Legal, Compliance and
Technology Executive Series

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.

EY
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.ntsb.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.

EY | Assurance | Tax | Transactions | Advisory

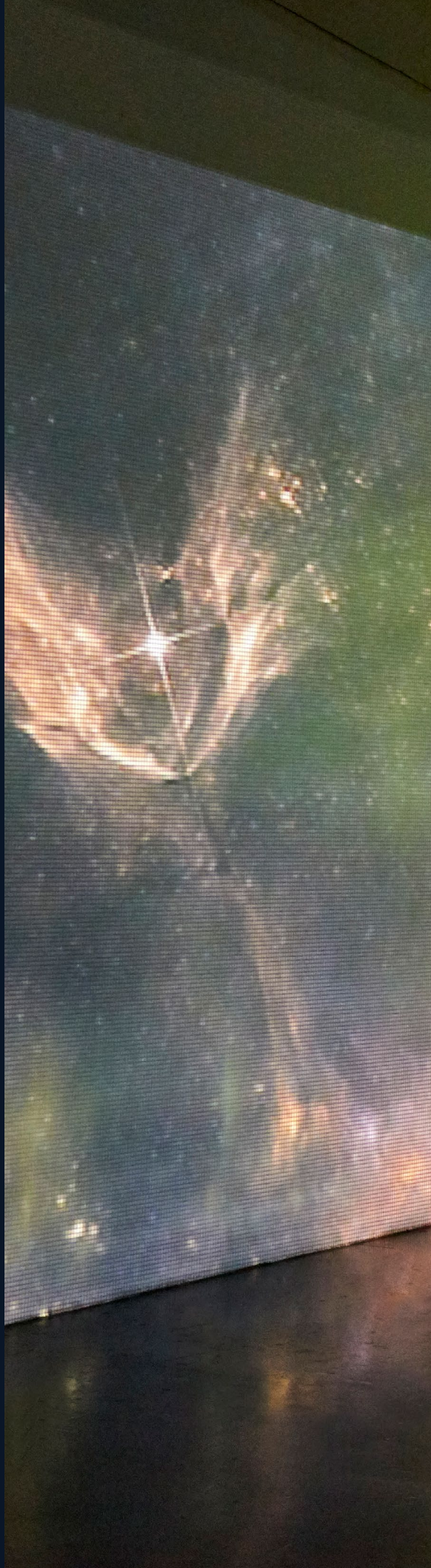
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders.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

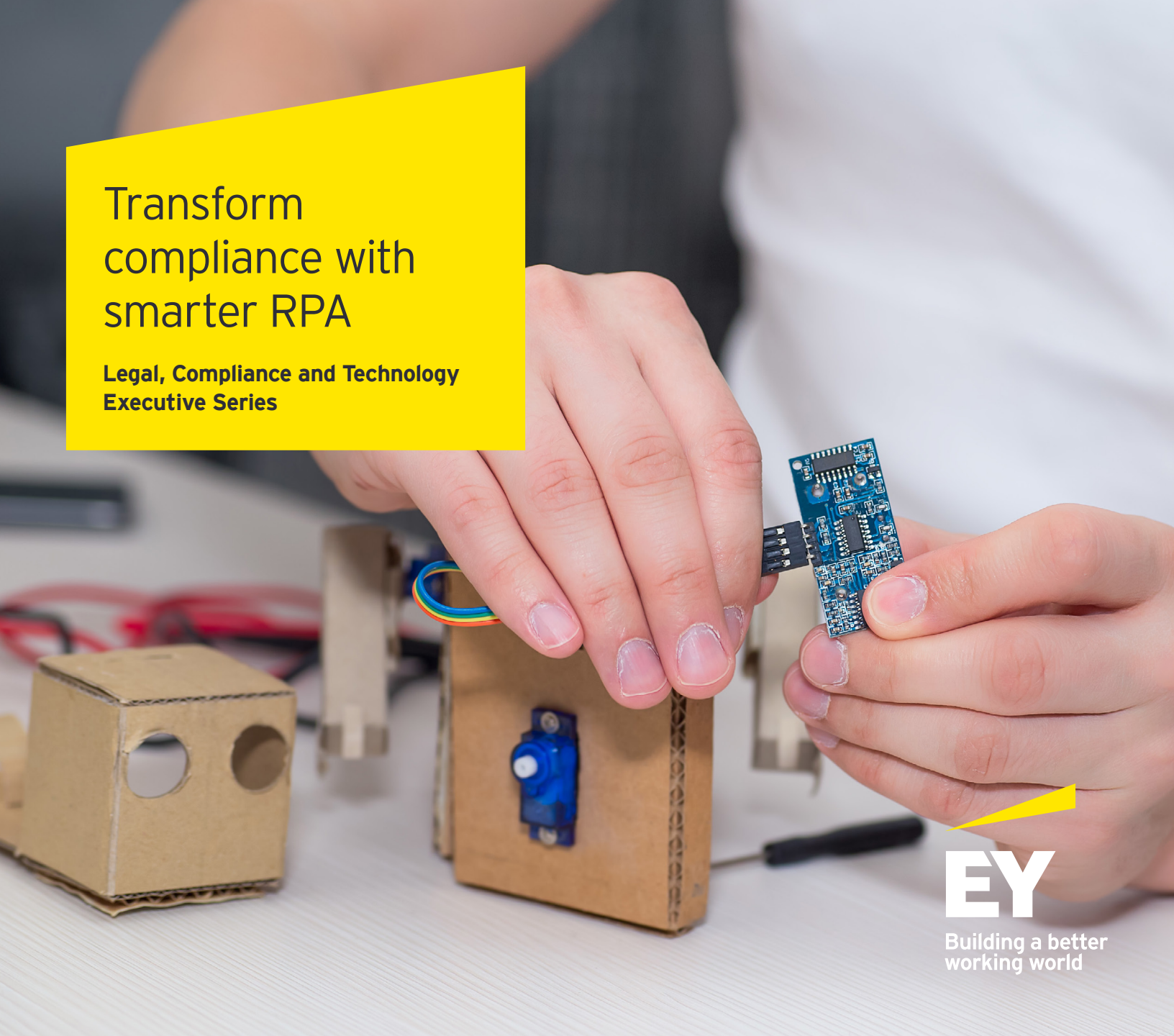
EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and 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.

