In Collaboration with Deloitte

WORLD ECONOMIC FORUM

Global Technology Governance Report 2021: Harnessing Fourth Industrial Revolution Technologies in a COVID-19 World

INSIGHT REPORT

DECEMBER 2020

Cover: Getty Images

Contents

Foreword

The Fourth Industrial Revolution will play a key role in ensuring our recovery from the pandemic and the avoidance of future crises.

William D. Eggers
Center for Government Insights Executive Director, Deloitte, USA

Ruth Hickin
Strategy and Impact Lead, World Economic Forum

The emerging technologies of the Fourth Industrial Revolution have a vital role to play as we recover from the COVID-19 pandemic and rebuild our economies. While these technologies can help drive enormous social breakthroughs and economic value, they can also potentially be misused.

An essential consideration for governments, businesses and civil society is how these technologies are harnessed and regulated to accelerate growth, encourage innovation and build resiliency. How governments and other stakeholders approach the governance of Fourth Industrial Revolution technologies will play an important role in how we reset society, the economy and the business environment. Working together, the public and private sectors have the opportunity to nurture the development of Fourth Industrial Revolution technology while mitigating the risks of unethical or malicious uses.

With this in mind, the Forum worked with Deloitte to produce a practical handbook to examine some of the most important applications of Fourth Industrial Revolution technologies if we are to thrive in a post-pandemic world and the governance challenges that should be addressed for these technologies to reach their full potential.

Harnessing and disseminating the technologies

The collaboration is part of a larger World Economic Forum platform, the Great Reset, that explores how, as the world undergoes a great reset, our ability to harness and disseminate the new technologies of the Fourth Industrial Revolution will play a key role in ensuring our recovery from the pandemic and the avoidance of future crises. The world will be a different place because of the pandemic and the vast technological change that will have taken place. The possibilities of new Fourth Industrial Revolution technologies, deployed appropriately, should be used as the baseline to reinvent the way we operate in the new context: everything from government services, education and healthcare to the way business interacts with and provides value to its customers.

Key insights

Our analysis revealed common challenges across the five Fourth Industrial Revolution technologies we focused on: artificial intelligence (AI); mobility (including autonomous vehicles); blockchain; drones; and the internet of things (IoT). These challenges include a lack of regulation, misuse of technology and challenges in addressing cross-border differences. For instance, one estimate suggests that bitcoin accounts for more than 90% of ransomware payments.[1] And the lack of effective regulation of facial recognition technologies coupled with incidents of misuse by law enforcement agencies have caused a backlash against this technology throughout the world.[2]

We profile a series of innovative governance and regulatory frameworks across the five Fourth Industrial Revolution technologies highlighted to address these and many other challenges. For example, Singapore's AI governance framework can assist the private sector by providing guidelines on internal governance, human involvement, operations management and stakeholder communication.[3] In Japan, the Financial Services Agency has accorded the Japan Virtual and Crypto Asset Exchange Association (JVCEA) the status of a self-regulatory body for the country's crypto exchanges – recognizing the private sector's role in providing effective governance.

Non-profit organizations are playing their part, too.[4] For instance, the United Nations Economic Commission for Europe facilitated a forum at which China, the European Union, Japan and the United States came together to develop a framework to harmonize autonomous vehicle regulations.[5]

This technology governance report aims to help governments, innovators and other stakeholders understand the current opportunity. The pandemic and its aftermath have accelerated the urgency of addressing current gaps with effective governance frameworks. Fourth Industrial Revolution technologies can play a major role in helping us emerge from the pandemic stronger than ever before. With these practical insights and examples, we hope that governments and industry can collaborate and foster innovation while providing effective governance. The study will enable conversations across a broad cross-section of stakeholders to partner on technology governance globally. The Forum looks forward to collaborating with public and private organizations to develop and deploy Fourth Industrial Revolution technologies responsibly.

Executive summary

The global technology governance outlook for 2020 and 2021.

This study examines some of the key applications of Fourth Industrial Revolution technologies for thriving in a post-pandemic world, as well as the complications of governance that may need to be addressed for these technologies to realize their maximum potential.[6] The report:

Describes governance gaps for each of the technologies. These include issues of privacy, liability, cross-border regulatory discrepancies and the potential for misuse by bad actors – such as the recent surge in ransomware attacks enabled by cryptocurrencies such as bitcoin or the risk of abuse posed by technologies like "deepfake" videos.[7]

How can regulatory agencies ensure the unrestricted flow of data necessary for many new technologies to operate robustly and efficiently while still safeguarding user privacy? Is facial recognition technology enough of a boon to police investigations to offset its potential for error and abuse? How vulnerable are IoT devices such as smart speakers and home cameras to hacks that put consumer data at risk?

Explores governance and oversight needs highlighted by the pandemic that should be addressed. These include balancing the need for human supervision of automated technology with the advantages of touchless operations in a post-COVID-19 world or assuaging consumers' privacy fears surrounding contact-tracing apps.

Profiles innovative government frameworks that may suit these future economic engines and outlines some emerging post-pandemic approaches. Finland, for example, requires private innovators in the transit sector to make certain data standardized and publicly available, which has enabled cities such as Helsinki to create an application that integrates both private and public modes of transport and enables users to plan and book a multimodal trip from start to finish using one interface.[8]

Countries such as New Zealand have introduced guidelines that incorporate privacy, human rights and ethical concerns into the design of government algorithms.[9] The pandemic has also increased public-private coordination, as in the United Kingdom, which formed a taskforce of pharmaceutical companies, regulators and academics to facilitate the rapid development of COVID-19 vaccines.[10]

Details many of the regulatory innovations in technology necessitated by the pandemic and explores whether or not they should become permanent. Regulatory agility, for example, has become increasingly important in the COVID-19 era, as governments ease restrictions to accelerate the development of new treatments and technology – such as autonomous delivery drones – to address the pandemic.[11] In other cases, governments have adjusted regulations based on user feedback or created experimental sandboxes that allow the private sector to test out new technology in a closed environment.[12]

> **COVID-19 has accelerated our transition into the age of the Fourth Industrial Revolution. We have to make sure that the new technologies in the digital, biological and physical world remain human-centred and serve society as a whole, providing everyone with fair access.**
>
> Klaus Schwab, founder and Executive Chairman of the World Economic Forum

Introduction

Efforts to recover from COVID-19 have triggered a tsunami of innovations in work, collaboration, distribution and service delivery – and shifted many customer behaviours, habits and expectations. Several of the emerging technologies of the Fourth Industrial Revolution – for instance, artificial intelligence (AI), mobility (including autonomous vehicles), blockchain, drones and the internet of things (IoT) – have been at the centre of these innovations and are likely to play a dominant role in what emerges post-pandemic. These technologies power applications that are themselves revolutionary, creating a self-reinforcing cycle that spins like a flywheel, surging on its own momentum.

AI and data analytics have helped Taiwan predict the risk of infection.[13] China has used drones and robots to minimize human contact.[14] The United Arab Emirates (UAE) is using blockchain to provide seamless digital services to its citizens,[15] and the United States is using autonomous vehicles to deliver test samples to processing labs.[16] Many countries are employing mobile apps as sensors for contact tracing.[17]

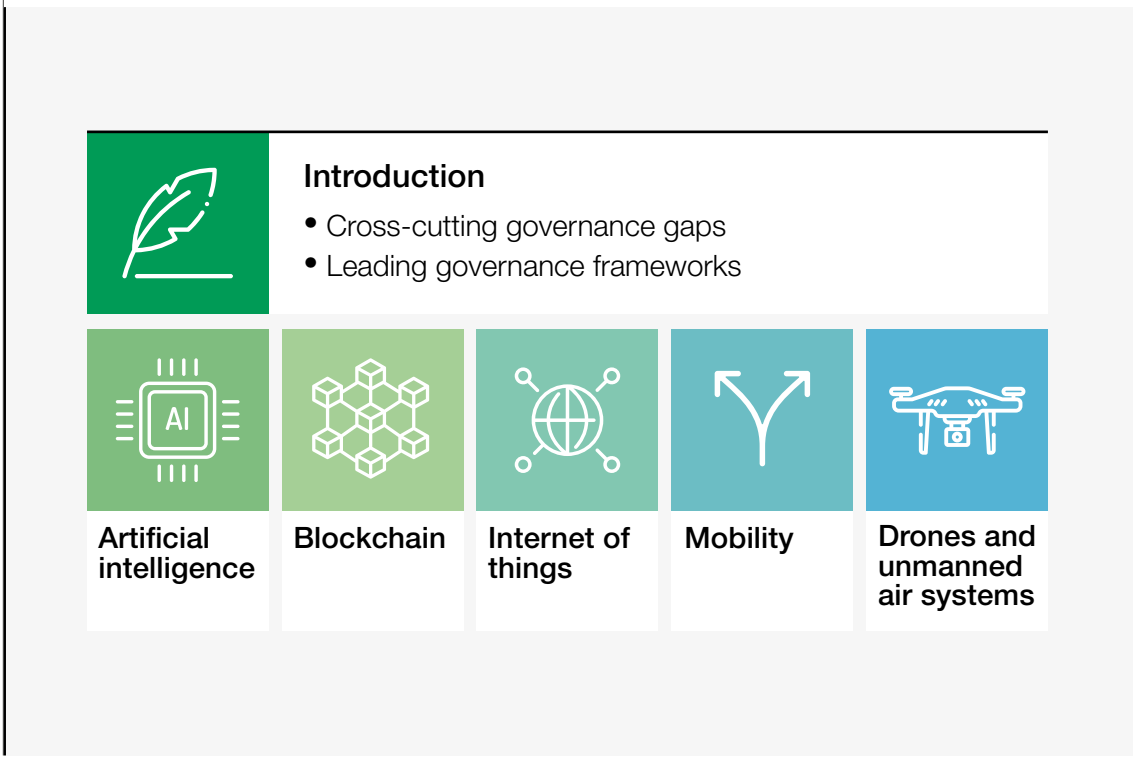
While these emerging technologies have the potential to drive enormous social breakthroughs and economic value, they also have the potential to lead to adverse and unintended consequences. An essential consideration for governments, businesses and civil society is how these technologies can be harnessed appropriately to maximize the benefits and mitigate potential risks or misuse.

Good technology governance, policies and norms are foundational to realizing the benefits of technology while minimizing its risk. The challenges to getting this right are clear: new technologies and business models of the Fourth Industrial Revolution do not fit easily into the frameworks regulators have traditionally used to supervise markets. They evolve rapidly, cross traditional industry boundaries, devour data, defy political borders and benefit from network effects when they share information. In the Fourth Industrial Revolution, old conceptions of regulatory siloes no longer apply.

AI does not quite fit into existing regulatory frameworks. International blockchain ledgers may violate current national financial laws. Drones and IoT have the potential to cause privacy concerns. Autonomous vehicles may transform traditional assessments of safety risks. All of these disruptions translate into a suite of technologies and capabilities poised to slip through gaps in governance.

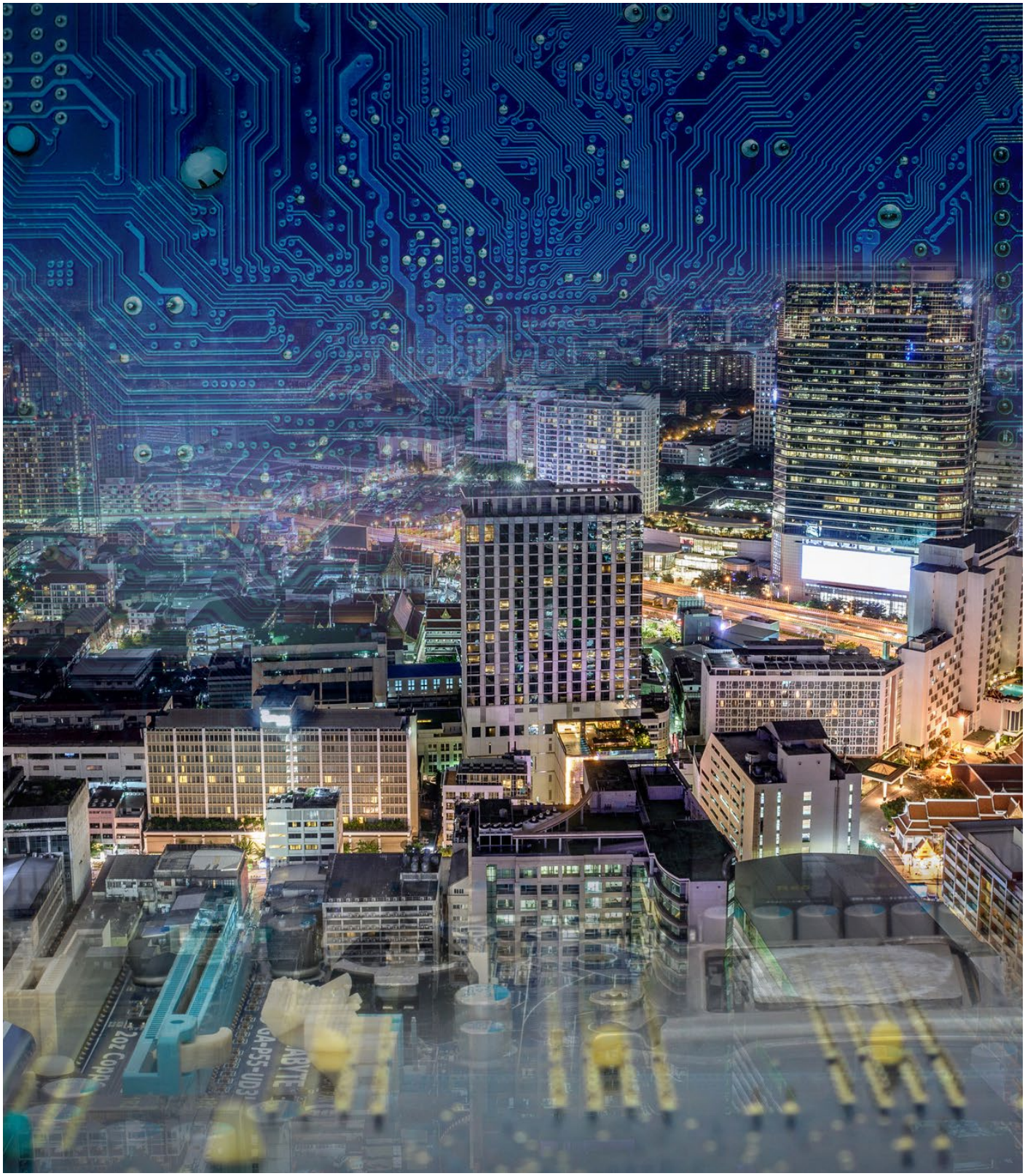
Governing these new technologies will require new principles, rules and protocols that promote innovation while mitigating social costs. Public-private collaboration will be crucial to making the right choices for future generations. A faster, more agile approach to governance is needed to

FIGURE 1 **Visual map of the report**



effectively respond and adapt to the ways these technologies are changing business models and social interaction structures – both seen and unforeseen. Such governance is not only a matter of supervision and regulation from government but also encompasses a wide range of frameworks such as multistakeholder approaches, self-regulation, non-binding guidance standards, certifications and non-profit guidance.

