgrounds and professional disciplines; and prevent exclusion, harassment or other forms of discrimination on the basis of gender, race, sexuality or disability, bearing in mind how exclusionary cultures can influence product bias

‣ Ensure that your digital integrity strategy is shared with and understood by customers, suppliers and partners in the supply chain, and also try to educate and get business parties to buy into your company's purpose

‣ Set up a means of remediation in case AI deployment results in consumer damages or harm since, having clear procedures in place will help when disasters strike or when there are any unanticipated consequences from emerging technologies

Information and communication:

‣ Communicate the corporate purpose, the code and other policies internally through multiple channels

‣ Offer protection for conscientious objectors and whistleblowers to encourage accountability and ethical decision-making

‣ Develop interactive ethical training programs for employees as this cross-functional training can serve as a creative platform for sharing best practices, joint problem solving and finding solutions to digital dilemmas

‣ Engage and communicate with competitors, other TMT companies and external groups of stakeholders on key digital topics such as regulatory environment, bias, civic and human rights, data protection, privacy, etc.

Monitoring activities:

‣ Set up AI audit trails that explain how particular algorithms were put together or what kinds of choices were made during the development process. This can provide some degree of "after-the-fact" transparency and explainability to outside parties[19]

---

[18] *AI Now Report 2018*, ainowinstitute.org/AI_Now_2018_Report.pdf.

[19] "The role of corporations in addressing AI's ethical dilemmas," *Brookings*, brookings.edu/research/how-to-address-ai-ethical-dilemmas/.

In conclusion

The TMT sector's technological strength and competitive advantage in the new digital economy have brought to the industry, opportunities and risk in equal measure.

While the opportunities for the industry are now clear, the risks of what Kristofer Ågren, Head of Data Insights for Division X for Telia Company, has called "the move fast and break things" approach are only now being revealed.[20] Being at the front-line in terms of global reach, technological edge, financial might and social influence has brought with it new and important responsibilities. The industry will need to find solutions to the digital dilemmas posed by AI and other new technologies, and engage with society in a proactive and constructive manner. Putting the corporate head in the sand is no longer an option.

In the absence of clear social or political guidelines about "what is acceptable" and "what is not acceptable," individual companies will also need to identify for themselves their own ethical principles. This can be done by following a path of common sense and voluntary self-regulation based on a more profound and considered understanding of the short-term and long-term consequences of the technology.

For a company, a good start is to put in place an Integrity Agenda backed by a digital integrity strategy. A company's commitment to purpose as well as profit must be made clear to all stakeholders, and the company must have the culture, structure and capabilities to see it implemented. With the help of a fully implemented digital integrity strategy which holistically and harmoniously integrates ethical considerations into the core business and technological processes, a company can begin to retain its competitive edge without compromising its values or harming society. In such a way, each company can live the values at all levels, from every strategic decision to every new product introduction, from every algorithm to every line of code.

Those companies that succeed in combining their entrepreneurial spirit and technological drive with integrity and a commitment to benefiting society will be generously rewarded by their shareholders, consumers and the broader public at large, both now and in future generations.

Author

Andreas Pyrcek
Partner, Ernst & Young GmbH
EY Global TMT Sector Leader,
Forensic & Integrity Services

[20] "New Global Hub Helps Companies Avoid the Ethical Pitfalls of AI," *Triple Pundit*, triplepundit.com/2019/01/business-hub-ai-ethics/.

EY | Assurance | Tax | Transactions | Advisory

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. 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.

ey.com/forensics