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

ey.com





Transform compliance with smarter RPA

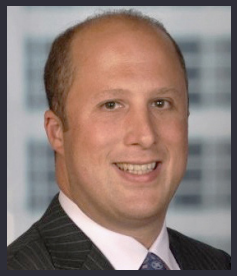
Legal, Compliance and Technology Executive Series

EY
Building a better working world

Of special interest to:

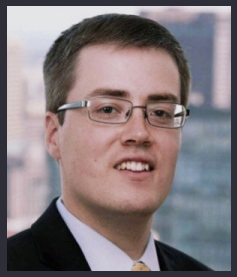
Legal counsel
Corporate security officers
Information security executives
Compliance executives
Risk management executives
Internal audit

Authors:



Todd Marlin

EY Global Forensic & Integrity Services Technology & Innovation Leader



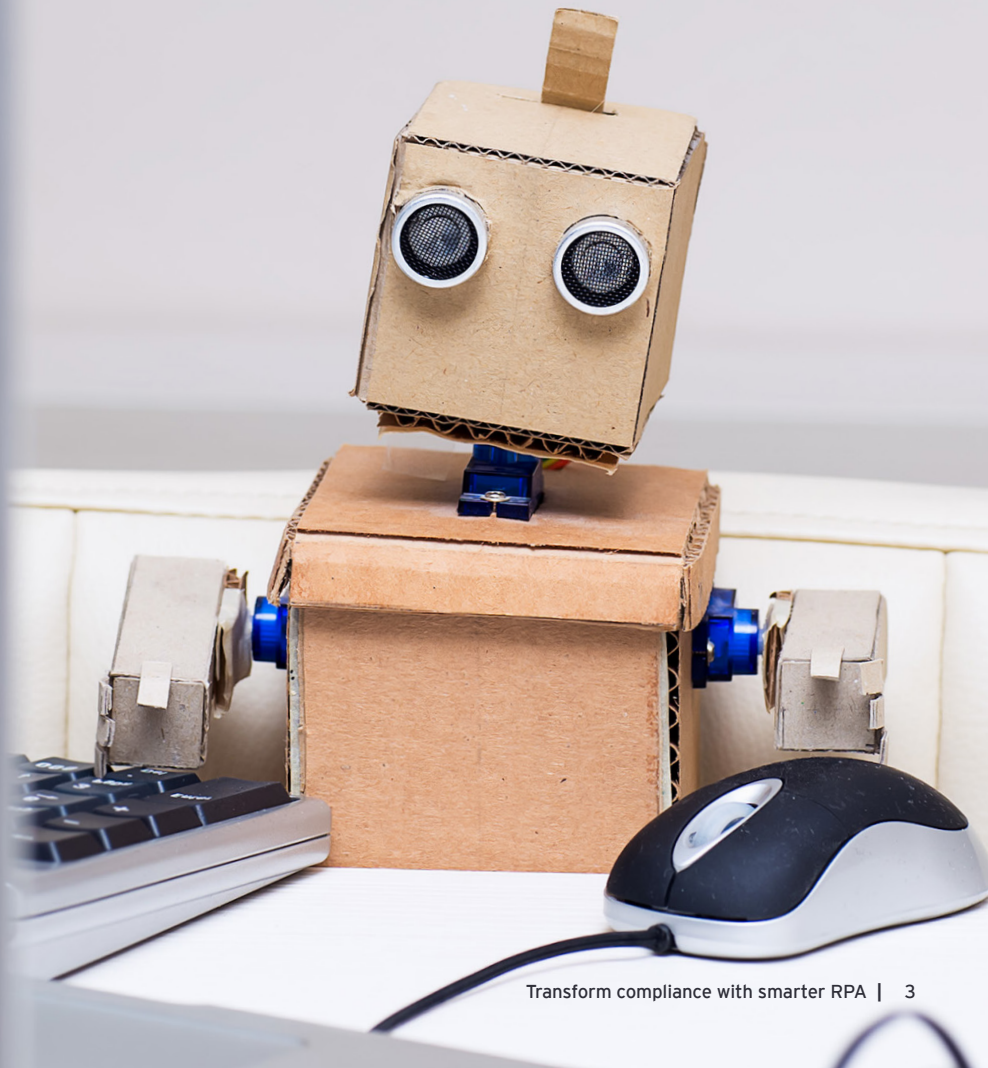
Jeremy Osinski

Senior Manager
Forensic & Integrity Services
Ernst & Young LLP

Transform compliance with smarter RPA

Companies intent on driving efficiencies in compliance management have increasingly turned to robotic process automation (RPA). The use of RPA helps deliver operational and cost efficiency, while improving quality by reducing human errors. But using RPA alone has its limitations — while it mimics human behavior, it cannot learn from mistakes or evolve with changing business environment. Technology-savvy organizations are gradually looking to enhance their automation efforts with artificial intelligence (AI) tools, such as machine learning and natural language processing (NLP).

This paper examines key areas of the compliance function that pose great opportunities to implement automation – in many cases, intelligent automation – by incorporating AI technologies.



Compliance under pressure

Governments around the world are enacting new regulations to keep pace with emerging technologies and the growing commercialization of consumer data. Companies doing business in multiple jurisdictions must determine how best to comply with conflicting laws. The cost of noncompliance is usually hefty fines.

Increasing digitization of business activities is also putting pressure on compliance functions. Compliance programs have long relied on data and now need to incorporate more data than ever. The large volume and wide variety of data types are becoming increasingly challenging, sometimes impractical, for humans to handle on their own.

Companies are increasingly adopting RPA in compliance programs

One of the fastest-growing markets for business software is RPA, which trains software "bots" to perform standard, rule-based processes. The rules-based and repetitive nature of many compliance processes make them strong candidates for RPA adoption. Many RPA tools today no longer require specialized technical skills, thus making it easier for compliance professionals to use them in their day-to-day activities. RPA bots are being created to automate the data ingestion process in compliance programs such as retrieval, cleansing and formatting. Routine regulatory reporting has also seen more bots at work.

While bots can be good at taking on rote work, they aren't smart enough to handle many complex legal and regulatory requirements that often demand in-depth analysis by aggregating and cross-referencing data. Companies are starting to turn to AI technologies to complement RPA. Redesigning business processes with AI-enhanced RPA not only shifts low-value human tasks to bots, it provides the insights to shape strategic decisions.

By 2022, 80% of RPA-centric automation implementations will derive their value from complementary technologies, according to Gartner. The most common ones are machine learning and NLP. Gartner predicts organizations that combine AI and RPA technologies with redesigned processes will cut nearly a third of their operational costs by 2024.[1]

[1] Kasey Panetta, "Gartner Top 10 Strategic Technology Trends for 2020," Gartner, 21 October 2019, https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/.