This study does not attempt to provide a complete landscape analysis of emerging technologies. Instead, it examines the opportunities and complications of governance for a set of Fourth Industrial Revolution technologies: artificial intelligence (AI), mobility (including autonomous vehicles), blockchain, drones and the internet of things (IoT). It describes governance gaps for each, and innovative government frameworks that may suit these future economic engines and even help drive them forward. The study also examines some of the most important applications of Fourth Industrial Revolution technologies if we are to thrive in a post-pandemic world.[18]



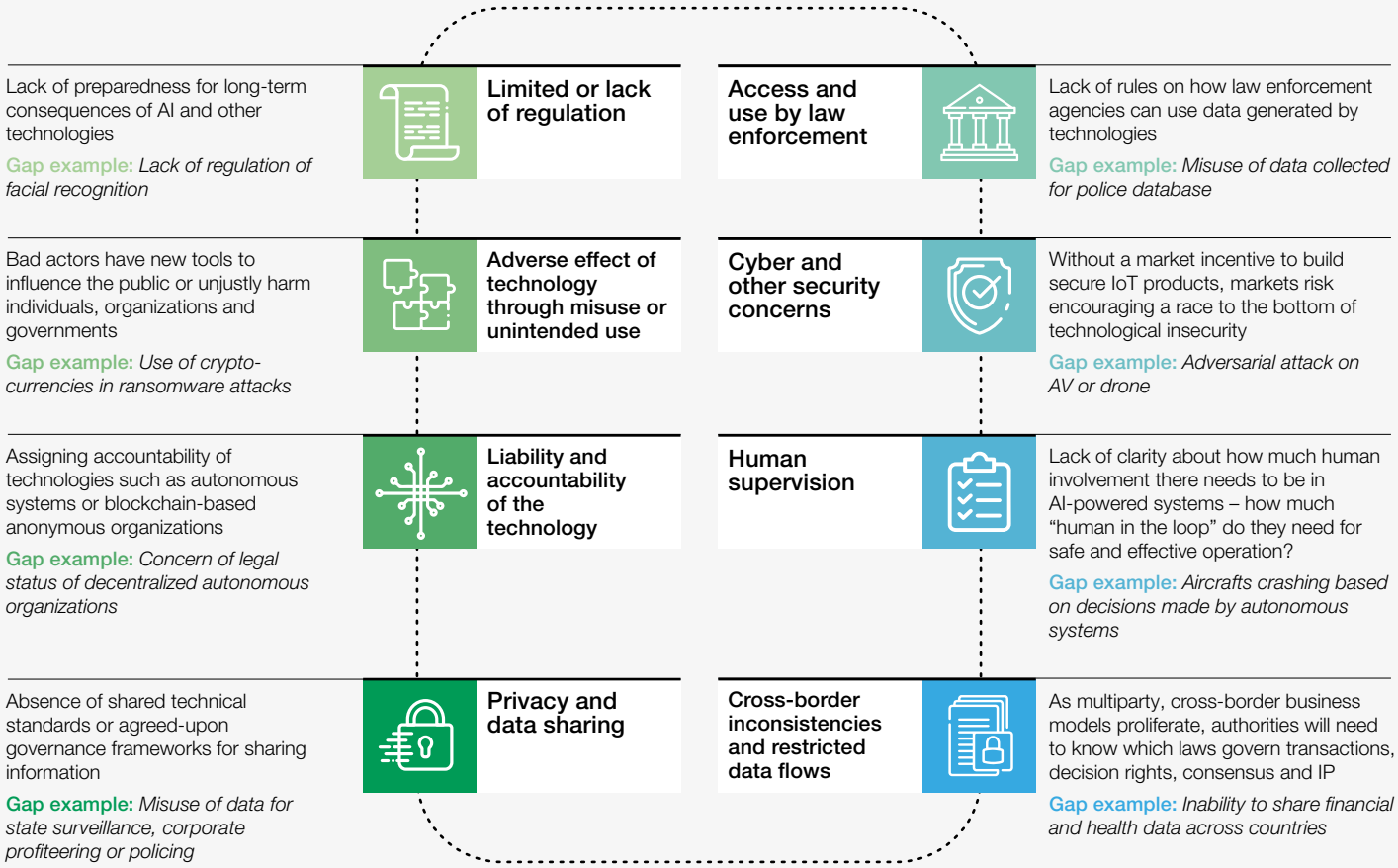
1 Cross-cutting technology governance gaps

Common themes across gaps in technology governance.

From drones to IoT, each individual technology presents its own unique set of governance challenges, many of which will be detailed in subsequent chapters of this study. But our analysis also revealed a host of common challenges across the five Fourth Industrial Revolution technologies on which we focused. While many predated COVID-19, the pandemic and its aftermath has accelerated the urgency of addressing them. These challenges include:

- Limited or lack of regulation
- Adverse effect of technology through misuse or unintended use
- Liability and accountability of the technology
- Privacy and data sharing
- Access and use by law enforcement
- Cyber and other security concerns
- Human supervision
- Cross-border inconsistencies and restricted data flows

FIGURE 2 **Cross-cutting technology governance gaps**



Source: Deloitte analysis

1.1 Limited or lack of regulation

In January 2020, Robert Williams, an African American man, was arrested in his driveway for a crime he did not commit based on a faulty match from facial recognition technology. He was detained for 30 hours before being released, according to The New York Times, which indicated he could be the first known American arrested due to a facial recognition mismatch.[19] Many regulatory bodies are unprepared for the legal consequences that could arise due to the use of facial recognition and other transformative technologies – much less any ethical ones.

These challenges persist in drones, blockchain, IoT and other technologies. Blockchain-enabled smart contracts, for example, which instantly transfer funds based on sensors that mark the physical location of goods, enable deals – and business disputes – that are beyond current financial regulations.

IoT cybersecurity breaches – such as the Mirai botnet, which hijacked home cameras and other IoT devices, briefly shutting down the internet on the US East Coast – represent market failures, according to technologist Bruce Schneier, who detailed the event in testimony to the US Congress.[20] Because consumers and governments lacked the expertise to demand security features, device manufacturers did not have a strong incentive to do anything beyond producing hardware quickly. The result was a vast array of unsecured IoT devices that fell easy prey to hackers.

1.2 Adverse effects of technology through misuse or unintended use

Technology that creates opportunities for growth and innovation also often creates opportunities for misuse. In October 2019, hackers attacked the City of Johannesburg and demanded $30,000 in bitcoins under the threat of publishing sensitive data. One estimate from Coveware suggests that bitcoin accounted for more than 90% of ransomware payments made globally in the first quarter of 2019.[21] Further, the anonymous nature of blockchain has made it difficult to identify the culprits who raised money through initial coin offerings (ICOs) and then ceased operation of their companies.[22]

Algorithms are very valuable for society. They enable us to withdraw cash from ATMs, increase agricultural yield, prioritize environment remediation and even save lives. However, without effective governance, algorithms can have adverse and unintended consequences. Algorithms play a role – and at times falter – in job interviews, educational institutions and even medical care. One elderly woman, suffering from cerebral palsy, was perplexed to see her care hours reduced to 32 hours from 56 hours per week. It was later discovered that Medicaid's algorithm had a coding error for the disease and her hours were restored.[23]

Those are just some of the dangers of AI's intended uses. AI trained using videos can create so-called "deepfakes", in which politicians, celebrities or news anchors can be made to appear as if they have said things they did not. Authoritarians need only muddy the waters with conspiracy theories to delegitimize real news and protect themselves from the consequences of outrageous truths – now bad actors have yet another new tool to influence the public or unjustly discredit individuals, organizations and governments.

At the distribution end, deepfakes pose a question of how much responsibility platforms take for the content they distribute, and their obligation to their users – both users who wish to misinform and those seeking a less hostile product.

1.3 Liability and accountability of the technology

When autonomous systems make decisions, it can be difficult to assign accountability for their actions. What if a drone crash damages a building? What if medical software misdiagnoses a disease?

Consider the case of a crashed autonomous vehicle. Responsibility could conceivably fall on the vehicle manufacturer, the software designer, the owner or the occupant. Legal systems will have to sort out these questions, a process that can be far less messy if legislators are prepared. Even for vehicles equipped with aircraft-like "black boxes", it may be near-impossible to deduce why an autonomous vehicle system made a specific decision.[24]

Blockchain enables other technologies to take consequential actions without human input. Decentralized autonomous organizations (DAOs) are digital entities that function through pre-coded rules – in effect, organizations run by code. These entities are largely self-sustaining, requiring little to no human input. Their primary mission is to execute smart contracts and record activity on the blockchain.[25] DAOs present some of the most pressing governance gap issues for blockchain. Whereas in the ordinary course of business it is usually clear that a corporation is a corporation and a partnership is a partnership, questions remain about how DAOs are categorized.[26] Other issues include security and the immutability of a DAO's code, once written.[27]

1.4 Privacy and data sharing

Privacy concerns will emerge in any field that collects personal data, and COVID-19 has brought those concerns to the fore. According to a survey, 71% of Americans said they would not download contact-tracing apps, with most citing privacy concerns.[28]

IoTs, embedded in many public utility assets or mobile apps, can generate a trove of personal information – especially in homes equipped with smart devices – and have been used to spy on estranged spouses, friends and relatives.[29]

Meanwhile, AI can provide personalized experiences to customers. However, to do so, some organizations have intruded on people's privacy by collecting personal information on an unprecedented scale.[30]

But looking at data only through a privacy lens is too narrow an approach to tackle this challenge. Regulators and lawmakers should protect privacy while also encouraging data sharing to ensure that technologies meet their potential. For example, as mobility technology grows increasingly complex, with an array of new entrants and services – ride-hailing, carsharing, microtransit, bikeshare, e-scooters, real-time traffic maps and integrated trip planners, to name a few – existing alongside well-established modes of transport such as underground railways and buses, there are many opportunities to share data. Consumers, public authorities and private companies can all share key data in order to fully benefit from these new technologies, but at present there is little in the way of shared technical standards or governance frameworks to regulate how such information can be dispensed.

Access and use by law enforcement

> Inaccurate use or misuse of technology can heighten systemic racism and affect the human rights of marginalized groups.

The issue of data sharing and access is particularly pronounced in law enforcement. Applications of AI, such as facial recognition, feed heightened concerns that private information could be misused for surveillance, border control and policing.[31] Most governance frameworks do not currently advise law enforcement agencies on how they can use the data generated by technologies such as IoT and drones. Can police interrogate personal virtual assistants? Use crime scene details captured inadvertently by a delivery drone? Use AI to scour mobile phone location data?

Such tracking of mobile phone location data through AI has led to discussions of surveillance potentially becoming a permanent feature of law enforcement post-COVID-19.[32]

Meanwhile, the use of facial recognition by law enforcement agencies has come under increased scrutiny in the wake of racial justice protests in the Western world.[33] Inaccurate use or misuse of technology can heighten systemic racism and affect the human rights of marginalized groups. One study, for example, concluded that facial recognition algorithms misclassified Black women up to 35% of the time.[34]

In the UK, 237 police officers had been disciplined for misusing law enforcement databases and accessing personal data as of November 2019.[35] As such technology proliferates, so will data collections, and with them, further opportunities for misuse. To increase trust in these technologies – and law enforcement – governments should determine how to balance the privacy of residents with lawful access to data.

1.5 Cyber and other security concerns

COVID-19 has been linked to a whopping 238% rise in worldwide cyberattacks against the financial sector between February and April 2020.[36] In the US, meanwhile, cyber breaches increased by 50% for hospitals and healthcare providers between February and May.[37] The World Health Organization (WHO) has additionally witnessed a fivefold rise in cyberattacks.[38]

The more potent the technology, the more dangerous its misuse. Hackers who access AI-based systems can modify decisions or outcomes – an adversarial attack could trick a combat drone into misclassifying a crowded civilian space as an enemy; or autonomous vehicles could be hacked to create gridlock. Multiple strategies can deliberately alter AI-powered systems.[39]

Adversarial attacks range from data poisoning (altering training data for machine-learning algorithms) to tricking image recognition systems (altering digital images or modifying physical objects). The impacts of these types of attacks could range from influencing a search algorithm to recommending a specific company's product to causing a self-driving vehicle to ignore a street sign or, in a worst-case scenario, to killing people by targeting a missile at the wrong place.

These vulnerabilities extend beyond AI. Criminals with access to sensitive healthcare data, such as a person's history of mental health issues or an HIV diagnosis, could intimidate individuals, discriminate against certain groups or create bioweapons. Such data could also be used to blackmail assets for military intelligence or industrial espionage.

Cyber risks are particularly acute for IoT devices, which often have inadequate security protection. A public-private working relationship with an organization focused on advancing the safe commercialization of evolving technology could be an effective model for quickly and efficiently establishing the baseline of transparency required for IoT security.

1.6 Human supervision

Should AI-powered systems be used only to augment human action and judgement, or should they also be used to power autonomous systems? There is considerable debate about when and how much human involvement AI-powered systems need for safe and effective operation. COVID-19 has added another dimension to this discussion as organizations around the world strive to minimize human touch to tackle the pandemic.

“ Technology creators are becoming increasingly confident in their products’ ability to work with minimal human involvement.

Aircraft have crashed and ships have broken down due to decisions made by autonomous systems.[40] This is why, when testing an autonomous vehicle, a back-up human driver may need to be ready to take control if there is a risk of an accident. However, expecting a passive passenger to suddenly become a driver may not be the safest option. These cases indicate that there may be a need for more human involvement in some cases, but in others it can be counterproductive. For instance, a sensor-enabled thermometer that requires a human touch to get the thermometer closer to the body of an individual would be counterproductive in current times; organizations may prefer a fully autonomous system to measure temperature.

Technology creators are becoming increasingly confident in their products’ ability to work with minimal human involvement. This will create questions about where exactly in the decision process humans should insert themselves. The Israel Aerospace Industries’ Harpy is an autonomous weapon used to attack radar installations without human permission or guidance.[41] The dangers are clear: an AI arms race could ensue, while proliferation risks AI weapons being acquired and deployed in asymmetrical warfare.

1.7 Cross-border inconsistencies and restricted data flows

Emerging technologies such as AI and blockchain transcend national boundaries, further complicating the regulation process. Data and privacy laws change from nation to nation, ranging from no-touch regulation to restrictive systems, which increases both the difficulty – of designing an effective blockchain, for example – and the risk that existing technologies will be non-compliant.

Further, many countries have restrictions on data sharing, especially related to finance and healthcare.[42] However, data is a vital ingredient for technologies such as AI autonomous vehicles and blockchain, and restricting its flow can inhibit the growth of data-dependent fields.

Likewise, blockchain’s multiparty and cross-border architecture ceases to function effectively when under the control of different nations’ regulatory positions. Regulatory stances on cloud adoption, national open application programming interface (API) standards, cybersecurity requirements and health information all vary from country to country.[43] As multiparty, cross-border blockchain business models proliferate, authorities will need to be well versed in the various laws governing transactions, decision rights, consensus and intellectual property (IP).

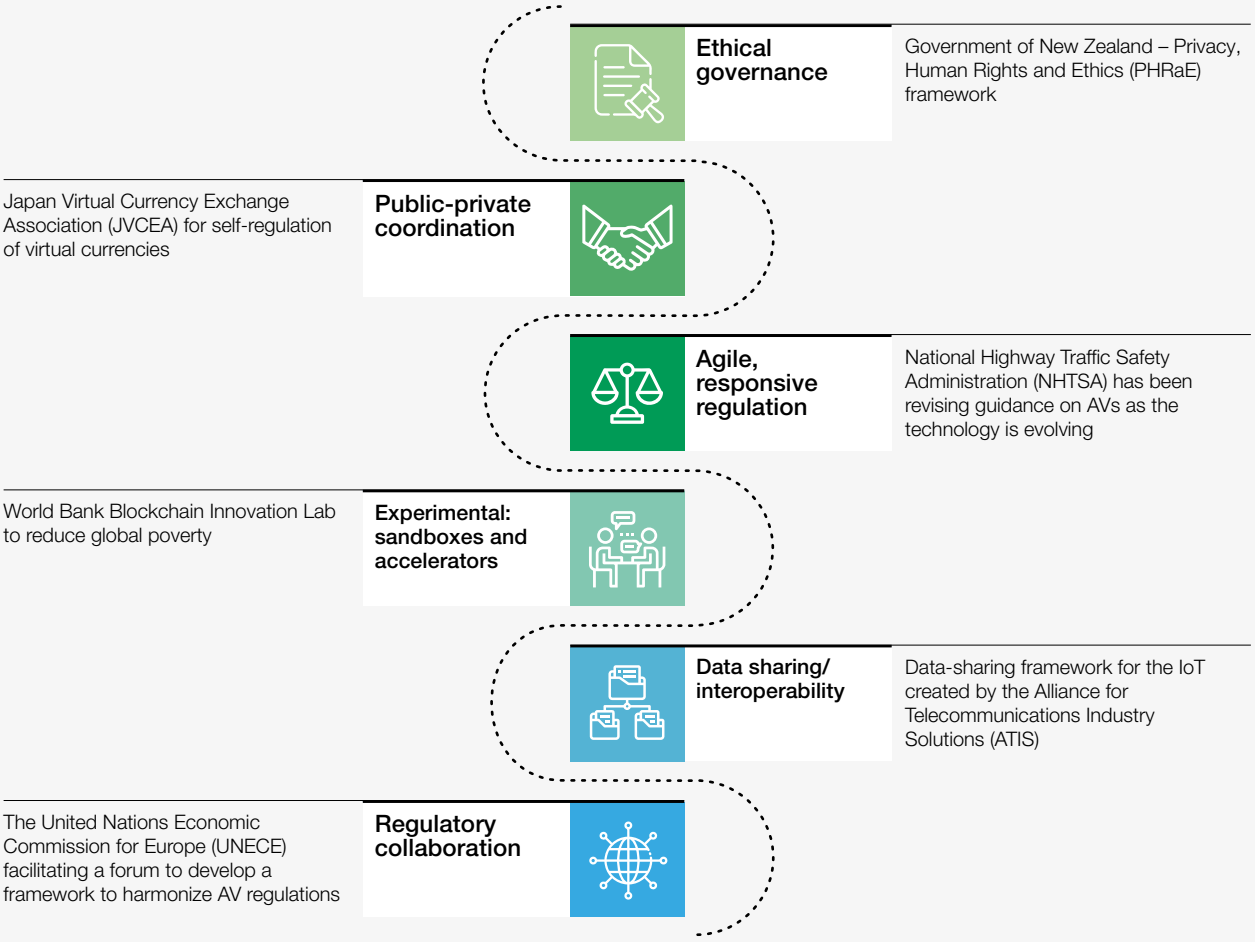
As these new technologies continue to evolve, regulators should anticipate their needs and risks. While it’s not always possible to get ahead of evolving technology, it is possible to prepare.