Complementary technologies enhance RPA implementation

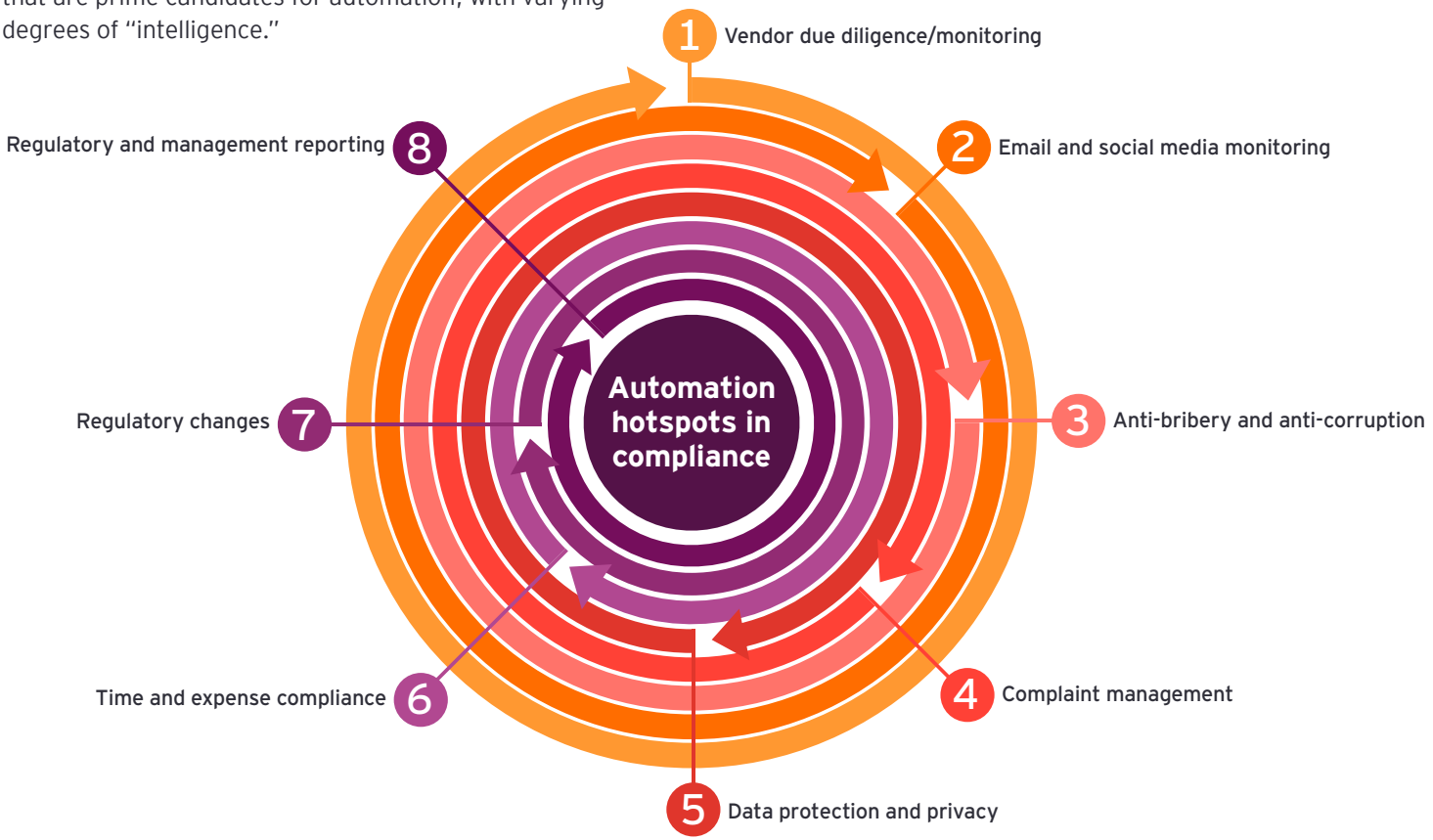
The use of analytics-driven technologies alongside RPA can help the compliance function enhance and expand the scope of its automation efforts. The most common technologies being used thus far are machine learning and NLP.

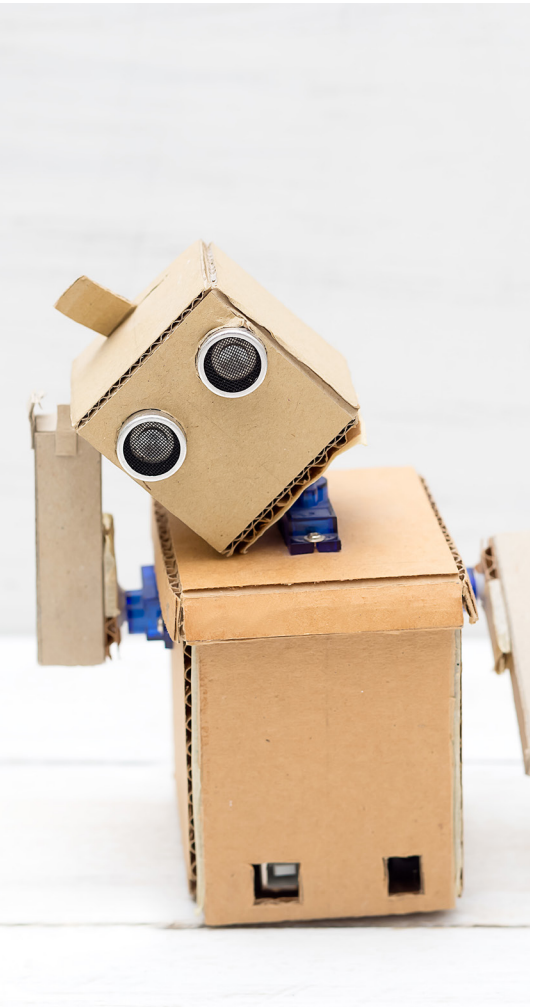
Machine learning helps analyze and understand unstructured data (e.g., comments in T&E data and customer service logs). Machine learning algorithms can be used to help detect hidden patterns of risky activities and relationships. Its self-learning feature improves analytic accuracy and reduces false positives over time.

NLP allows computers to understand human language, both text and speech. NLP models decipher meaning, measure sentiment and categorize the data. For example, NLP can be used to analyze notes in sales transactions to detect potential fraud by emotive tone analysis.

Automation hotspots in compliance

Based on client engagement experience, EY teams have identified several key areas in a compliance function that are prime candidates for automation, with varying degrees of "intelligence."





Vendor due diligence

Vendor due diligence often involves many laborious tasks that are ideal for RPA implementation. Bots can be set up to automate clearly defined checkpoints (e.g., check against a pre-established list of banned vendors or vendors that could cause conflict of interest). Machine learning technologies can be used to integrate a much wider range of data sources (e.g., sanction data, court records) and perform in-depth analysis to uncover risks that otherwise may not be obvious by the traditional method.

Email and social media monitoring

RPA software can be set up to regularly scan corporate emails and public social media posts with pre-defined key word searches intended to identify risk activities and relationships. However, deploying NLP can greatly enhance risk detection. NLP can be used with sentiment analysis tools that evaluate the emotion, tone and intent of messages. Critics charge this violates employee privacy, but messages can be kept anonymous during processing and access to identified risk activities can be controlled. These tools can produce real-time heat maps of employee engagement — even analyzing emojis, in addition to text.

Anti-bribery and anti-corruption (ABAC)

Standard, rules-based ABAC tests can be programmed in bots to analyze data and identify red flags in transactions (e.g., round dollar payments, miscellaneous payment description). But the range of data sources that can be accessed or analyzed can be limited if using RPA alone. Using machine learning technologies, the bots' risk assessment abilities can be greatly enhanced by integrating a much broader set of data sources and generating scores to indicate the level of potential risks.

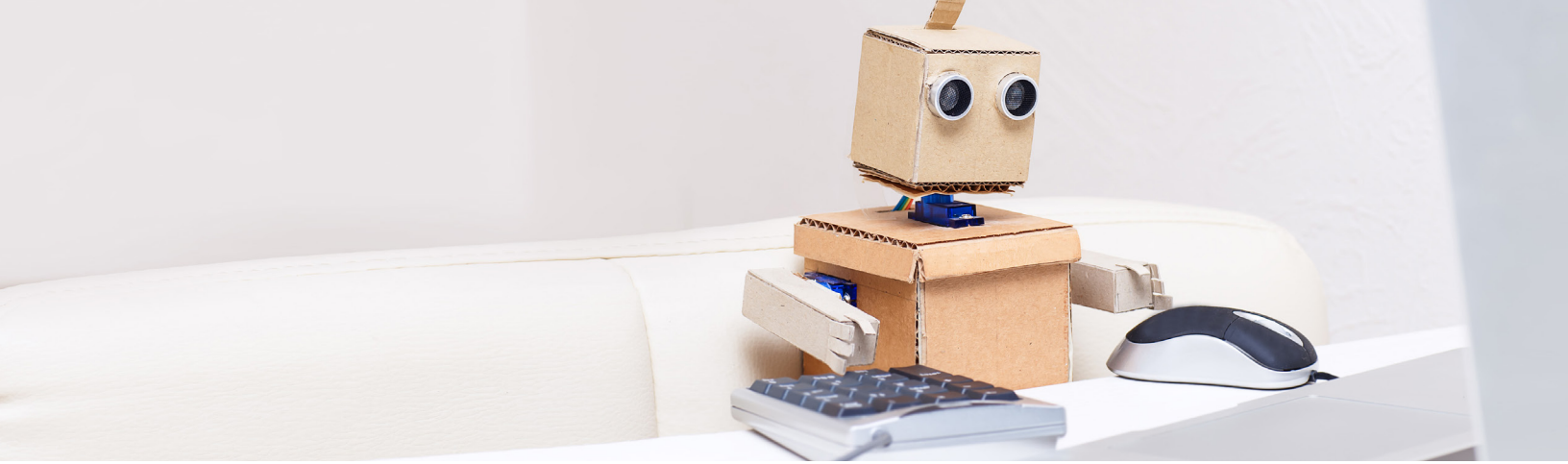
Complaint management

Taking lessons from how RPA and AI tools are already transforming customer service in the consumer space, companies can greatly enhance the handling of calls to ethics hotlines. For example, IBM Watson's Tone Analyzer uses machine learning to analyze chatbot conversations as they occur to help predict customers' emotions and issue automatic apologies. Voice analysis detects negative emotions from both the customer and service representative, providing real-time feedback to employees that helps them resolve the call, or flags the conversation for escalation to a supervisor. Successful complaint resolution mitigates legal risks while trends can be detected by categorizing and analyzing complaints.

Reducing risk with digital twins

A team of professionals from EY Forensic & Integrity Services collaborated with General Electric (GE) to improve its compliance training with an automated solution using advanced analytics. Risk profiles were created for each employee from GE systems data — becoming part of that employee's "digital twin" and allowing GE to automate and personalize compliance communications and training, rather than relying on mass emails and courses that may be ignored.

For example, if an employee is about to travel to a high corruption-risk country to meet with a new customer, the employee automatically receives a message in a preferred communication channel that summarizes risks and links to relevant GE policies and processes. The system also creates integrity scores, so managers can reward employees with high scores or coach those with lower ones.



Data protection and privacy

The surge in data protection laws around the world is accelerating the move to AI-enhanced automation solutions. Technologies that automate the discovery, inventory and classification of sensitive data help reduce noncompliance risk but often need machine learning algorithms to handle complex aspects of the tasks, especially when it comes to discovery and classification. Gartner predicts more than 40% of privacy compliance technology will rely on AI over the next three years, up from 5% in 2020. Gartner also finds most companies are now handling privacy requests from customers manually at an average cost of $1,400 each, while taking at least two weeks to respond.[2]

Time and expense compliance

Requiring managers to manually approve employee time and expense reports can be a laborious task that takes time away from important business decision-making. Expense management tools are using RPA to automate simple checklist type of tasks such as matching credit card receipts to approved types of charges. Adding machine learning allows companies to detect irregular expenses and patterns, flagging them for human review. For example, machine learning algorithms can be developed to categorize expense policy violators based on their risk levels and send email warnings tailored to the severity of the problem.

Regulatory changes

The unending flow of new regulatory or legal requirements can be managed more effectively with automated solutions. For example, a global effort to phase out interbank offer rates (IBORs) means any existing contracts or transactions linked to IBORs maturing after 2021 will require contract amendments or fallback language. Professionals used to have to manually analyze pages of documents to understand exactly what was needed to comply. There are many document intelligence tools that can be used to automate a large portion of the work and convert legacy contracts into digital formats that can be processed by contract management software.

[2] "Gartner Says Over 40% of Privacy Compliance Technology Will Rely on Artificial Intelligence in the Next Three Years," Gartner press release, 25 February 2020, https://www.gartner.com/en/newsroom/press-releases/2020-02-25-gartner-says-over-40-percent-of-privacy-compliance-technology-will-rely-on-artificial-intelligence-in-the-next-three-years.