2 Innovative governance frameworks

New and emerging ways to regulate technology to maximize the benefits and avoid potential risks.

To address these and other challenges, innovative governance and regulatory frameworks are emerging to support the technologies of the Fourth Industrial Revolution. These are detailed in the chapters focused on particular technologies. Additionally, our analysis found a number of common themes across the areas of technology discussed in this report.

FIGURE 3 **Innovative governance frameworks**



Source: Deloitte analysis

2.1 Ethical governance

Many countries have developed ethical governance frameworks that provide guidelines on how to develop emerging technologies responsibly. In 2017 and 2018, the New Zealand Ministry for Social Development and Tim Dare, an independent university ethicist, published materials to incorporate privacy, human rights and ethics into the design process of government algorithms. Their framework is an iterative process that covers the entire life cycle of a project.[44] In 2020, New Zealand also published the Government Algorithm Charter to provide a set of principles guiding the use of algorithms and data by government agencies. Close to two dozen government agencies have committed to the charter.[45]

In 2019, the UK government's Facial Recognition Working Group released an interim report on ethical issues relating to the use of real-time facial recognition for policing. Their report also outlines a set of nine "ethical principles to inform the use of live facial recognition", including public interest, effectiveness and the avoidance of bias and algorithmic injustice.[46] The European Commission, in coordination with other European agencies and member states, has released guidelines and a toolbox for designing and developing COVID-19 contract-tracing apps. The guidelines stress the need to be compliant with the General Data Protection Regulation (GDPR) and the ePrivacy Directive.[47]

2.2 Public-private coordination

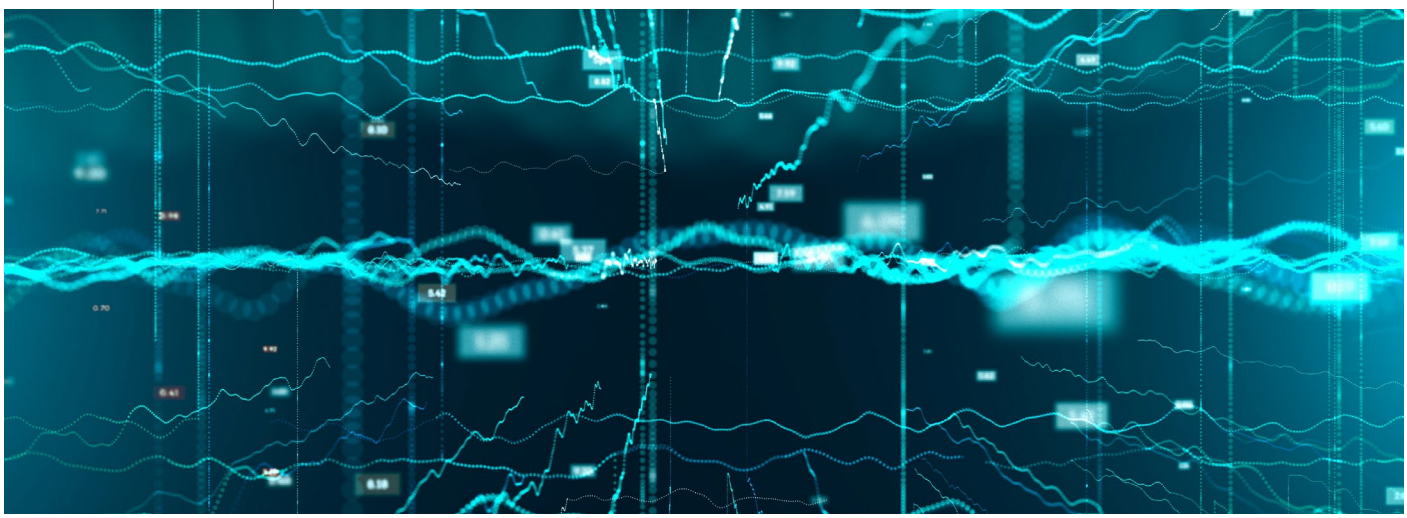
Governments need to protect the public from harm and provide stewardship for new technologies, while companies need to take responsibility for their social obligations. The public and private sectors should collaborate to achieve both – using mechanisms such as multistakeholder engagement, co-created regulation and, where appropriate, self-regulation.

For example, the Financial Services Agency (FSA), Japan's financial regulator, has afforded the country's cryptocurrency industry official status to self-regulate and police domestic exchanges ahead of other countries. The public-private body is authorized to establish binding guidelines on behalf of the cryptocurrency industry, including rules for local trading platforms and accurate reporting of transactions.[48] To enhance transparency, the self-regulatory body periodically releases data on trading volume and the value of cryptocurrencies.[49]

Similarly, community-led effort BetterIoT has launched an online self-assessment tool that evaluates a connected product on various dimensions including privacy, licensing provisions and interoperability.[50] Its workshops in Europe are designed to increase awareness of privacy and ethics for IoT.[51]

A major theme across the technology areas is the significant degree to which regulators are engaging with the private sector and other stakeholders as they craft approaches. For example, an industry working group and Federal Aviation Administration (FAA) regulators have proposed the remote identification rule, a framework for remote identification of all drones operating in the airspace of the United States. Widespread use of drones for package delivery or flight in densely congested airspace would be largely impossible without such a drone ID.[52]

Public-private coordination has also become more evident than before in various governments' responses to COVID-19. For example, the UK formed a taskforce of pharmaceutical companies, regulators and academics to facilitate the rapid development of vaccines for COVID-19.[53]



2.3 Agile, responsive regulation

Typically, regulations are not "future-proof". They tend to be prescriptive in nature, take months or years to enact, require the review of extensive public comments and stay rigid once created. In contrast, technologies of the Fourth Industrial Revolution are often developed in agile sprints, beta tested on early adopters and swiftly updated. A traditional regulatory approval process for a drone-delivered AI defibrillator, for example, would not keep pace with the evolution of the technology. Traditional regulatory approval would tend to regulate technology slowly so that, by the time it is approved, the technology itself is outdated.

For innovation to thrive, agile and responsive regulation will be crucial in the post-pandemic world. Business models are changing rapidly, and regulators will need to keep pace with these changes without stifling innovation.[54]

This could mean regulation that, like an agile process, checks its effectiveness against user feedback. For example, the National Highway Traffic Safety Administration (NHTSA) issued its guidelines for autonomous vehicles in 2016. Since then, based on feedback from industry participants, the guidelines have been revised and iterated four

times as AV technology has evolved.[55] A similar regulatory agility is visible in how governments have responded to COVID-19, such as when India's Ministry of Health and Family Welfare (MoHFW) announced guidelines in response to COVID-19 that allow registered medical practitioners to deliver services via telemedicine.[56]

In certain cases, agile and responsive regulation can also mean giving more leeway to low-risk products and services. The European Aviation Safety Agency (EASA) has divided drone regulations into three categories based on the risks they pose. The regulatory framework identifies drone operations as: open (low risk); specific (medium); and certified (high risk). Low-risk drones that do not fly beyond the line of sight would not require any formal authorization, while high-risk drones are subject to the same rules as the manned aircraft with which they share airspace.[57]

The city of Lisbon exhibits responsive regulation in its approach to new transit technologies. For "greenfield" innovation, where outcomes are unclear but there is a potential upside, the city focuses more on "soft" regulation and guidance. For "brownfield" innovation, where the risks are better known, the city may instead adopt "hard" regulation. Lisbon's evolving approach to e-scooters provides an illustrative example. Initially the city took a hands-off approach and nine companies entered the city within one year. As the process evolved, a forum was created in which both the city and the operators meet and discuss the changes that must be put in place to address the potential problems and risks that arise. The city has also announced the first-ever corporate mobility pact, in collaboration with several private-sector partners, to accelerate sustainable urban transformation.[58]

The World Economic Forum's project on Agile Regulation for the Fourth Industrial Revolution is supporting governments around the globe to adopt more agile, experimental and collaborative approaches to regulation.

2.4 Experimental: sandboxes and accelerators

Sometimes regulators simply observe the consequences of a new technology in the safety of an isolated environment. This environment, called a sandbox after the closed operating system researchers use to observe computer viruses, provides enhanced regulatory support and enables firms to test their models and develop proofs of concept. In this way, regulatory structures can also emulate a start-up accelerator by deliberately encouraging innovation. In April 2020, the Financial Conduct Authority of the UK launched a digital sandbox for financial organizations experimenting with innovative business models and products to tackle the pandemic.[59]

Many countries are piloting sandbox approaches for drones. Sandboxes in India, Malawi, Japan and the US have had success in moving from pilot to scale across the country. Malawi's sandbox was the first in Africa established to test the use of drones for humanitarian purposes such as delivering medical supplies.[60] In the US, the Department of Transportation and the FAA conducted a pilot study with 10 public-private partnerships to test unmanned aerial systems.[61] "The pilot programs will test the safe operation of drones in a variety of conditions currently forbidden," said Elaine Chao, Secretary, Department of Transportation. "These include operations over the heads of people, beyond the line of sight and at night."[62]

"The pandemic has also highlighted the role drones can play in moving medical supplies, minimizing human contact and supplying essentials to remote areas.

The pandemic has also highlighted the role drones can play in moving medical supplies, minimizing human contact and supplying essentials to remote areas. In April 2020, the UK Civil Aviation Authority admitted a drone operator to the sandbox to test beyond visual line of sight (BVLOS) operations in shared airspace.[63]

Meanwhile, Digital Jersey, a government-backed economic development agency and industry association in the Channel Islands, has launched an IoT sandbox for the island.[64] Like other sandboxes, it relaxes legal barriers in order to encourage businesses to test new ideas.[65] The sandbox is open to businesses outside of Jersey as well. A Swiss company tested the model of a "flying weather station" in which a drone embedded with sensors collects atmospheric data that can be used to forecast weather and develop other innovative services.[66]

2.5 Data sharing/interoperability

Since many technologies rely on data to refine their operations – especially those employing AI and data analytics – more data should mean better results. Rapid advances in facial recognition software show what deep pools of quality data can produce and shed light on the kinds of revolutionary outcomes that sharing data on cancer treatments or carbon emissions could produce. But in many countries, this type of data is very sensitive information, hampered by differing rules across borders, and sometimes stored in formats that are incompatible.

Countless initiatives across the globe focus on how to vastly accelerate improved data sharing within ethical guardrails. The Alliance for Telecommunications Industry Solutions (ATIS), a standard-setting body, created a framework for IoT to promote data sharing, data exchange marketplaces and public-private partnerships among smart cities.[67]

Meanwhile, revisions to Finland's Transport Code require public transport operators to make certain data (timetables, routes, ticket prices) available via open APIs. Now commuters in cities such as Helsinki can plan, book and pay for trips using multiple public and private modes via a single application interface.[68]

2.6 Regulatory collaboration

Because emerging technologies permeate national boundaries – while also giving rise to second- and third-order effects rippling out from innovation – regulating them calls for collaboration among agencies within a country (escaping regulatory siloes to gain a whole-of-relevant-government approach) as well as cross-border collaboration.[69]

"To operate effectively on a global scale, companies need a standard framework and guidelines at the international level.

To operate effectively on a global scale, companies need a standard framework and guidelines at the international level. The fintech sector has seen some regulatory convergence in the past few years, with more than 60 bilateral cooperation agreements finalized since 2016.[70] The Global Financial Innovation Network (GFIN) is a network of 50 organizations, mostly financial regulators, that enable firms to test their products and services in other countries via a global fintech sandbox.[71]

International bodies also have a vital role to play in setting global standards to avoid regulatory divergence. For instance, the United Nations Economic Commission for Europe (UNECE) facilitated a forum in which China, the EU, Japan and the US came together to develop a framework for harmonizing autonomous vehicle regulations.[72] As a result, more than 50 countries across Europe, Africa and Asia have agreed to binding rules on Automated Lane Keeping Systems that will come into force in January 2021.[73]

When faced with rapidly adapting technologies, regulators must also learn to swiftly adapt. These governance frameworks describe the various ways in which they have achieved that goal and helped nurture propulsive technologies while mitigating unexpected fallout. Just as these technologies blur international borders, they also entangle the border between public and private. This presents a serious challenge. But pioneering public-sector innovators are learning that with creativity and forethought the sectors can work together to effectively govern Fourth Industrial Revolution technologies.

3 Research approach

The methodology to identify governance gaps and innovative frameworks.

The study followed three primary steps to identify and refine relevant governance gaps and governance frameworks. These steps were:

Step 1: Conducting a survey
A joint World Economic Forum-Deloitte survey was launched to help identify governance gaps and governance frameworks in each of the five Fourth Industrial Revolution technology areas analysed: AI, blockchain, drones, IoT and mobility. The survey was conducted with the Forum's network of collaborators and Deloitte's subject matter specialists between 8 January 2020 and 3 February 2020.

The survey asked about the most significant ways in which gaps in technology governance will manifest in the future, including which are the most impactful, emergent or unexpected gaps the world's leaders do not know about but should. The survey also asked about the most innovative ways in which government, industry and other key stakeholders are using governance today to maximize the benefits and minimize the risks of technology.

Step 2: Performing an extensive literature review
In the next step, research leaders from Deloitte and the Forum in each technology area conducted an extensive literature review to gather examples of governance gaps and governance frameworks. Overall, the report focused on bringing a diverse set of examples from different sectors, technologies and geographic areas to demonstrate the breadth and depth of gaps and governance frameworks.

Governance gaps were identified and used to illustrate the potential impact of such a gap, the scale at which such a gap is believed to exist and how that gap could affect investment and innovation. The criteria also included prioritizing gaps that seemed to lack effective governance and that have received little public attention.

The researchers also identified innovative case studies relating to the governance frameworks. Case studies were also selected based on the degree to which they are globally relevant, seem to have produced tangible outcomes or are currently being implemented.

Step 3: Finalizing gaps and frameworks
In the third and final stage, for each of the technology areas, a dedicated virtual working session was organized in which professionals from the Forum and Deloitte worked collaboratively to finalize their thoughts on the governance gaps and governance frameworks. The session also helped to classify the gaps into the three categories listed below. These categories were developed on the basis of input from the survey, a review of the relevant literature and the research team's experiences.

- **Now:** Gaps that governments and other organizations are starting to address in many instances. For these gaps, there is a general agreement that they do represent an issue.
- **Near:** Gaps that are known, but on which little or no action has been taken. Few countries or organizations are addressing these gaps and there is a lack of agreement in the community about the issue.
- **Next:** Gaps that are hypothetical or emerging and have a large degree of uncertainty associated with them.

4 Artificial intelligence

As AI technologies become more pervasive, efforts have increased to better govern their application in order to protect and benefit all in society.

As the use of artificial intelligence (AI) technologies becomes more pervasive, efforts have increased to better govern their application in order to protect and benefit everyone in society. As a general-purpose technological "tool", AI sits at a nexus of data privacy and security, human rights and equality, automation and job security, and universal economic development. If AI is not handled properly and with foresight, society risks missing out on the benefits the technologies could bring.