Regulatory and management reporting

Corporate regulatory reporting is a complex and time-consuming process that begs for technology solutions. RPA bots can be used in straightforward data collection and cleansing tasks. It's been a common practice to use AI and advanced analytics technologies to provide deep insights and uncover hidden risks in regulatory and management reporting. The sheer volume of reporting required by a compliance function makes this the most promising area for joining AI and advanced analytics with RPA.

Moving forward

To stay competitive and reduce risks, companies must become more agile, strategic and efficient in managing compliance. Investing in intelligent automation is a critical consideration for compliance leaders looking to achieve these goals.

Here are some tips for successfully implementing intelligent automation:

1. Start small

RPA on its own can quickly add a great deal of value. Assess your current processes to identify low-hanging fruit. Look for high-volume, routine, rules-based tasks that can be more efficiently performed by bots. Adopt a phased approach with your automation efforts to minimize disruption to the business and to demonstrate measurable results along the way.

2. Understand your data

Before any large-scale AI implementation, determine what data the technologies will run on. Identify the data sources, know how to access them and establish a central data platform. AI algorithms require clean, quality data to function properly.

3. Ensure human involvement

Don't ever assume that automation can run on its own. There should always be a monitoring process in place where humans can assess performance of the automation systems and intervene when needed. Many AI technologies, such as machine learning, have self-learning capabilities that require human input. In addition, business and regulatory environments evolve quickly in today's age that human engagement is critical to ensure compliance programs are up-to-date.

To learn more, visit ey.com/ForensicDataAnalytics

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. 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
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

EYG no. 002496-20Gbl
WR #2003-3462434
ED None

ey.com

Can you trust what you read?

Debunking fake news in the digital age

Legal, Compliance and Technology Executive Series

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

EY
Building a better working world

Of special interest to:

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

Author:
Todd Marlin
EY Global Forensic & Integrity Services
Technology and Innovation Leader

Executive summary

Fake news — the intentional spread of false information — erodes public trust, harms institutions and individuals, and confuses a public trying to make sense of an increasingly complex world. Even with quality control measures in place, there have been many times reporting in the mainstream media is found to be false. Social media and online news platforms allow anyone to be a reporter without the same level of due diligence levied on professional reporters by their affiliated media outlets, which only increase the risk of fake news. Media companies, consumer watchdogs and governments are taking steps to address the issue, but their efforts are far from enough.

Russia's documented attempts to influence the 2016 US presidential election with fake social media accounts that posted false information woke up many to the danger of fake news. COVID-19, perceived as the most significant pandemic in the age of social media, only intensified the issue. Panic over a deadly disease, misleading and conflicting information from government officials, and partisan politics have sent a tidal wave of fake news swirling around the globe. The inability of the public to determine what is true or false can have life-and-death consequences.

Digital media companies have long been criticized for failing to remove obvious falsehoods from their channels. The coming of another contentious election year in the US, coupled with the COVID-19 pandemic, is putting renewed pressure on them. As social media companies step up their efforts to counter fake news, governments are also increasingly inclined to take action. Many global corporations have begun monitoring social media and news coverage about them.

Amid the calls to crack down on fake news, technology company professionals as well as academics are working to develop effective counter measures. It has proven to be a challenging journey, but not short of promising outcomes. The purpose of this paper is to share some of the fake news detection methods to date, their successes and limitations, and to explore innovative ideas as the world continues its fight for the truth.

Fake news poses a growing threat

The ability to share and reshare content online means people can spread false information, sometimes so quickly that it drowns out the truth. The *2019 CIGI-Ipsos Global Survey* found 86% of internet users said they have been duped by fake news at least once.[1] While this hurts all aspects of society, it poses special risks for businesses that can suddenly see their reputation and revenue damaged.

Misinformation takes many forms

Misinformation can come from satire or parody, forms of entertainment that embellish actual news in a comedic fashion. Late night talk shows and satirical pieces such as those found in *The Onion* typically exaggerate real events in such a way that the audience easily understands the difference between truth and fiction. But completely fictional entertainment can also dupe the public, as when the 1938 "War of the Worlds" broadcast convinced some radio listeners that Martians were landing. In the 1990s, many movie-goers thought "The Blair Witch Project" was true because of marketing for the low-budget horror movie.

False advertising claims can be another form of misinformation. In addition, celebrities often use their status to shape public opinion, sometimes heavily influenced by personal bias and financial incentives. Many celebrities have been fined for making misleading claims, while others have sued companies for creating fake endorsements using their names and images.

The focus of this report is on deliberate lies, often shared through social media and online news channels. While US President Trump pioneered the practice of calling reporting he disagrees with "fake news," a term typically reserved for information designed to deceive.

Perhaps the most unsettling form of fake news is state-sponsored propaganda or disinformation, such as documented Russian efforts to influence the 2016 US presidential election and the 2019 EU elections. The problem has grown even more urgent with the COVID-19 pandemic with fake news inundating social media and adding stress to an already tense situation.

[1] *CIGI-Ipsos Global Survey: Internet Security & Trust*, Ipsos Public Affairs and the Centre for International Governance Innovation, 2019.

Fake news erodes public trust and damages businesses

A Massachusetts Institute of Technology (MIT) study of Twitter from 2006 to 2017 found that fake news stories were 70% more likely to be retweeted than true stories, with the truth taking about six times as long to reach 1,500 people as falsehoods. Falsehoods were spread farther and faster than the truth in all categories, with political news leading the way and business rumors coming in third.[2] People have a predisposition to favor information that is more novel than accurate reporting or confirms what they already believe.

Fake news can cause a public relations crisis and even drive down a company's stock. Pepsi was threatened by boycotts after false reports circulated saying the company CEO told Trump supporters to "take their business elsewhere." A video showed a Tesla self-driving car crashing into a robot, even though Tesla doesn't make a self-driving car. An Indian e-commerce firm saw its market value drop 71% in one day following false messages regarding its financial stability circulated on social messaging apps.

Small businesses with limited resources may be at even more risk than resource- and cash-rich large corporations. One Indian restaurant in London saw its business cut in half after it was accused of serving human meat. Researchers analyzing fake stock promotion articles prosecuted by the U.S. Securities and Exchange Commission found fake news impacted the price of small cap companies more than large companies.[3]

> "A lie gets halfway around the world before the truth has a chance to get its pants on.
>
> **Winston Churchill**

COVID-19 pandemic leads to an explosion in fake news

COVID-19 has been unprecedented in changing the way the world lives and works, so it's not surprising that the virus has led to an outbreak of fake news, with people around the world sharing content on everything from lockdowns to tips for warding off the virus. Nearly half of Americans say they've read fake news related to the virus in some form of media and nearly a quarter seemed to believe the false story that COVID-19 was intentionally created, according to a Pew Research Center survey.[4]

Business leaders have also fallen victim to fake news in the wake of COVID-19. The chief medical officer of a US company sent an email to employees encouraging them to drink warm water to ward off the virus, after reading about the advice on a viral post, falsely attributed to Stanford University. The university denied issuing it and epidemiologists say the advice is not valid. While the advice was not harmful, the episode embarrassed both the company and executive.

[2] Peter Dizikes,"Study: On Twitter, false news travels faster than true stories," *MIT News*, 8 March 2018, http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

[3] Harlan Loeb, "Business Must Combat Fake News," Edelman, 20 February 2019, https://www.edelman.com/insights/business-must-combat-fake-news.

[4] Amy Mitchell and J. Baxter Oliphant, "Americans Immersed in COVID-19 News; Most Think Media Are Doing Fairly Well Covering It," 18 March 2020, Pew Research Center, https://www.journalism.org/2020/03/18/americans-immersed-in-covid-19-news-most-think-media-are-doing-fairly-well-covering-it/.

It takes a village to fight fake news

Fake news impacts every organization, private or public, as well as the individual consumer. Well before the COVID-19 pandemic, many organizations were taking steps to manage the risk of fake news, but those efforts have dramatically increased.

Internet companies step up efforts to stop the spread of fake news

While billions of people around the world use social media, three-quarters of internet users surveyed in 2019 said they don't trust social media companies and 65% don't trust search engines.

After being criticized for spreading Russian-generated posts to millions in the 2016 US presidential election, Facebook stepped up efforts to mitigate fake news. Users can categorize a post as false; if enough people flag it, fact-checkers employed by Facebook will review it. Deceptive or fabricated posts are tagged as "disputed" and linked to a corresponding article explaining why. However, relying on users has drawbacks. An MIT study[5] found that people then become likely to believe untagged stories, even if they are also untrue, given that only a small percentage of posts are ever tagged as disputed.

Twitter allows users to report accounts that attempt to impersonate a brand or person. It also suggests users use its muting option to block offensive words and phrases, as well as tweets from strangers and new accounts. Critics say this sidesteps the problem of false content.

In 2019, YouTube undertook efforts to retool its detection algorithms and was able to reduce watch time of what it calls "borderline content" by 70%. YouTube is also putting authoritative news content at the top of viewers' feeds.[6]

The COVID-19 pandemic has raised the stakes for internet companies working to reduce the spread of fake news. Twitter changed its policies to remove tweets that run the risk of causing harm or panic, as well as tweets advising ineffective treatments for the virus. Facebook, which reported in March 2020 that more than half of the articles read on its site were about COVID-19, updated its algorithms to promote official accounts and remove false content. It's also banning ads for items like face masks, hand sanitizer and virus test kits that are prone to gauging. Google banned coronavirus-related apps from its smartphone store and ads from people trying to profit from the pandemic.

[5] Peter Dizikes, "The catch to putting warning labels on fake news," *MIT News*, 2 March 2020, http://news.mit.edu/2020/warning-labels-fake-news-trustworthy-0303.

[6] Julia Alexander, "YouTube claims its crackdown on borderline content is actually working," *The Verge*, 3 December 2019, https://www.theverge.com/2019/12/3/20992018/youtube-borderline-content-recommendation-algorithm-news-authoritative-sources.

Fact-checkers join the fight

Over the last decade, news organizations have taken on many initiatives to help the public distinguish between truth and fiction, such as fact-checking sites and guides to spotting fake news. With the coronavirus outbreak, many added special coverage to debunk fake news. NewsGuard created the Coronavirus Misinformation Tracking Center, which lists dozens of sites spreading false information about the virus. Websites like factcheck.org, Snopes and PolitiFact allow the public to verify information before sharing it or flagging it as dubious content. The International Fact-Checking Network supports more than a hundred projects in 40 countries, helping to surface common positions across fact-checkers.

More governments legislate against fake news

Many countries have started to introduce legislation to protect the public from fake news, even though champions of a free press worry legitimate reporting may be stifled under these types of laws. Some also set up task forces and media literacy campaigns. Italy created an online portal where citizens can report fake news to the police. A German law aimed at hate speech forces social networks to remove "obviously illegal" posts within 24 hours.

Several Asian jurisdictions have enacted laws that criminalize creating or spreading fake news. Fake news posts about COVID-19 have led to arrests in Mainland China, Hong Kong, Malaysia, India, Indonesia, and Thailand. Singapore's 2019 law against online falsehoods requires social media outlets to tag posts with government warnings saying they contain misinformation.

Businesses step up efforts to protect themselves

Corporate public relations departments have long tracked news stories about their organizations, but now companies are expanding surveillance to include social media and websites known to traffic in false stories. There are now service providers that collect content from a wide range of sites to identify misinformation and send alerts to their subscribers.

Fighting fake news requires data and technology

Fears of fake news during the US 2020 election season and the COVID-19 pandemic have put increased pressure on internet companies to block fake news. News organizations are working to educate the public on techniques for spotting fake news. But the deluge has been so overwhelming that fact-checking sites like Snopes told its readers in March 2020 it was unable to keep up due to resource constraint. The failure to control fake news, despite increased efforts, shows the need for better methods to detect fake news.

Enhancing human review with machine learning

One common approach adopted by social media companies relies on humans (users, employees or contractors) to flag potential false content. A major limitation to human review is that flagging is subject to personal bias. Nor is it practical given the large volume of information in the media in today's digital era. Inevitably, the use of artificial intelligence (AI) has come into focus in the fight against fake news.

A common AI-based hybrid approach builds on two classification models: content and social context. Content model analyzes topic distribution within the news article. However, the model itself is rarely used on its own because relying on content alone makes it difficult to differentiate intentional deception from bias. The content model often is complemented by the social context model, which focuses on key aspects of social network (e.g., followers, user characteristics, interaction and engagement history). The drawback of this approach is that analysis is performed based on the news content only. The limited scope can make it difficult to understand the broader context of the news and potentially, the type of fake news.