The COVID-19 pandemic has focused attention on the capability and limits of AI-powered systems as well as the risks of using such systems. There have been some promising applications of AI across a broad range of medical-related issues in the face of this current public health crisis. AI technologies have been helping with advanced patient care, drug discovery and vaccine development, contact tracing, predictive management of medical equipment and automated health consultations via chatbots.[74]

Facing new pressures and harsh economic realities due to the pandemic, many businesses and governments are increasing their focus on and investment in AI to help transform their operations. Many businesses are putting a greater emphasis on automation and improving efficiency across their organizations.[75] This can include enhancing their understanding of supply chains to better manage disruptions and using conversational AI to help augment overwhelmed customer contact centres.[76] In this environment, some governments have started to use AI-powered chatbots to handle the high volumes of pandemic-related unemployment claims.[77]

Even prior to the pandemic, most businesses were struggling with uncertainty about AI governance. According to Deloitte's State of AI in the Enterprise survey, a majority of global respondents agreed that their organization is slowing adoption of AI technologies because of the emerging risks.[78] Many are looking for guidelines and guardrails to help – 62% said that AI technologies should be regulated by the government. However, a majority also worry that too much regulation will potentially slow innovation.

This desire for guidance in conjunction with the accelerated deployment of AI technologies during the pandemic has elevated the need for discussions about ethics, matters of privacy and potential regulation.[79] To help provide some structure in relation to this fast-moving issue, numerous different frameworks, working groups and statements of principle have been developed by governments, professional organizations, policy groups and companies. They are looking to balance responsible use and technology innovation. Examples include the Global Partnership on Artificial Intelligence (GPAI), the EU's "Ethics Guidelines for Trustworthy Artificial Intelligence", and the Vatican's "Rome Call for AI Ethics".[80]

We should begin to move beyond frameworks and guidelines and into more formal practice and policy. The global pandemic has afforded us a chance to do things differently. We can manage AI's risks head-on and set guidelines for the technology's principled use.[81] There are many different governance gaps relating to AI with which society is struggling – some well-known, others still revealing themselves. By identifying these gaps and recognizing good examples of how best to address them, we can realize the benefits of AI as the world recovers.

Governance gaps

Now

1. Low **AI literacy** among policy-makers
2. Issues with **bias, fairness, transparency and explainability**
3. Use of AI for **disinformation and digital manipulation**
4. **Data privacy and data rights** issues
5. A more **human-centric approach** to the development of AI-powered systems

Near

6. Use of **lethal autonomous weapons systems** and a potential escalation in capabilities
7. Use of **adversarial AI** systems to conduct cyberattacks and disrupt other AI-powered systems
8. **Geopolitical technological competition** – AI systems reflecting different principles
9. AI-powered systems used in **surveillance** and the need for facial recognition safeguards
10. Ensuring the **equitable distribution of benefits** from AI systems across all of society

Next

11. **Concentration of power** arising from smaller numbers of AI-powered systems guiding greater numbers of decisions
12. **Impact on children's** cognitive abilities, behaviour and decision-making capabilities from long-term use of AI-powered systems
13. How to best manage **AI-powered autonomous and decentralized companies** or AI-led companies
14. Inadvertent, large-scale **technological unemployment** from widespread use of AI systems

Now gaps

1. **Low AI literacy among policy-makers:** Many technology and business leaders worry that there is a general lack of understanding of AI among lawmakers. A dearth of expertise could potentially lead to ineffective or potentially detrimental regulations. Regulators and lawmakers should be educated on the basics of AI and exposed both to positive examples and potential problems in order to form balanced views.

2. **Issues with bias, fairness, transparency and explainability:** AI is increasingly used to make important hiring, economic, medical and education decisions. However, an algorithm is only as good as the dataset used to train it. If a dataset is biased in some way, or not truly representative, the algorithm will reflect and propagate that bias. We have seen examples of potential algorithmic bias already in a number of cases. During the pandemic, in the rush to build new tools with new datasets, this issue has been a challenge.[82] Another consideration is that when an AI-powered system makes a decision or recommendation, it is sometimes important to understand how it came to its conclusions. Companies may need to be able to explain to their boards, investors and regulators how an AI-driven decision was made if problems arise.

3. **Use of AI for disinformation and digital manipulation:** There is a growing concern and debate over whether individuals are losing the capacity to determine what is real and what is made up online. Whether through false news stories, rumours and conspiracies or deepfake videos, there are those who want to unjustly discredit individuals, organizations and governments or influence the public. Part of the debate revolves around the balance between content moderation and free expression. For example, Facebook has been challenged to use its AI-powered content moderation systems to quickly stem the flow of COVID-related misinformation.[83] This problem is further exacerbated now that misinformation-as-a-service can be easily purchased via the dark web.[84]

4. **Data privacy and data rights issues:** There are numerous potential issues in terms of how the data that is used to train, develop and test AI-powered systems is collected and managed. Additionally, as we have seen during the pandemic, model drift is a concerning issue as the environment in which algorithms operate can change rapidly. This issue gets more complex given the broad array of disconnected data privacy legislation, data localization requirements and government strategies, including GDPR, CCPA, the "European Strategy for Data" and other proposed legislation (e.g. the Algorithmic Accountability Act in the US).

5. **A more human-centric approach to the development of AI:** It is important that individuals are always considered first when designing, building and deploying AI-powered systems. The Vatican's "Rome Call for AI Ethics" envisions "a future in which it is clear that technological progress affirms the brilliance of the human race and remains dependent on its ethical integrity".[85] The importance of interpersonal justice for public services and commercial transactions should be recognized. This can be as simple as notifying a user when a bot is communicating with a person or as complex as the increased use of affective computing techniques – when computer systems can interpret the emotions of individuals and react accordingly.

> The Vatican's 'Rome Call for AI Ethics' envisions 'a future in which it is clear that technological progress affirms the brilliance of the human race and remains dependent on its ethical integrity'.

Near gaps

6. **The pursuit of lethal autonomous weapon systems (LAWS) and a potential escalation in capabilities:** There is great debate over the regulation and potential banning of AI-powered weapons systems that require no human involvement to make a lethal decision. For example, the Israel Aerospace Industries' Harpy is an autonomous weapon used to attack radar installations without human permission or guidance.[86] The lack of a comprehensive international agreement could potentially cause a new arms race based around this set of emerging technologies. In addition, non-state actors may gain access to this technology to use it as a means of asymmetric attack.

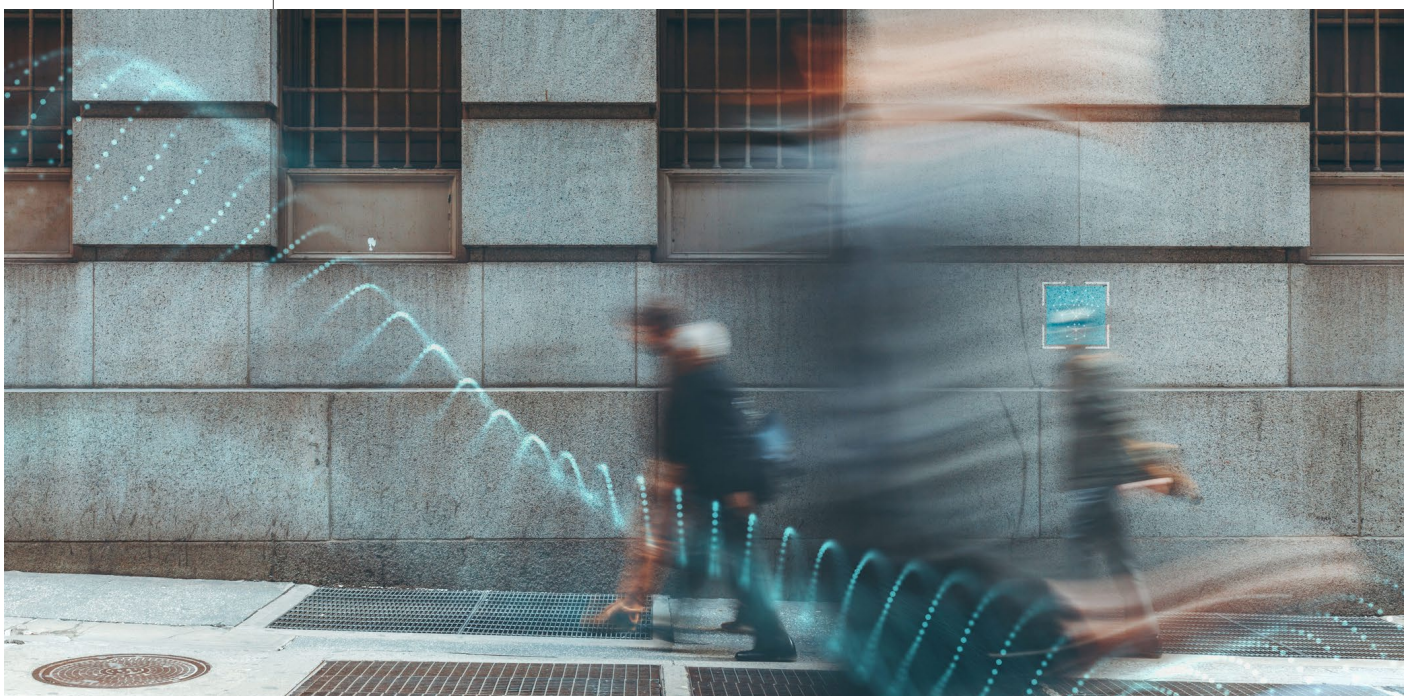
7. **Successful attacks on AI-powered systems jeopardizing safety and reducing public trust:** There is an increasing number of ways in which to deliberately alter the behaviour of AI-powered systems. Many types of adversarial attacks can be used, ranging from data poisoning (altering training data for machine learning algorithms) to tricking image recognition systems (by altering digital images or modifying physical objects). The impacts of these types of attacks could range from influencing a search algorithm to recommending a specific company's product to causing a self-driving vehicle to ignore a street sign. It is essential that AI-powered systems are secure

so that individuals or organizations cannot take advantage or game the system.

8. **Geopolitical technological competition between AI systems:** Many countries around the world see AI as a key economic enabler and source of competitive advantage for the future.[87] The leaders in AI research and development could significantly increase their influence and gain an advantage economically and militarily for decades.[88] Countries that are developing AI algorithms and systems all have different views and agendas and there is concern that the AI-powered systems produced will potentially reflect and spread certain principles to the detriment of others.

9. **The use of AI-powered systems or facial recognition for surveillance of individuals or groups:** Vast datasets can be used to better manage traffic patterns, conserve energy or identify individuals who may be at risk of disease. They can also be used to build profiles of individuals in order to eliminate or alter behaviour found unacceptable by governments or private entities. This can lead to systemic racism or the denial of rights based on the outputs of AI-powered systems. Because of this, IBM, Microsoft and Amazon have all recently altered their approach to facial recognition technology – abandoning some uses and technologies and placing a moratorium on others. Additionally, in the US, cities have now banned the use of facial recognition applications by government organizations and law enforcement and the federal government is pursuing similar action.[89]

10. **Ensuring the equitable distribution of benefits from AI systems:** There is the potential that the benefits of AI-powered innovation will not be shared equally across all levels of society, whether that is between people from different socioeconomic backgrounds or between developing and developed economies. Governments and businesses should not only consider fairness, trust and respect for human rights but also bear the principles of distributive justice in mind.



Next gaps

11. **A reliance on a small number of companies and their AI-powered algorithms could limit choice:** Governments, industry organizations and policy groups should be wary of fewer and fewer companies providing more and more of the AI-powered technology that drives decision-making in our society. This could potentially limit choice when it comes to economic, education, health and entertainment decisions. Could we get to a point at which society limits people to a decreasing number of solutions? Governance must ensure fair competition and prevent consumer lock-in.

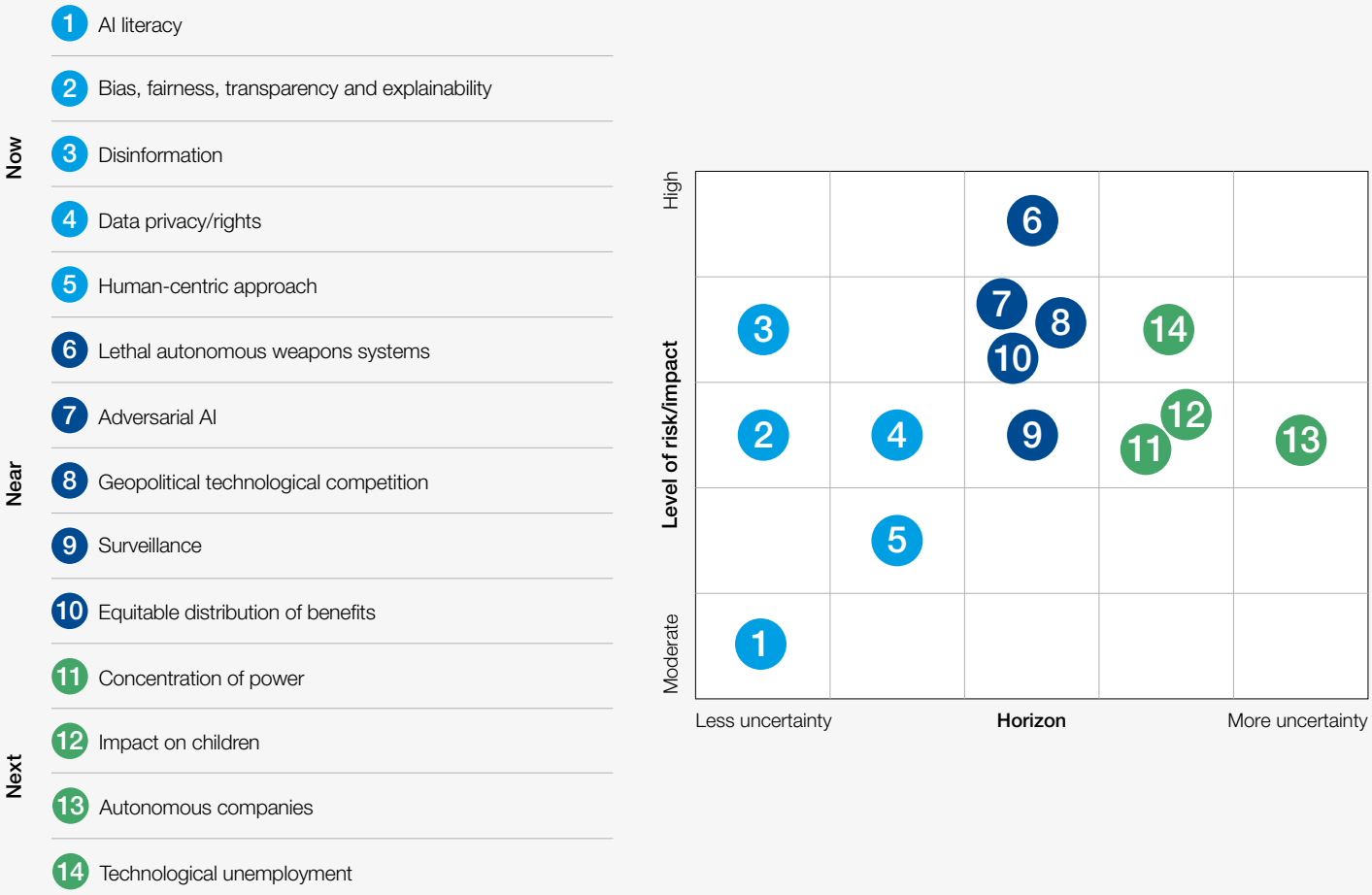
12. **Growing up alongside AI-powered technology may negatively affect how children make decisions as adults:** There is uncertainty about how exposure to AI-powered technology (e.g. voice-enabled assistants, smart toys) throughout early development may affect children – especially if they do not receive adequate education on how the technology works. How

will it change their relationship with technology? Will these children, as adults, give too much authority to AI-powered systems? What types of safeguards need to be put in place? Education about technical concepts and the social impact of AI will become increasingly important.[90]

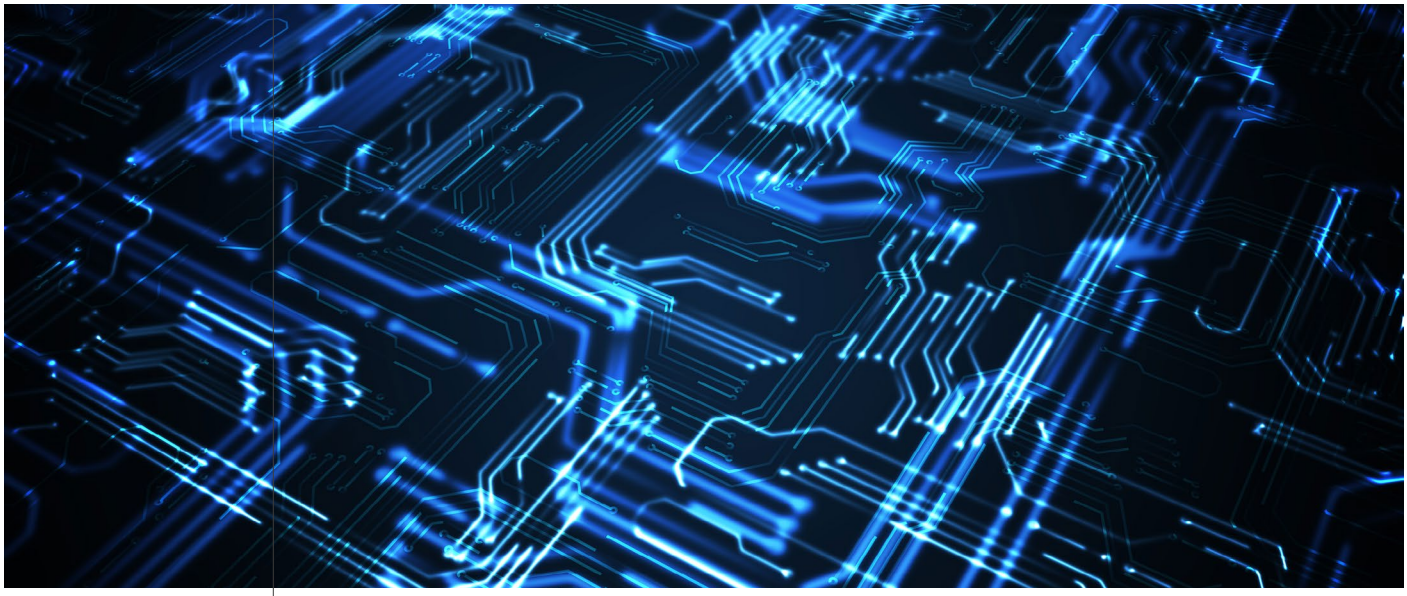
13. **How to best manage AI-powered autonomous and decentralized companies or AI-led companies:** AI-powered systems could become so advanced that they, combined with other emerging technologies (e.g. blockchain), could potentially run a company without any human intervention. Think algorithm-as-CEO. There may also be companies with very few human employees in which AI drives all of the major decision-making. How would these be regulated by financial institutions? How would they be viewed by investors?