Another approach championed by MIT focuses on news sources. Researchers from MIT's Computer Science and Artificial Intelligence Lab and the Qatar Computing Research Institute developed machine learning models to assess the authenticity or neutrality of news sources. The drawback of this approach is that while certain facts in an article may be fabricated or embellished, the overall point of the article may still be authentic.

A new way of thinking

In examining the fake news problem, it may be worthwhile to learn from government counterespionage efforts. Open source intelligence (OSINT) is a key element of the government's counterintelligence strategy. OSINT refers to any information that can be legally gathered from free, public sources. The information can be about an individual or an organization.

Given its reliance on freely available data, OSINT can be compromised if an individual or organization falsifies information in the public domain. However, this can be addressed by cross-checking relevant pieces of information about an individual to look for inconsistency. For example, by starting with an author's social media information to find out about his/her work history, one can then use the work history to search the employer website and court records to verify the author's online profile. Given the vast scope of data covered in OSINT, extensive cross-checking can be done to minimize the risk of false information.

The detection methods as described in earlier parts of this paper will continue to serve as the foundation for fake news analysis. But by bringing in additional data from OSINT, particularly data outside of what is in the news content, we can greatly increase the scope of analysis, aided by machine learning and natural language processing technologies. The outcome is much more comprehensive insights that can be used to determine the authenticity and nature of news content, whether fake or not.

Using OSINT, an EY team has run through a series of tests using known misinformation. The preliminary results have shown very encouraging opportunities in commercializing this approach in organizations' fight against fake news.

Organization-wide planning is important

While fake news has existed throughout history, modern digital life has significantly amplified the issue and the harm it can do to our society. Both the public at large and businesses need to step up their efforts to proactively look for new ways to detect and contain fake news, while making sure they don't contribute to the problem in the same time.

Key actions to manage the risk of fake news

- Build a culture of integrity, compliance and ethics. If your organization has a reputation for ethical behavior, it stands to be damaged less by false claims of wrongdoing.
- Develop a crisis management plan for dealing with potential risks that can result from damaging fake news. Stress test the plan in worst case scenarios.
- Strengthen employee education and build vigilance on detecting, transmitting, and reporting fake news.
- In addition to traditional news outlets, monitor social media and fake news sites to flag potentially damaging coverages.
- Develop data-driven detection programs through innovative use of OSINT and AI technologies.

For more information, visit: ey.com/Forensics

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. 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
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

The views of third parties set out in this publication are not necessarily the views of the global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.

EYG no. 001603-20Gbl
WR #2003-3460064
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

The spy in our pockets

How location tracking is raising the stakes on privacy protection

EY
Building a better working world

Authors:

Meribeth Banaschik

Partner, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Germany

Kristina Miggiani

Senior Manager, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Germany

Introduction

Our attachment to smartphones has made them the perfect devices to track our movements – providing invaluable data to businesses and governments. Little do we know that many apps on our phones allow location data companies to pinpoint how we spend our days. A *New York Times* investigation was able to use a data set to track the movements of individuals commuting to their offices, picking up their children at school and even breaking their routines to go on a job interview.[1]

Rising concern over location tracking is just one example of how protecting privacy is becoming increasingly complex. COVID-19 is exacerbating the issue as governments and businesses experiment with new technologies to track and contain the outbreak. These efforts are saving lives, but they also raise fears about intruding on privacy and exposing personal health data.

Privacy management is often seen as the responsibility of compliance and legal professionals, aided by the cybersecurity team. But more and more organizations are realizing that privacy is impacting stakeholders in just about every corner of the organization. Managing privacy risk brought on by location tracking requires a concerted effort that also includes human resources, operations, information security, communications and investor relations.

[1] Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *The New York Times*, 19 December 2019, www.nytimes.com.

Privacy claims for location tracking subject to public and regulatory scrutiny

Did you know that having a weather app on your phone could mean your personal movements are tracked second-by-second and sold to third parties, even when you're not using the app? That's the basis of a 2019 lawsuit filed by the Los Angeles City Attorney's office. The suit charges that the information on selling data to third parties was hidden in the privacy policy and privacy settings sections of the app, which "the vast majority of users" don't read.[2]

Many companies that collect location data claim it doesn't violate privacy because the data is anonymous, users consent to be tracked, and data is kept securely. But the *New York Times* investigation shows these claims don't always hold up to legal or regulatory scrutiny. For example, pings showing a daily route from a house to an office easily identify a person.

While phone apps supply much of the tracking data sold to third parties, cellular companies are also under fire. The four largest US cellphone carriers promised to stop selling location data in 2018, but two years later, the U.S. Federal Communications Commission (FCC) proposed hundreds of millions of dollars in fines because the carriers were found to continue selling customer data and violating agency rules to protect personal information.[3]

[2] Eriq Gardner, "All the Time and Money on California's New Privacy Law Wasted?" *The Hollywood Reporter*, 15 June 2020, www.hollywoodreporter.com.

[3] Drew FitzGerald and Sarah Krouse, "FCC Probe Finds Mobile Carriers Didn't Safeguard Customer Location Data," *The Wall Street Journal*, 27 February 2020, www.wsj.com.

COVID-19 raises the stakes for location tracking

The COVID-19 crisis led some governments to launch phone apps with geolocation tracking to trace an individual's contacts and to determine whether they are complying with quarantine and social-distancing directives. Tracking individuals has helped some countries limit the virus's spread, but a Guardsquare security analysis of 17 government tracking apps found the "vast majority" are easy for hackers to breach.[4]

Human rights groups are concerned these apps are too invasive and could be used beyond the pandemic. For example, Norway's Data Protection Authority banned its country's tracking app after determining it collected far more data than needed.[5]

Businesses are also exploring new technologies to protect the health of their employees, using smartphone apps, cameras or wearable Bluetooth devices to monitor employee movement at work. If an employee tests positive for COVID-19, the company can quickly identify employees who came close to the infected worker. While many countries allow employers to track employees during work hours, privacy advocates fear surveillance could be extended around the clock and continue long after the crisis ends.

The pandemic has also raised privacy concerns with employee health data. An IAPP-EY survey published in May 2020 found nearly a quarter of businesses have taken their employees' temperatures, and 60% keep records of those diagnosed with COVID-19. Nearly one in five provided the names of COVID-19-positive employees to other staff or government authorities, contrary to the advice from the European Data Protection Board.[6]

4 Grant Goodes, "The Proliferation of COVID-19 Contact Tracing Apps Exposes Significant Security Risks," 18 June 2020, www.Guardsquare.com.

5 Scott Ikeda, "After Being Ranked Among the World's Most Privacy-Invasive, Norway Suspends Use of Contact Tracing App," *CPO Magazine*, 2 July 2020, www.cpomagazine.com.

6 Müge Fazlioglu, "Privacy in the Wake of COVID-19: Remote Work, Employee Health Monitoring and Data Sharing," IAPP-EY report, May 2020, https://iapp.org/resources/article/iapp-ey-report-privacy-in-wake-of-covid19.

Privacy regulations aim to control location tracking

The rising interest in protecting privacy has led to new regulations around the world. One of the most influential statutes, the General Data Protection Regulation (GDPR) of the EU, treats location data as personal data. This means users must specifically and freely agree to location tracking, rather than opting out. Google's lead data regulator in Europe launched a new investigation in 2020 after complaints that Google manipulated users into providing their location data. Google says it's constantly working to improve user controls and transparency.[7]

Location tracking is also addressed by the California Consumer Privacy Act (CCPA), which the state began enforcing in July 2020. Under the CCPA, California residents can opt out of having their personal information, including geolocation data, sold to third parties. While the law covers only state residents, many large firms are extending its rights to all Americans. California's attorney general estimates businesses will spend more than US$55 billion to comply with the CCPA.[8]

If your company sells location data, consider adhering to these GDPR requirements:

- Ask in clear and simple terms for freely given, specific and informed consent for location data, rather than simply requiring users to opt out.
- Clearly inform customers what types of location data you will process, what it will be used for, how long you will keep it and whether it will be sold to third parties.
- Before engaging third parties, review their ability to secure data properly and meet GDPR requirements.

7 Natasha Lomas, "Google's location tracking finally under formal probe in Europe," *TechCrunch*, 4 February 2020, www.techcrunch.com.

8 "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," prepared for California Department of Justice Office of the Attorney General, August 2019, dof.ca.gov.

Addressing privacy risks from location tracking requires cross-functional collaboration

Addressing privacy risks related to location tracking goes beyond the scope of legal and compliance departments. It requires flexibility and agility as organizations respond to fast-evolving technological and regulatory environments. Cross-functional collaboration is essential as it impacts a wide range of stakeholders. Legal and compliance professionals should take the lead in working with other functions — particularly IT departments — to help them identify, monitor and mitigate risks. Businesses need to keep privacy concerns in the forefront as they develop products or services that involve location tracking features. Talent management should focus on employee education and communication so that when used, location tracking doesn't compromise employees' privacy and its objective is well understood by employees. Information security and technology professionals need to stay on top of the rapidly evolving technologies to understand their impact and potential risks. Above all, privacy by design should be woven into the organizational culture.

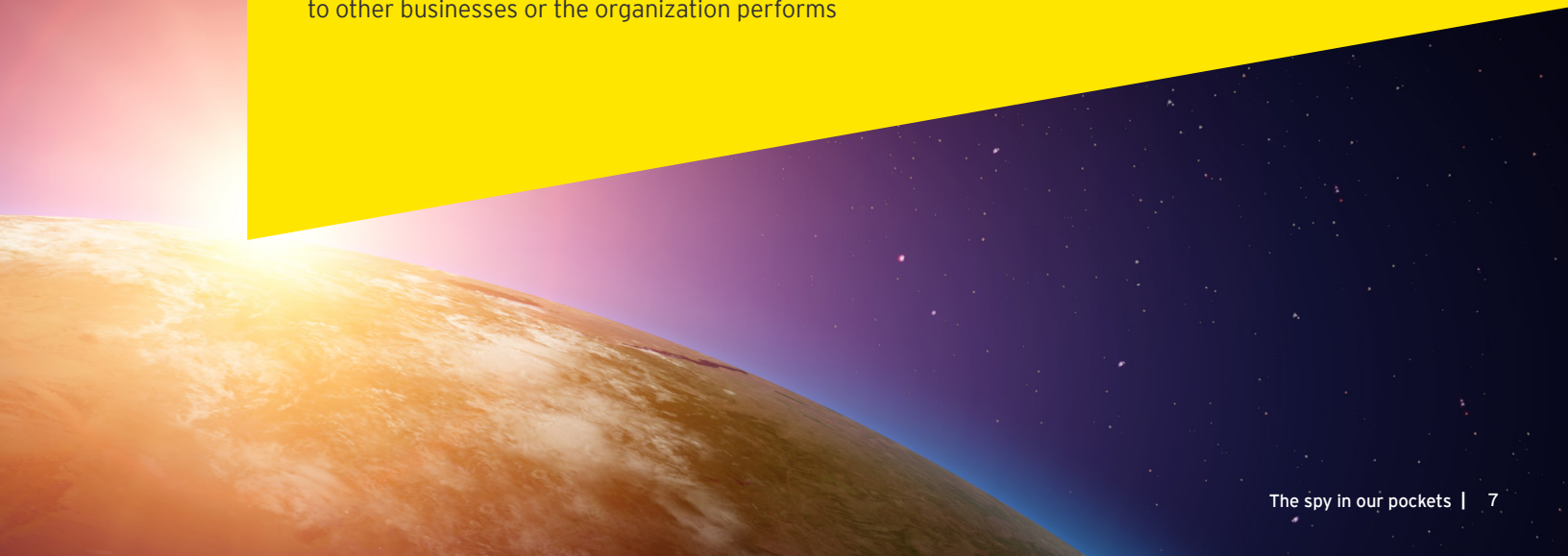
If not managed well, location tracking can become a huge liability that runs the risk of regulatory noncompliance, lawsuit, reputation damage, employee discontent and revenue loss. If managed well, location tracking can enhance product capability, boost service delivery and protect employees and the organization.

Key takeaways

Location tracking is becoming an important privacy concern, as it is increasingly used in many software applications that dominate our daily personal and business lives. The COVID-19 pandemic has heightened the issue as governments and organizations race to contain the spread of the virus. Businesses that hastily made operational changes during the pandemic, such as tracking employee movements or sharing personal health data, need to carefully evaluate their impact on privacy.

Compliance professionals should work collaboratively across the enterprise to mitigate risks around location tracking, whether the business markets data to other businesses or the organization performs location tracking on employees for internal purposes. These risks can result in regulatory and legal actions, data breach, employee morale and privacy concerns, as well as damage to the brand.

Adhering to data privacy regulations can be expensive and challenging. But businesses that manage location tracking activities transparently and securely will discover a competitive advantage as privacy protection becomes more important for both consumers and employees. We may love our phones but we don't want them spilling our secrets.



EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting 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
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

EYG no. 005657-20Gbl
WR #2007-3544685
ED None

ey.com