14. **Large-scale technological unemployment from widespread use of AI systems:** The majority of organizations are not developing and deploying AI-powered systems for the express purpose of replacing workers. Most are looking to improve efficiency, enhance their current products and services, and speed up decision-making. However, as more and more AI-powered systems are deployed over time, we may see greater levels of gradual, inadvertent technological unemployment. There is widespread debate about the potential for and extent of AI-driven job loss and which industries and workers it may affect the most. In the wake of the COVID-19 pandemic, many companies are looking to blunt the economic impact by deploying even more automation technologies (e.g. physical robots, robotic process automation [RPA], AI systems etc.), potentially accelerating this issue.

FIGURE 4 **Time horizon and risk level of emerging governance gaps**



Source: Deloitte analysis



Sample innovative governance frameworks

1. **Canada's Directive on Automated Decision-Making**
   This directive, which took effect in April 2019, is meant to guide the Government of Canada in using "any technology that either assists or replaces the judgement of human decision-makers". It includes requirements such as algorithmic impact assessments, providing notice before and explanations after decisions, recourse options and reporting on the effectiveness and efficiency of systems. The directive is intended to be updated as technologies and their use evolve.[91]

2. **UNICEF's Generation AI programme – Memorandum on Artificial Intelligence and Child Rights**
   UNICEF's Generation AI programme is working with multiple partners to research the opportunities and challenges in relation to the responsible use of AI in order to safeguard child rights. As part of this programme, the Human Rights Center of the University of California, Berkeley School of Law developed a set of recommendations for educators, corporations, governments and parents.[92]

3. **Government of New Zealand – Privacy, Human Rights and Ethics (PHRaE) framework**
   In 2017 and 2018, the New Zealand Ministry of Social Development developed a set of materials with Tim Dare, an independent university ethicist, to incorporate privacy, human rights and ethics into the design process of government algorithms. The PHRaE framework is an iterative process that covers the entire life cycle of a project. It has broad government support and has been going through the testing and feedback process.[93] The Government of New Zealand is currently working with the Forum to advance the development of AI governance frameworks that are inclusive, promote trust and minimize risk while maximizing benefit.[94]

4. **Montréal Declaration for Responsible Development of Artificial Intelligence**
   In late 2018, the Université de Montréal released an ethical framework for the development and deployment of AI. It consists of a set of 10 principles, based on research and interviews with more than 100 diverse experts. They were guided by the principles of equitable, inclusive and ecologically sustainable development.[95]

5. **Finnish Center for Artificial Intelligence (FCAI) – AI education programme**
   In 2018, the University of Helsinki launched "The Elements of AI", a series of free online courses aimed at educating the layperson on the fundamentals of AI. It will soon be translated into every language in the EU, and could serve as a model for other public education efforts.[96]

6. **US Food and Drug Administration (FDA) – proposed regulatory framework for modifications to artificial intelligence/ machine learning (AI/ML)-based software as a medical device (SaMD)**
   Medical device manufacturers are increasingly using AI in their products. The US FDA is producing "a total product life cycle-based regulatory framework for these technologies that would allow for modifications to be made from real-world learning and adaptation, while still ensuring that the safety and effectiveness of the software as a medical device is maintained".[97]

7. **Government of Singapore – Model AI Governance Framework**
   In early 2020, the Government of Singapore's Personal Data Protection Commission (PDPC) released the second edition of its Model AI

> UNICEF's Generation AI programme is working with multiple partners to research the opportunities and challenges in relation to the responsible use of AI in order to safeguard child rights.

Governance Framework, intended to help the private sector. It covers internal governance, human involvement, operations management and stakeholder communication. The PDPC also provides use cases and an implementation and self-assessment guide.[98]

8. **IEEE – News Site Trustworthiness Working Group**
   Part of the Institute of Electrical and Electronics Engineers (IEEE) Global Initiative on Ethics of Autonomous and Intelligent Systems, this working group is developing a standard to help the public better determine which news stories are factually accurate and which are not. Using an open, automated system and a clear set of standards, they aim to rate internet news providers on several different factors.[99]

9. **UK government – Biometrics and Forensics Ethics Group, Facial Recognition Working Group**
   The Facial Recognition Working Group of the independent Biometrics and Forensics Ethics Group of the UK government released an interim report in 2019 on the ethical issues related to the use of real-time facial recognition for policing. Their report also outlines a set of nine "ethical principles to inform the use of live facial recognition", including public interest, effectiveness, the avoidance of bias and algorithmic injustice, and necessity, among others.[100]

10. **World Economic Forum – AI procurement guidelines**
    In 2019, the Forum released a collection of government procurement guidelines for AI. The 10 guidelines were developed to help governments, which might not have a high level of experience with AI yet, quickly bring the benefits of the technologies to the public sector. They include practices to align governments and AI providers on articulating needs, mitigating risks, managing data use and assuring accountability and transparency. Pilots using the guidelines are ongoing with the UK government, the Dubai Electricity and Water Authority and the Government of Bahrain.[101]

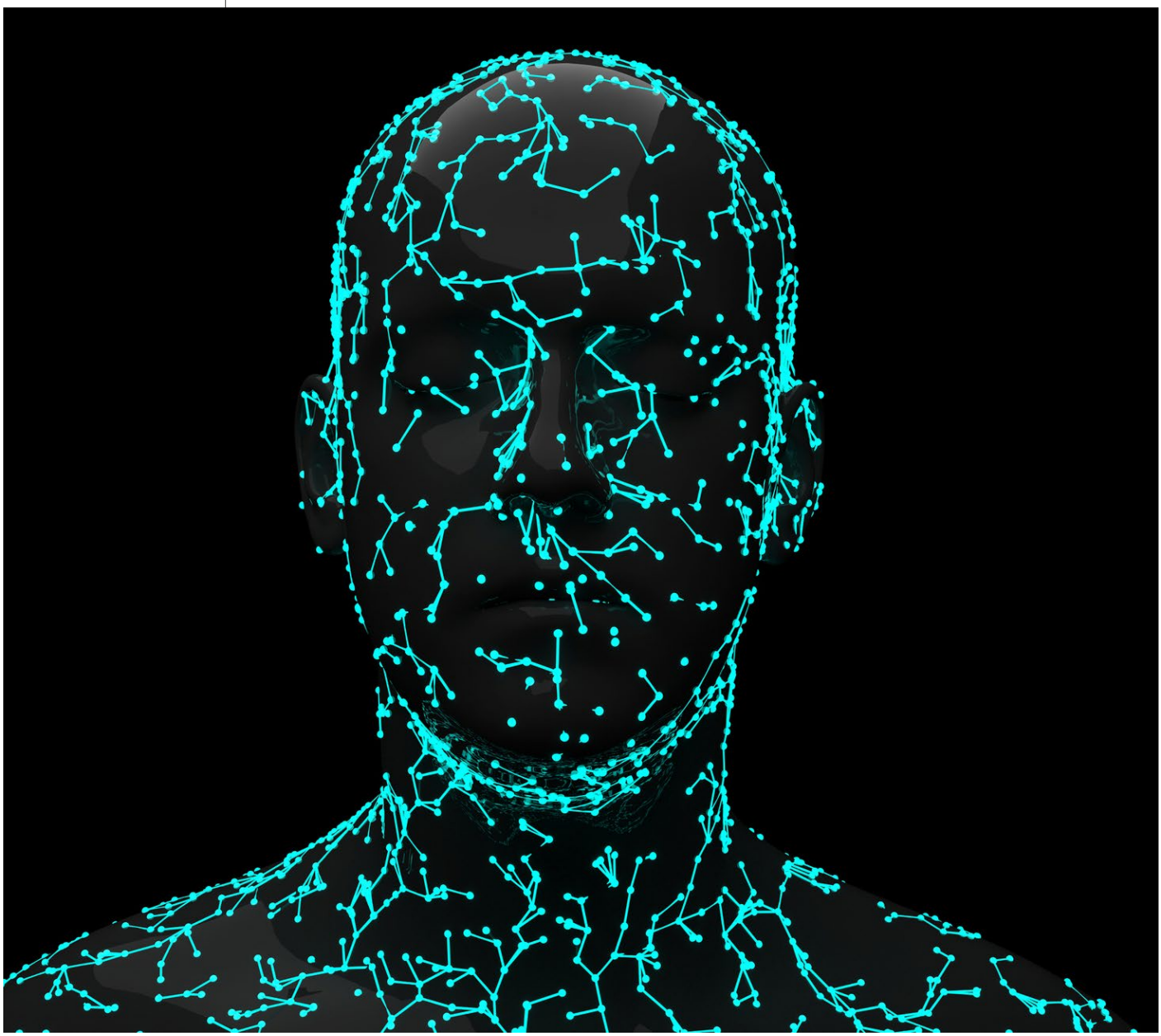


TABLE 1 | **Innovative governance framework criteria**

Framework	Agile	Fit for purpose	Globally relevant	Inclusive	Innovative	Evidence-based	Produced outcomes	Currently live
1. *Directive on Automated Decision-Making* (Canada)	●	●	●	●		●		●
2. *Memorandum on Artificial Intelligence and Child Rights*		●	●	●		●		●
3. Privacy, Human Rights and Ethics (PHRaE) framework (New Zealand)		●	●	●	●	●	●	●
4. *Montréal Declaration for Responsible Development of Artificial Intelligence*			●	●				
5. Finnish Center for Artificial Intelligence – AI education programme	●	●	●			●		●
6. FDA regulatory framework for modifications to AI/ML-based software as a medical device		●	●		●	●		
7. *Model AI Governance Framework* (Singapore)		●	●		●			●
8. News Site Trustworthiness Working Group					●			
9. Biometrics and Forensics Ethics Group, Facial Recognition Working Group (United Kingdom)		●	●	●	●			
10. AI procurement guidelines (World Economic Forum)	●	●	●	●	●			●

Source: Deloitte analysis

5 Blockchain

The pandemic has revealed limitations in the capacity of global infrastructure to respond to crisis – what role can blockchain play in future crises?

The pandemic has revealed limitations in the capacity of global infrastructure to respond to crisis. As the world economy embarks on its journey of recovery, new questions are emerging about the role that disruptive technologies may play in preparing global infrastructure to respond to the next crisis. Certainly, no technology – including blockchain and digital assets – can ever serve as a silver bullet in this regard. Despite challenges and a limited number of large-scale projects to date, the characteristics of blockchain and digital assets – such as their capacity to increase trust through transparency of transactions and the establishment of a "single source of truth" – may help in meaningful ways in the longer term.

"Blockchain's characteristic immutability and transparency of transactions as a "single source of truth" could increase trust in the accuracy of critical official data during a crisis.

For example, blockchain could offer the kind of auditability that ensures material provenance is completely traceable. The use of smart contracts – self-executing contracts that contain conditions embedded in code – could provide situational flexibility as supply chains experience changing circumstances. Blockchain's characteristic immutability and transparency of transactions as a "single source of truth" could increase trust in the accuracy of critical official data during a crisis. The proliferation of digital assets could also help facilitate stimulus payments and charitable giving during a crisis. The list goes on.

While blockchain and digital assets may not serve as an immediate solution in the current crisis, initiatives in development could illustrate the potential of the technology for future crises:

- Supply-chain optimization: Blockchain can be deployed to drive collaboration between diverse actors in the supply chain. BunkerTrace, a joint venture between Blockchain Labs for Open Collaboration (Bloc) and Forecast Technology, is a collaborative blockchain solution that tracks marine fuel.[102] Collaborative ecosystem solutions such as these may one day lessen the stress placed upon supply chains during a crisis, especially during its early stages.[103]
- Central bank digital currency (CBDC): Mastercard has recently announced a tool to evaluate the efficacy of a CBDC under varying test conditions.[104] According to reports, many central banks are considering issuing a digital currency, including China's digital Yuan CBDC project, although no central bank has issued a digital currency at scale yet. Anticipated benefits include greater efficiencies in government services such as tax collection or stimulus payments. We will discuss current CBDC initiatives – including China's CBDC trials – later in this paper.[105]
- Blockchain-based global remittances: Global remittances represent an important part of support for families across the globe – especially during times of crisis. According to the World Bank, remittances to low- and middle-income countries (LMICs) reached a record high of $554 billion in 2019, with a predicted 20% decline in 2020 due to COVID-19.[106] Currently, money transfer operators (MTOs) – entities that work with banks to facilitate transfers – often face high transaction fees, technical limitations and regulatory ambiguity. These challenges can be exacerbated during a period of crisis. Some have proposed blockchain as a solution to overcome such challenges in developing countries. Standard Chartered has launched a blockchain-based remittance system, now in commercial testing; it uses blockchain technology to create a real-time, distributed payments network across a digital banking platform, using the remittance provider's technology software and a Chinese blockchain technology application. The system enables Bangladeshi ex-pats in Malaysia to transfer remittances to their home country without the limitations of the more labour-intensive traditional approach – in essence increasing transparency and allowing funds to be distributed at speed.[107]

Governance gaps

Now

1. **Cybersecurity in a blockchain world**
2. **Regulatory fragmentation** in terms of digital identities, assets and cryptocurrencies
3. Technical **interoperability and the need for standards**
4. **Consortia** governance
5. Enforceability of **smart contracts**

Near

6. **Data integrity**
7. **Cross-border regulatory** inconsistencies
8. **Audit/third-party guidance** in a blockchain context
9. **The preservation and challenge of anonymity** in an immutable blockchain world
10. Blockchain and **energy consumption**

Next

11. Blockchain and **copyright**
12. **Global digital identity**

Now gaps

1. **Cybersecurity in a blockchain world:** No platform – including blockchain – is entirely invulnerable to malicious cyberattacks. Points of vulnerability may exist at important points of access to the blockchain platform, and quantum computing and its potential ability to overcome cryptographic methods may one day present a severe challenge to the successful adoption of blockchain.[108] Certainly, the idea of insider collusion, such as a "51% attack", is more than hypothetical.[109] In a recent Deloitte survey, 58% of respondents said that cybersecurity is an area of focus for their blockchain or digital assets-related strategy and another fifth of respondents said that cybersecurity issues were enough in their own right to preclude blockchain and digital assets investment altogether.[110] Although cybersecurity does not represent the most serious issue for some, the methods of those who engage in cyberattacks will probably only become more sophisticated and, as such, require the highest form of vigilance.

2. **Regulatory fragmentation on digital identities, assets and cryptocurrencies:** Regulatory fragmentation refers to the varying and at times contradictory regulatory regimes with which an organization must comply within and across geographical jurisdictions. In a financial context, regulatory fragmentation may be especially acute. In the EU, for example, different regulatory regimes across the member states have made anti-money laundering (AML) enforcement more challenging. But the problem becomes even more difficult with cryptocurrencies, given their digital and potentially opaque ownership identity. The EU's Fifth Anti-Money Laundering Directive was designed to address this problem by specifically subjecting cryptocurrency service providers to its AML regulatory requirements.[111]

   One of the most important manifestations of tax regulatory fragmentation is the varying ways in which cryptocurrencies are defined by different governments, or even within the same government. In the US, for example, the Internal Revenue Service (IRS) treats cryptocurrencies as property and taxes them as such, even though they are often used as currencies.[112] Moreover, the IRS recently issued new guidance on reporting gains and losses from the disposition of cryptocurrencies in an apparent effort to step up enforcement, but some critics argue that this raises more questions than it answers.[113] Other US federal agencies may treat cryptocurrencies as commodities or securities.[114] There is disagreement on how cryptocurrency is treated within governments and by different governments – and, therefore, how they are taxed. This invites open-ended questions about the tax implications of cryptocurrencies, including: 1) How should holders estimate the fair market value of cryptos for tax purposes?; 2) How should investors determine the cost basis of cryptos upon liquidation?; 3) What are the inheritance implications of cryptos?; 4) What if someone exchanges one crypto for another? Tax regulatory fragmentation can hamper the adoption of cryptocurrencies, as their use invokes tax considerations.[115]

3. **Technical interoperability and the need for standards:** As blockchain implementations become more complex, it is increasingly likely that a blockchain implementation is part of a larger network that requires interoperability to achieve the aims of efficiency and connectivity. However, many distributed ledger protocols, platforms and applications currently do not have the capacity to communicate with one another. Some of the differences are purely technical, such as differing consensus

protocols, while others are related to proprietary characteristics of the blockchain's security. Regardless of the reasons, interoperability challenges can create barriers for organizations looking to scale blockchain technology. For example, a lack of platform standards and data interoperability have reduced the efficacy of the technology for critically sensitive value chains such as food traceability.[116] A number of projects are looking to address the issue.[117] Any long-term interoperability framework should also address key issues about governance and legal framework, data ownership, data standardization, revocation rights and antitrust legislation, among many others.

4. **Consortia governance:** To go far with blockchain technology, organizations should go together. In the consortium model, actors who are often competitors come together to find solutions to common problems. In recent years, much of the conversation revolved around the basic idea of "coopetition" and some of the inherent challenges in overcoming the standard competitive mindset. Conversations have centred on issues related to governance, including consortium operational rules, funding and profit-sharing, IP, overcoming antitrust issues, data ownership and legal structure. Indeed, a recent Deloitte survey found that an "inability to create fair and balanced governing rules" was the greatest barrier to participation in a blockchain consortium among respondents.[118] While consortia should continue to play a key role in overall blockchain adoption, there may be heightened efforts on the part of organizations to understand what key governance issues are at stake – and the terms that they find acceptable – prior to joining a consortium.

5. **Enforceability of smart contracts:** Smart contracts are blockchain-based contracts that are automatically executed once certain specified criteria coded into the contract are met. Smart contracts serve as a form of open-source decision-making that can represent the entirety of the responsibilities of the parties or supplement a traditional written agreement.[119]

   Smart contracts may be useful in a whole host of use cases – but are smart contracts truly enforceable?[120] Indeed, smart contracts often trigger an array of questions that can leave their legal status uncertain. In most jurisdictions, smart contracts based on blockchain are not accepted as legal contracts, leaving the aggrieved party without any legal recourse should a dispute arise. While real potential exists, the smart contract is still limited by unresolved issues, especially with respect to the absence of case law history. We could see an uptick in case law and legislation in efforts to reconcile the confusion.[121]

"While real potential exists, the smart contract is still limited by unresolved issues, especially with respect to the absence of case law history.

Near gaps

6. **Data integrity:** "Garbage in, garbage out" remains an issue with blockchain technology and, in fact, in some instances may be "garbage in, garbage forever". Whether by accident or through fraud, incorrect data may be validated on a blockchain. This may be an especially difficult problem within the supply chain context. A food processor may claim a level of purity about a product or that the product was harvested by a specific farm on a specific date, all by way of data entry onto a blockchain. A consensus protocol may validate that the food processor did in fact enter specific data, but it may not have anything to say about the intrinsic veracity of the data. This challenge may be even more pronounced when the supply chain involves natural resources and original actors up the chain in remote regions who may have less than robust methods of data capture. While these errors may ultimately be flagged, the human and financial costs can be devastating, including issues that go to the heart of consumer protection.[122] Clearly, this is just one example, and data integrity obviously goes well beyond the supply chain context. Additional use cases could include digital identity, financial transactions, decentralized finance (DeFi, a cryptocurrency-based financial system without central authority) and more. And, indeed, industry is working on a variety of solutions.[123] But any enduring answer to the challenge of data integrity that goes beyond simple solutions will likely require industry and regulators to work together.

7. **Cross-border regulatory inconsistencies:** Since blockchain often involves a cross-border architecture, different geographies are taking distinct regulatory positions on the status of blockchain and digital assets.[124] These differences can present challenges to cross-border blockchain adoption and make global initiatives tougher to realize. For example, regulatory views on cloud adoption, national open API standards, cybersecurity requirements and health information, among others, all vary from country to country.[125] A homogeneous cross-border blockchain platform may struggle to comply with all of these regulations under different regimes. Further, within some countries differences may exist among different regions or states where federal authority is not pre-emptive on the issue.[126]

   In 2020 and beyond, as cross-border blockchain business models become more mainstream, the issues in terms of which laws govern transactions, decision rights, consensus and IP, among other areas, could become increasingly confusing and contradictory. For example, imagine a blockchain model across countries with differing data privacy laws. Which laws apply? Or what if one operates in no clearly recognized jurisdiction of governance at all? There are many other potential issues that derive from cross-border multiparty configuration – including whether regulators in any given country actually regulate from a perspective of genuine technical understanding.

8. **Audit/third-party guidance in a blockchain context:** Uncertainty about properly certified financial and process records is expected to grow as blockchain becomes more widely used, raising several questions: How do auditors check for compliance when the requirements are unclear?; how does an auditor test for anti-money laundering/know your customer (AML/KYC) compliance within the construct of blockchain?; how can a true audit be performed if companies other than the one under audit control the data? These and other questions may drive auditors to develop a deeper understanding of blockchain technology in the near term.

9. **The preservation and challenge of anonymity in an immutable blockchain world:** Blockchain's ability to provide anonymity (in practice, pseudonymity) and traceability within the context of its inherent immutability has triggered challenges over what authorities – and others – have a right to know and how to delete data when an individual or organization tries to exercise the "right to be forgotten".

   For example, with respect to immutability, the GDPR that governs data protection and privacy within the EU – and applies to all organizations conducting business in the EU regardless of national origin – promulgates a "right to be forgotten" that enables EU citizens to request erasure of personal data from network storage repositories. This provision may be at odds with the immutable character of digital ledger technology.[127]

   And with respect to anonymity/traceability, in the US the Health Insurance Portability and Accountability Act (HIPAA) limits how personal health information is handled, which may be inconsistent with blockchain-based solutions within the life sciences context.[128] Perhaps because enforceability in a nearly opaque transaction medium such as blockchain is so difficult, the IRS recently issued additional guidance on the tax treatment of cryptocurrency.[129] Her Majesty's Revenue & Customs (HMRC), the UK tax authority, has also set forth guidance to collect taxes on income derived from the disposition of cryptocurrencies.[130] In the near term, we will likely see increased efforts at enforcement and greater efforts to preserve anonymity and privacy.

"In the near term, we will likely see increased efforts at enforcement and greater efforts to preserve anonymity and privacy.

10. **Blockchain and energy consumption:** Some blockchain platforms use a consensus mechanism that involves a "proof of work", a mining process that requires the simultaneous use of high-powered computers, which consume a substantial amount of energy. With respect to bitcoin alone – the most common public blockchain using the proof of work protocol – one 24-hour period of mining (300,000–350,000 transactions) is thought to consume enough energy to support about 320,000 American homes for just over three weeks.[131] Some estimates suggest that over the course of a year the bitcoin application of blockchain (reflecting about 125 million transactions) consumes around 75 terawatt hours' energy, which rivals the energy use of a small- to medium-sized industrialized nation such as Chile.[132]

Whether in 2020 or soon thereafter, the amount of energy consumed by public blockchain will need to be addressed. Already, various research organizations have proposed alternative approaches, including more efficient proof of work/consensus mechanisms.[133] But no concerted policy initiative at the government level appears imminent. This issue is significant enough, however, that it may have an impact on blockchain's long-term viability.[134]

Next gaps

11. **Blockchain and copyright:** There is much discussion in the literature of how blockchain can protect against copyright infringement.[135] A much less widely debated topic is how blockchain could abet copyright infringement. In theory, there is no practical limit as to what can be characterized digitally and therefore be considered a digital asset. But if something can be rendered digitally, couldn't it also be posted on a blockchain in violation of copyright laws? The answer is "yes" – in theory. The good news, for now, can be found in scaling limitations that would render it difficult to post many kinds of digital assets such as photography. But the ability of a blockchain configuration to accommodate ever-increasing file sizes means this may be an issue going forward, especially in blockchain configurations that have inadequate consensus mechanisms to establish true ownership.

12. **Global digital identity:** If the vision of a truly decentralized financial system (DeFi) ever reaches fulfilment, a global digital identity would be a prerequisite. Identity is a fundamental part of the financial transaction life cycle, and true cross-border decentralization requires the portability that a global digital identity would provide. One of the more significant hurdles to global decentralized financial transactions is the varying AML/KYC regulations within and between individual countries – all adding to transaction complexities and barriers. What a global digital identity might achieve is a harmonization of differing regulatory regimes in terms of identity, and this could help fight identity-based crimes. It might also promote financial inclusiveness, since a global digital identity could make those on the periphery of the banking community "safer" bets to lending organizations. Right now, a global digital identity is more of an abstraction than a reality, however much different initiatives are being piloted to pursue it.[136] For a global digital identity to become something more than an abstraction would require harmonized and enforceable technical and data standards across platforms and geographies.[137]

FIGURE 5 | **Time horizon and risk level of emerging governance gaps**

Now

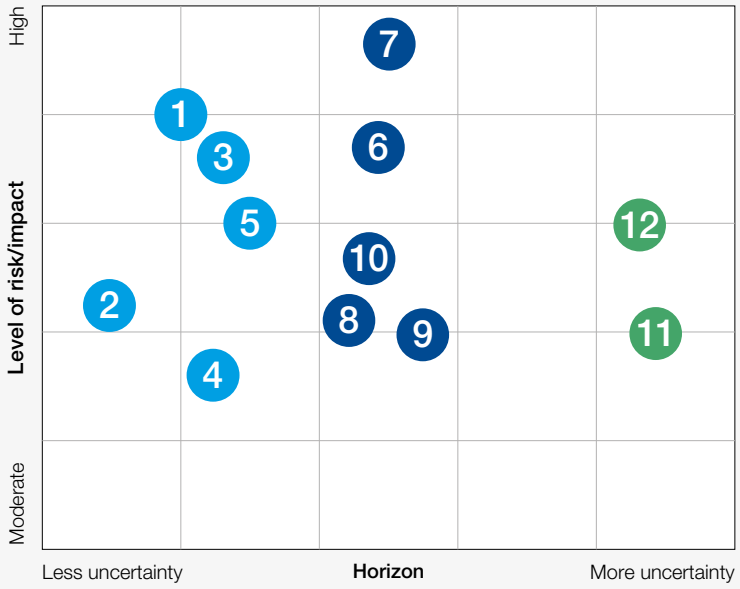
1. Cybersecurity in a blockchain world
2. Regulatory fragmentation in terms of digital identities, assets and cryptocurrencies
3. Technical interoperability and the need for standards
4. Consortia governance
5. Enforceability of smart contracts
6. Data integrity

Near

7. Cross-border regulatory inconsistencies
8. Audit/third-party guidance in a blockchain context
9. The preservation and challenge of anonymity in an immutable blockchain world
10. Blockchain and energy consumption

Next

11. Blockchain and copyright
12. Global brand identity



Source: Deloitte analysis

Sample innovative governance frameworks

1. **Regulatory sandboxes – Singapore, South Korea and the UK**
   Dozens of countries have implemented or announced regulatory sandboxes – an emerging innovative framework covering a number of focus areas, including blockchain and digital assets. This demonstrates the regulator's ability to invest in innovation and education through collaboration with industry.[138] A few of the many relevant examples include:

   – The Monetary Authority of Singapore (MAS) fintech regulatory sandbox provides forms of regulatory relief to member organizations that explore financial services innovation. One recent story is the approval of a tokenized securities trading platform developed by a Singaporean blockchain infrastructure developer that is a member of the sandbox.[139]

   – In late 2018, the South Korean government established a regulatory sandbox dedicated to spurring innovation, investment activity and job creation in blockchain technology. Run by the country's financial regulatory agency, the sandbox is reported to have created close to 400 blockchain and fintech jobs and about $110 million in new investments.[140]

   – The Financial Conduct Authority (FCA) – a regulator of financial companies in the UK – operates a regulatory sandbox that allows fintech organizations to explore and validate innovative products, models, services and channels of delivery. In July 2020, the FCA announced the projects accepted into its sixth cohort under the scheme and indicated that among these will be projects "safekeeping and transacting of digital assets using distributed ledger technology".[141]

2. **Japan Virtual and Crypto Asset Exchange Association (JVCEA) – Japan's crypto regulating body**
   The Financial Services Agency (FSA), Japan's leading financial regulator, has granted the country's cryptocurrency industry the power to self-regulate and police domestic exchanges. In so doing, the FSA created the JVCEA, the country's self-regulatory body for crypto exchanges. The JVCEA is authorized to establish guidelines on behalf of the cryptocurrency industry, including rules for local trading platforms. Since its founding, the JVCEA has put forth an array of guidelines for blockchain and cryptocurrency organizations. It also announced a fourfold jump in leverage in crypto margin trading.[142]

3. **Bermudan Regulatory Activity – digital stimulus token and changes in banking laws**
   The Bermudan government is aiming to build up

the country as a hub for blockchain and digital assets. Recent activity includes the test-piloting of a digital stimulus token, a stablecoin, to evaluate the viability of a digital token for food and other necessary goods and services. It is designed as a way to facilitate assistance to specific sectors of the economy.[143] In 2019, the government allowed for the payment of taxes in USDC stablecoin and launched the development of a blockchain-based digital ID platform.[144] Earlier, the government amended its banking laws to allow for the creation of a category of banks that serve blockchain and cryptocurrency companies. The Bermudan premier, David Burt, reiterated his vision of the country as a "leader in supporting innovative private-sector digital-asset solutions" in a September 2020 statement.[145]

4. **CBDC experimentation – Thailand and China**
Many countries have explored the potential of a central bank digital currency (CBDC) but only a few have moved beyond the theoretical phase. Examples of CBDC initiatives that have attracted particular attention include:

   – The Bank of Thailand's Project Inthanon. In 2018, the Bank of Thailand, the country's central bank, announced the launch of Project Inthanon, a three-phase initiative whose aim was to encourage players in the Thai financial services industry to work together to understand and ultimately accept distributed ledger technology (DLT); and to develop a prototype of a wholesale CBDC as a medium of cross-border funds transfer and settlement. The first phase exhibited the potential of DLT as a platform to meet high-level payment functions in real time, among other objectives. The second phase addressed the efficacy of DLT in achieving regulatory compliance settlement processes. Completed in late 2019, the third phase explored ledger interoperability with the Hong Kong Monetary Authority. Future steps may include the widening of the network beyond Hong Kong as well as the development of retail CBDCs for Thai domestic organizations.[146]

   – China's digital yuan. In many respects, China has stood at the forefront of blockchain innovation. One of the most widely discussed developments is the emergence of a digital version of the yuan, the Chinese fiat currency. Testing of the yuan CBDC occurred in select cities earlier in 2020, and additional trials are under way in a wider array of locations. Some believe that the full-scale roll-out of the yuan CBDC may occur in late 2020 or early 2021, though when exactly is unknown. The approach to roll-out is expected to be two-tiered: The first level will involve transactions between the People's Bank of China and commercial banks; the second, distribution of the CBDC to the general public. The CBDC is expected to serve both wholesale (interbank settlements) and retail, for the general population. When finally rolled out, however, it would serve as the first large-economy CBDC in circulation.

     There appear to be various motivations behind the push for the yuan CBDC. The official reasons are related to transaction efficiencies, the expense of fiat currency production and processing, fighting terrorism, and more efficient monetary policy enforcement, among others. However, some feel that the initiative is also motivated in part by the desire to internationalize the yuan; in essence, to make it a global currency in competition with the US dollar and emerging global stablecoins. Some have also raised concerns about the data trail that the yuan CBDC may leave and the accompanying data privacy implications.[147]

TABLE 2 **Innovative governance framework criteria**

Framework	Agile	Fit for purpose	Globally relevant	Inclusive	Innovative	Evidence-based	Produced outcomes	Currently live
1. Regulatory sandboxes			●	●	●	●	●	●
2. JVCEA				●	●		●	●
3. Bermudan regulatory activity	●	●		●	●			●
4. CBDC experimentations	●	●	●	●	●	●	●	●

Source: Deloitte analysis

6 Internet of things and connected devices

IoT is not one technology but an architecture of several technologies that can transform the spaces in which we live for a more sustainable future.

Technology governance is about so much more than telling companies what they cannot do – rules should help guide corporate players through minefields of uncertainty to provide the best outcomes for users and citizens. However, striking that balance can be difficult, especially when it comes to still-developing technology such as IoT, which holds great promise – and real risks.

This challenge is made doubly difficult by the fact that IoT is not one technology but an architecture of several technologies. The enabling technologies that make up IoT allow information about the world to be processed digitally and then used back in the world (see Figure 6).

Such a wide definition means many use cases in many industries fit under the purview of IoT. Everything from connected blood sugar monitors in medicine to cold chain verification in logistics to smart streetlights can qualify as IoT, yet still bring very different benefits and pose very different risks.

IoT is not new. Even the term is now more than two decades old. However, it seems to have garnered significantly more attention in the past few months as the global coronavirus pandemic has uncovered the power of digitally processing data about the physical world. Industries as disparate as public health and electronics manufacturing began searching for and trialling new IoT solutions. Some of these solutions may spur greater adoption of IoT in some areas, such as in overburdened hospitals. In other cases, such as mobile phone-based contact tracing, IoT is raising technology governance questions due to its pervasive nature.

The good news is that, thanks to the increased attention being paid to IoT, progress is being made in several areas. The pandemic has led to new frameworks that can help tackle some of IoT's enduring challenges such as security and privacy. Many of these successes have seen government and industry working collaboratively, moving beyond their traditional roles of tech producer and regulator to show rather than dictate positive uses of the technology. Innovative solutions such as security self-assessments or the use of IoT in real-time government planning can help ensure both the proper use of technology and better, more equitable outcomes for all.

“ Innovative solutions such as security self-assessments or the use of IoT in real-time government planning can help ensure both the proper use of technology and better, more equitable outcomes for all.

FIGURE 6 **The information value loop**

Governance gaps

Now

1. **Regulating smart contracts, instant payments** and other IoT-enabled transactions may demand new approaches to keep up with the speed of such transactions
2. Mismatch between **digital goods and paper taxes** should be addressed
3. **Market failure of device security and quality** often leaves the public with unsupported and insecure IoT devices
4. During the COVID-19 pandemic, the use of IOT-based **contact tracing has spurred privacy concerns**

Near

5. The fragility of supply chains during the pandemic has **renewed calls for supply-chain tracking**
6. **Regulation of new IoT business models** is needed as wholly new products and services emerge
7. **Law enforcement access to data from IoT** is stuck in a tension between the needs of investigators and the desire to protect citizen privacy
8. **Domestic harassment and privacy invasion through IoT** devices is also an emerging threat to privacy

Next

9. **Cyber liability** remains an uncertain field for both companies and governments
10. **IoT and terms and conditions** represents a unique challenge in terms of keeping consumers informed on devices that may not even have screens

Now gaps

1. **Regulating smart contracts, instant payments:** Smart contracts enable the instant movement of funds based on the physical movement of goods (which can be tracked by sensor), allowing for a number of scenarios not covered by current financial regulations. Challenges range from how to handle disputes or errors in automated payments (what if a sensor goes bad and over- or under-bills?) to novel financial instruments based on goods in transit. A lack of understanding and ineffective regulation of novel financial instruments have caused problems before, as with mortgage-backed securities during the financial crisis of 2008.[148]

2. **Digital goods and paper taxes:** IoT-enabled supply chains and smart contracts allow goods and services to move around the globe at unprecedented speed. However, most tax functions – whether direct or indirect – remain paper-based. The lag between business moving at digital speed and taxation moving at paper speed can pose a significant risk for businesses. For example, a company that can track items with radio-frequency identification (RFID) and can bill or be billed in real time via smart contracts could end up holding tax liability on its books while waiting for paper-based forms to process. Finding ways for revenue agencies around the world to accept, process and use IoT-based data can be vital in accelerating not just the pace of government, but business as well.

3. **Market failure of device security and quality:** In testimony before Congress, technologist Bruce Schneier described how IoT-driven cybersecurity events such as the Mirai botnet were due to market failures.[149] Because consumers valued price and functionality ahead of security features and governments did not require such features, some device manufacturers had no incentive to do anything other than produce cheap hardware quickly. The result was a vast array of non-secured IoT devices that fell easy prey to hackers looking to create criminal botnets. Governments should consider establishing a security rating system or evaluation organization for new hardware and software products. A public-private working relationship such as Underwriters Laboratories (a non-profit dedicated to advancing the safe commercialization of evolving technology) may be an effective model for quickly and efficiently establishing the baseline of transparency required for IoT security.[150]

4. **Contact tracing spurs privacy concerns:** IoT-based technologies are proving to be critical tools in stopping the spread of COVID-19. From contact-tracing apps to thermal sensors in public spaces, IoT can provide desperately needed information as people try to combat the virus. However, the prospect of governments and private companies gathering such a large volume of information about individuals has raised privacy concerns. The need to collect information to stop the spread of the virus amid increased sensitivity to privacy issues may accelerate progress on tools and regulations that balance social needs with individual rights. The European Commission, for example, has established guidelines and toolkits for app development for its member states.

Near gaps

> IoT devices are recording more data about daily life in more and more locations, increasing the likelihood that they will record information about a crime, whether intentionally or unintentionally.

5. **Renewed calls for supply-chain tracking:** High-profile incidents of stolen or counterfeit pharmaceuticals and personal protective equipment (PPE) amid the pandemic have renewed calls for greater tracking within supply chains. IoT-based solutions – especially when paired with immutable records such as blockchain – can help monitor goods in shipment and give an immutable record of their provenance, vouching for their security and quality. The pandemic could increase adoption of such solutions in the near future.

6. **Regulation of new IoT-enabled business models:** The faster flow of data and goods enabled by IoT is creating new business models including many as-a-service forms of business for physical goods. Many of these business models represent entirely new ways of delivering goods and services, and so may challenge or stretch existing regulations. For example, if an oil pipeline worker damages a smart valve that is being managed on an as-a-service basis and that valve fails, resulting in an oil spill, who is responsible? While such small uncertainties may not be holding back progress for these business models, they could introduce problems into society.

7. **Law enforcement access to data from IoT devices:** IoT devices are recording more data about daily life in more and more locations, increasing the likelihood that they will record information about a crime, whether intentionally or unintentionally. However, it is uncertain whether law enforcement can – or should be allowed to – gain access to that data. In some cases, IoT personal assistants have witnessed crimes, but technology companies have been unwilling to reveal what the devices may or may not have recorded. A common framework is needed to determine when and how law enforcement can gain access to IoT-recorded data in order to balance privacy concerns with criminal investigations.

8. **Domestic harassment and privacy invasion through IoT devices:** In a growing number of cases, smart home or other IoT devices have been used to harass or disturb another person. Using information gained through past consensual relationships, people can change a thermostat, lock doors remotely or monitor in-home smart cameras, among other activities, to harass and invade the privacy of others. Laws governing the use of IoT technologies by third parties are poorly understood, even as the devices are proliferating in homes.

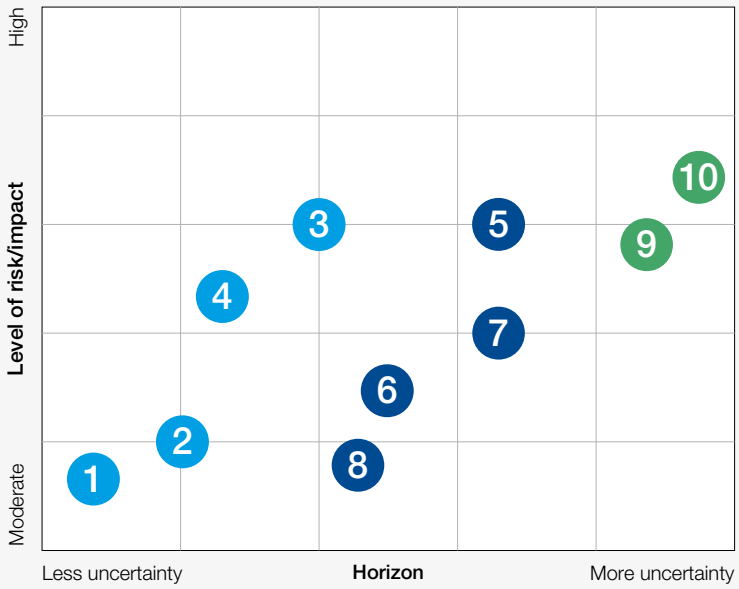
Next gaps

9. **Cyber liability:** IoT-enabled cyberattacks present another question of liability. When IoT devices can be hijacked and used as attack vectors, who is responsible? The hacker, the device manufacturer, the IoT device owner – or even the target, in instances of negligence? The list goes on. This uncertainty can result in costly litigation, with each link in the chain looking to pass the buck. Clear accountability guidelines are necessary to prevent manufacturers from creating poor devices and users from operating them poorly.

10. **IoT and terms and conditions:** IoT presents unique challenges to citizens' right to informed control over their data and its use. How can an IoT device that lacks a screen, for example, present intelligible terms and conditions to a consumer? Lack of informed consent by consumers can drive misuse of citizen data and engender public mistrust of both technology and government.

FIGURE 7 **Time horizon and risk level of emerging governance gaps**

1. Regulating smart contracts, instant payments
2. Digital goods and paper taxes
3. Market failure of device security and quality
4. Contact tracing spurs privacy concerns
5. Renewed calls for supply chain tracking
6. Regulation of new IoT business models
7. Law enforcement access to data from IoT
8. Domestic harassment and privacy invasion through IoT devices
9. Cyber liability
10. IoT and terms and conditions



Source: Deloitte analysis

Sample innovative governance frameworks

1. **Cybersecurity labelling for IoT devices**
Finland has launched a cybersecurity labelling system to inform consumers about which IoT products meet digital safety standards. The move is aimed at promoting secure-by-default IoT product lines and spreading awareness of the dangers associated with increased connectivity. The labelling initiative will see a stamp placed on every smart device that adheres to Finland's cybersecurity safety guidelines. Vendors can apply for security badge certification through a website, which consumers can also consult to make informed purchases. The UK has proposed a similar law. In January 2020, the UK government announced its intention to draw up legislation holding all consumer smart devices sold in the UK to rigorous security requirements.[151] Such government-driven models are not the only solution to IoT challenges. Models based on public-private partnerships or third-party certification are also being explored.

2. **Self-service security assessments**
Researchers with BetterIoT, a community-led effort to promote responsible, secure and well-designed IoT products, recently launched a self-service online assessment tool for new IoT products.[152] Using this tool, designers can assess their planned products on such dimensions as privacy, licensing provisions, openness, interoperability, life cycle, permissions, transparency, data governance and security. This tool can serve as a guide to ensure poor products do not accidentally slip onto the IoT market and put citizens at risk.

> The increased demand for healthcare services and the strain placed on providers by the COVID-19 crisis has led to greater adoption of IoT in healthcare settings.

3. **Example of effective transnational standards on international flows of data and money**
   The Financial Action Task Force (FATF) offers an example of how transnational standards for cross-border flows can be applied to the IoT-enabled flow of data and goods. FATF has prepared a standards document, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, to support countries and their financial institutions in designing AML measures and combatting the financing of terrorism. In this way, FATF helps member nations meet the goal of financial inclusion without compromising crime-fighting measures. Through a common understanding of the FATF standards and the flexibility they offer – particularly regarding the risk-based approach (RBA) – jurisdictions can craft effective and appropriate controls for IoT-enabled technologies.[153]

   The FATF's approach has been agreed to by almost every country – and strong penalties are imposed on those that do not implement it. Additionally, the agency places states considered to be safe havens for terrorism on a so-called "grey list". While the Economist Intelligence Unit (EIU) and others assess the economic impact of being placed on the grey list as minimal, it is often still enough to spur a state to reform.[154]

4. **Sharing good IoT code**
   Making government source code publicly available can be an important tool in preventing the vulnerabilities and unintended consequences that can arise from "function creep" (that is, when something is used in unexpected ways) of IoT devices and code. The US shares its open-source software on code.gov, and has made several IoT code bases available. By taking code from uses as varied as managing sensor arrays that monitor volcanoes to an IoT and AI fusion that can predict pollution in waterways, these code repositories can help spread IoT by making code that can tackle tough problems available for free. More importantly, because the government stands behind the quality of that code, it can help spread good code, helping reduce the likelihood of vulnerabilities and breaches caused by bad code in IoT systems everywhere.

5. **Accelerated adoption in healthcare**
   The increased demand for healthcare services and the strain placed on providers by the COVID-19 crisis has led to greater adoption of IoT in healthcare settings. Uses range from simple systems designed to monitor vital signs or adjust ventilator settings remotely to devices that enable at-home care for elderly patients. IoT has provided greater care to patients while protecting healthcare workers and may provide a model of care even after the pandemic ends.

6. **Use of IoT data in response planning**
   Both governments and private companies discovered the power of IoT-derived data during the coronavirus crisis. As companies struggled to keep supply chains moving and governments worked to deploy needed resources, both came to rely on IoT data when making real-time decisions about how to respond. By integrating IoT data with digital twins of supply chains – or even whole cities – companies were able to move orders to suppliers less affected by the pandemic or reroute shipments of raw materials to keep production moving. Similarly, governments used data to deploy and adjust city services to get the right resources to the hardest-hit areas, turning even the most mundane operations into smart city services.

TABLE 3 | **Innovative governance framework criteria**

Framework	Agile	Fit for purpose	Globally relevant	Inclusive	Innovative	Evidence-based	Produced outcomes	Currently live
1. Cybersecurity labelling for IoT devices	●	●	●			●		●
2. Self-service security assessments	●	●	●	●	●	●		●
3. Example of effective transnational standards on international flows of data and money		●	●			●	●	●
4. Sharing good IoT code		●	●	●	●			
5. Accelerated adoption in healthcare		●	●			●	●	●
6. Use of IoT data in response planning	●	●	●	●	●		●	●

Source: Deloitte analysis

7 Autonomous vehicles, shared mobility and digitally enabled transport

Moving towards a more inclusive mobility future in a post COVID-19 world.

Perhaps no area of human activity has been as disrupted by the COVID-19 pandemic as mobility. Seemingly overnight, we went from a world in which daily life was, in large measure, defined by how, when, where and why we travelled from place to place, to one in which personal mobility became impossible or laden with risk. The impacts are by now familiar, but no less staggering: Use of public transport plummeted by more than 90% in some cities;[155] traffic reduced to a trickle;[156] a surge in walking and cycling contributed to a shortage of bicycles in some markets;[157] and home deliveries were made at volumes usually witnessed only during the end-of-year holidays.[158]

As the world cautiously and unevenly begins to move again, there is still significant uncertainty about the long-term impacts of COVID-19 and its economic fallout on mobility. But several trends have emerged that seem likely to persist:[159]

- **Trip substitution via digitization.** Telework, telemedicine and e-learning are likely to become permanent fixtures for some portion of the population, reducing their need to access mobility. The magnitude of these shifts, and whether they will create a material change in overall demand, whether in miles travelled or mode choice, will depend largely on how long the pandemic and associated stay-at-home orders persist. Roughly 37% of jobs in the US could be done from home, by one estimate, and those jobs tend to be higher-paying.[160] At the same time, lower-income households disproportionately rely on public transport,[161] suggesting widely varying impacts among individuals and transit modes.

- **A new focus on – and expanded definition of – safety.** Safety in mobility has long meant avoiding car crashes, even as too little attention was sometimes paid to crime and the physical safety of vulnerable groups on public transport. Now, as people begin to travel again, a "safe" trip will probably also mean one that is sanitary and hygienic. The role of mass transport and shared modes in spreading the virus remains unclear – some research suggests it is minimal[162] – but as long as there is a public perception that densely packed travel is risky, we can expect a wide range of preventive measures to be deployed where people gather to travel together.

- **Growing reliance on e-commerce and home delivery.** The perceived health risks of venturing into crowded shops coupled with stay-at-home orders have accelerated the rapid shift towards online retail and home delivery. As a result, we will probably see increased attention to, and innovation around, supply-chain optimization, long-haul trucking and last-mile freight movement. We should also expect expanded testing and deployment of automated delivery using robots and drones, as well as remote operation and autonomous driving for long-haul trucking.[163]

Governing emerging forms of mobility becomes both more urgent and more complicated amid and in the wake of the pandemic. The locus of activity for autonomous vehicles, for example, might shift to freight and last-mile delivery applications, and governance structures will likely need to adapt quickly to keep pace. Many of the existing governance gaps – from ensuring equitable access, to shifting people to more sustainable modes, to shoring up public transport – could be complicated by fears of the virus and by the acute, and unevenly distributed, economic damage. However, as in many domains, the upheaval of recent months also creates a rare opportunity to fundamentally rethink "business as usual", with both public authorities and the private sector looking to make some potentially permanent changes, such as creating new space for active modes such as walking and cycling.

❝ Governing emerging forms of mobility becomes both more urgent and more complicated amid and in the wake of the pandemic.

Governance gaps

Now

1. **Enabling mobility data sharing**
2. **Creating sustained shifts in travel patterns**
3. **Cannibalization of public transport**
4. **Governing the roadside**

Near

5. **Autonomous goods movement, driver-assist and workforce requirements**
6. **Avoiding a new mobility divide**
7. **Creating a seamless integrated mobility system (SIMSystem)**

Next

8. **Balancing public-sector and private-sector roles**
9. **On-street testing and liability for autonomous vehicles**

Now gaps

1. **Enabling mobility data sharing:** The mobility landscape is growing increasingly complex, with an array of new entrants and services – such as ride-hailing, carsharing, microtransit, real-time traffic maps and integrated trip planners – existing alongside well-established modes of transport such as underground railways, buses and personal cars. To fully benefit, consumers, public authorities and private companies would all need to share key data, but at present there is no shared technical standard nor agreed-upon governance framework for what, when, how and with whom information should be made available. As lockdowns ease in some places and people begin to travel more freely, a need to monitor flows and density accurately and in real time – how crowded is the next bus, for example – and to convey that information to travellers is likely to grow more acute, and multiparty data sharing seems to be a necessary component.

2. **Creating sustained shifts in travel patterns:** In the face of climate change, congestion and various health and safety challenges, there is a growing consensus that we need to rethink the role of internal combustion engine-powered private cars as a means of getting from A to B and instead shift travel to other modes. But mobility habits are sticky and difficult to change, and fears of using mass transport and shared modes amid a pandemic could prompt people to increasingly choose private cars. Authorities have a growing array of tools at their disposal to shape modal choice, from congestion pricing to improved transport options or more cycling infrastructure – but they lack a comprehensive governance framework that incorporates the trade-offs among these options and can guide policy-making to create sustained outcomes.

3. **Cannibalization of public transport:** Public transport is the backbone of the transport system in many cities. As new, more convenient services such as ride-hailing emerge, there is a risk that public transport users with the means to do so will defect to other options, further reducing revenue for public authorities. Pandemic-induced concerns about using public transport are likely to accelerate this shift in some markets, exacerbated by dramatic declines in revenue that are likely to lead to reduced service and failure to carry out maintenance and improvements.[164] The result could leave so-called “captive” riders, who tend to have lower incomes and few viable alternatives, bearing the brunt of reduced service levels and deferred maintenance – further widening the mobility divide.

4. **Governing the roadside:** As e-commerce, parcel deliveries and door-to-door shared mobility continue to grow, roadside space is growing increasingly contested and valuable, leading to double parking, for example, and by extension congestion. The pandemic has only underscored the importance of this critical liminal space, as some cities have reallocated street and pavement areas to pedestrians and cyclists to enable physical distancing. As some consider making those changes permanent, stay-at-home orders have also increased reliance on home delivery. What technologies and policies will enable cities and others to more effectively manage the roadside?

Near gaps

5. **Autonomous goods movement, driver-assist and workforce requirements:** Advanced driver-assist, remote piloting and fully autonomous long-haul trucks are being actively piloted in many markets. Aside from the obvious questions about safety standards and certification, how do these technologies affect existing driver requirements? For example, do hours-of-service standards such as mandated rest periods change if a portion of the time "driving" is spent in driver-assist mode? What types of cargo can be transported using different autonomous driving technologies, and do the rules differ for hazardous materials? As COVID-19 places renewed emphasis on creating "touchless" supply chains and more resilient goods movement networks, the time frame for deploying these technologies could be accelerated.

6. **Avoiding a new mobility divide:** New mobility technologies and services could open up access to jobs and education and healthcare opportunities that have historically been out of reach for many underserved communities. However, they could also exacerbate existing gaps if they fail to reach the areas most in need, are predicated on participation in the digital economy – such as smartphone ownership or digital payments – or are too expensive to be viable options. Exacerbating the challenge, the pandemic has drained public coffers and disproportionately affected vulnerable communities. How can we create a governance framework that meets the needs of all residents while still enabling private-sector providers to capture value?

7. **Creating a seamless integrated mobility system (SIMSystem):**[165] There are many new technologies and solutions in the area of mobility. But when they are deployed as one-off, isolated endeavours, they often only exacerbate the current transport system's friction and inefficiencies by adding complexity and additional transaction costs. A citywide digital platform, overlaid onto today's transport system, could enable a more efficient outcome in the near term while facilitating transparency, interoperability, coordination and control. What type of governance is needed to enable such a system to emerge?

Next gaps

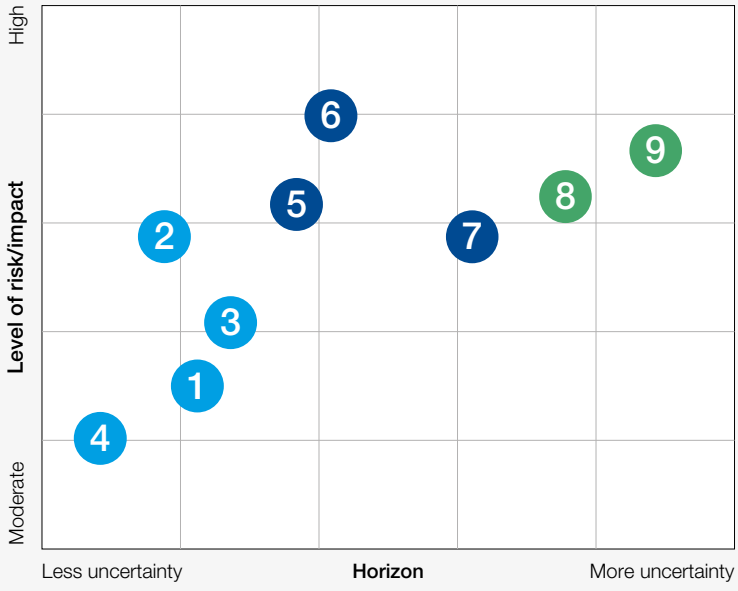
> Cities should decide how to create incentives for all players to have a stake in the system while creating a receptive environment for innovation and meeting city goals.

8. **Balancing public-sector and private-sector roles:**[166] New mobility services and technologies have often outpaced regulation. As public authorities come to grips with this more dynamic transport environment, they will probably have to choose whether to proactively legislate the private sector or allow a more open market-based approach to drive the pace of innovation and let regulation follow. Regulation and policy can help set needed standards, encourage knowledge-sharing and mitigate negative externalities or misalignment with public-sector goals and strategic plans. However, it would require a more active role from government and a willingness to get private-sector players to comply. On the other hand, emerging mobility innovations such as dockless bicycles and scooters have arguably created significant value for end users, which might not have been realized or might not have been realized so quickly in the face of more stringent rules. Cities should decide how to create incentives for all players to have a stake in the system while creating a receptive environment for innovation and meeting city goals. The question of which comes first is not easy to answer – and in many cities, it will depend on existing governance models and structures. Further into the future, as residents increasingly rely on new services such as ride-hailing, e-scooters and more, what happens when private-sector providers unilaterally alter or remove those services from a market? How can the public sector create "mobility continuity" while still enabling competition and innovation?

9. **On-street testing and liability for autonomous vehicles:** As companies continue to refine autonomous driving systems, being able to test and refine in real-world conditions grows increasingly important. Such vehicles have already been deployed on the streets for years – at times with little or no explicit indication they are operating in self-driving mode – and regulatory approaches have varied widely across the globe. Given that members of the general public are, effectively, unwitting test subjects in this process, what is an appropriate governance approach that balances communicating and educating other road users with the industry's desire for rapid testing?[167] And as the vehicles approach commercial deployment, with whom does the fault lie when a self-driving car crashes? With the vehicle manufacturer? The designer of the operating system software? The owner or occupant? Will each vehicle be required to possess a "black box" similar to the one used in aircraft to help determine liability? Even then, in instances where deep learning algorithms are at work, it may be near-impossible to deduce why an autonomous vehicle system made the decision it did.[168]

FIGURE 8 **Time horizon and risk level of emerging governance gaps**

1. Enabling mobility data sharing
2. Creating sustained shifts in travel patterns
3. Cannibalization of public transport
4. Governing the roadside
5. Autonomous goods movement
6. Avoiding a new mobility divide
7. Creating a seamless integrated mobility system
8. Balancing public- and private-sector roles
9. On-street testing and liability for autonomous vehicles



Source: Deloitte analysis

Sample innovative governance frameworks

1. **Mobility Data Specification/ Open Mobility Foundation**
   Los Angeles, led by its Department of Transportation (LADOT), is pioneering various public sector-led initiatives around open data exchanges. LADOT developed the Mobility Data Specification (MDS), an open-source "common language" for collecting and sharing mobility data across cities. The recently established Open Mobility Foundation seeks to manage the MDS's continued development and deployment, and to share best practices across 50 cities in the US and dozens internationally. With two APIs – one for government to push "ground truth" data to providers and one for mobility companies to share data with government – it provides a mechanism for the city to better understand the mobility landscape and to enforce regulations. However, highlighting the tensions about data sharing, privacy and value creation, the MDS has also prompted strong pushback from some private-sector mobility providers.

2. **Finland's open mobility law**
   Revisions to Finland's Transport Code require public transport operators to make certain data (timetables, routes, ticket prices) available via open APIs. This has enabled cities such as Helsinki to become pioneers of mobility-as-a-service by giving riders the ability to plan, book and pay for trips using multiple public and private modes via a single application interface.

3. **Singapore's unified, top-down approach**
   The city-state has deployed a unified autonomous vehicle testing framework administered by a single authority (the Land Transport Authority), avoiding the patchwork of rules seen in many other countries. The country has also been effective in shifting travellers away from private cars and on to alternative modes through a combination of carrots and sticks: making private cars extremely expensive to own and deploying dynamic congestion pricing on the one hand, and improving the level of service and quality of public transport on the other.

4. **Lisbon's "greenfield" vs. "brownfield" regulation**
   Lisbon calibrates its approach to mobility regulation based on what type of service is emerging. For "greenfield" innovation, where outcomes are unclear but there is a potential upside, the city focuses more on "soft" regulation and guidance. For "brownfield" innovation, pertaining to established modes or where the risks are greater or better known, the city may use "hard" regulation. While the line between greenfield and brownfield is admittedly blurred, Lisbon's evolving approach to e-scooters provides an illustrative example. Initially the city took a hands-off approach. Nine companies entered the city within one year. As the process evolved, a forum was created in which the city and operators met to discuss the changes that must be put in place to address potential problems and risks. Now the city is considering adopting the Mobility Data Specification (see point 1, above) as scooters have taken a firmer foothold in the Lisbon landscape. By engaging through informal meetings with operators and micromobility providers, the city has created the feedback loop necessary for effective regulation. As part of its stance on public-private collaboration, the city also announced the first-ever corporate mobility pact, in collaboration with the World Business Council for Sustainable Development and several private-sector partners, to accelerate sustainable urban mobility transformation.[169]

5. **Transport for London's open data approach**
   Transport for London's policy has been to make available data such as timetables and service status and disruption information, resulting in

more than 80 data feeds available through a unified API. This in turn has nurtured a system of 13,000 app developers who have developed more than 600 new products used by more than 40% of the population.[170] Research by Deloitte suggests that providing this free and open data has boosted the London economy by up to £130 million a year through improved journeys, time savings, job creation and new innovations.[171]

6. **Driverless delivery exemptions in the US**
The National Highway Traffic Safety Administration (NHTSA), part of the US Department of Transportation, in February 2020 granted a two-year exemption for autonomous vehicle start-up Nuro to operate its R2 shuttle for goods delivery in several American markets.[172] Such regulatory carve-outs can be useful workarounds when creating a more holistic or enduring governance framework is not feasible, especially in the face of near-term needs.

7. **Collaborative data sharing to assess the impact of driver-assist technology**
The US Department of Transportation's Partnership for Analytics Research in Traffic Safety (PARTS) programme was launched as a cooperative effort between major automotive original equipment manufacturers (OEMs and the government, with a neutral third-party vendor securely hosting and analysing data covering some 10 million vehicles and 4 million crashes.[173] By pooling data across manufacturers and marrying it with highly granular federal data, the project was able to demonstrate that vehicles equipped with automatic emergency braking were less likely to experience rear-end collisions than those without. In January 2020, the Department of Transportation announced a second phase of the PARTS programme, expanding the number of participating OEMs and extending its coverage to include lane departure warnings and adaptive cruise control.[174]

TABLE 4 **Innovative governance framework criteria**

Framework	Agile	Fit for purpose	Globally relevant	Inclusive	Innovative	Evidence-based	Produced outcomes	Currently live
1. Mobility Data Specification/Open Mobility Foundation	●	●	●	●	●		●	●
2. Finland's open mobility law					●	●	●	●
3. Singapore's unified top-down approach	●					●	●	●
4. Lisbon's "greenfield" vs. "brownfield" regulation	●	●		●		●		●
5. Transport for London's open data approach		●	●	●	●	●	●	●
6. Driverless delivery exemptions in the US	●	●					●	●
7. Collaborative data sharing to assess the impact of driver-assist technology		●			●	●	●	●

Source: Deloitte analysis

8 Drones

COVID-19, and its accompanying need for physical distancing and remote work, has driven drone use to new levels.

In recent years the use of unmanned aerial systems (UAS), or drones, has risen on a largely ad hoc basis, as various uses – from facilities inspection to product delivery, videography and even sports – have become possible. The COVID-19 pandemic has only accelerated the growth of these uses, especially in delivery and facilities inspection, as agencies seek to reduce human interaction and enable remote work.

However, this increase in adoption has been met with slow regulatory change. Often, and especially in the case of COVID-19, regulators are left playing catch-up as companies seize new UAS opportunities. But UAS use has reached sufficient levels in recent years for some regulatory gaps to be foreseen and regulations developed pre-emptively.

Doing so could help enable UAS industries to mature, by improving a baseline level of knowledge through training, increasing access to airspace with amended equipment needs and gaining the trust of aviation authorities – while also ensuring the nascent technology is introduced into the marketplace responsibly.

Although drone use started small in a few large governments decades ago, it has since become common among governments large and small, in the commercial sector and for sports enthusiasts. Use cases can range from military and law enforcement to disaster management, job-site safety or agriculture. Some even race drones recreationally for sport.

Recently, COVID-19 and its accompanying need for physical distancing and remote work drove drone use to new levels.[175] Functions such as surveying saw as much as a 90% increase in use, while in the construction industry there was a 56% increase in use for remote job-site monitoring.[176] Other use cases such as medical supply delivery and stadium sanitization also saw growth as a result of the pandemic.

While governments have taken many extraordinary measures during COVID-19, these new drone applications have proven sufficiently useful for them probably to remain after the COVID-19 pandemic is suppressed.

But new ways of using drones present new challenges. Issues of data privacy, UAS integration into urban environments, drone operator certification, legal and ethical concerns related to law enforcement's use of drones, and ensuring that new UAS business models are accounted for properly within existing business regulations all demand consideration.

Existing tools used in other industries can present useful frameworks for filling UAS regulatory gaps without excessive burden on the emerging UAS market. Tools such as regulatory sandboxes, which are already in use, enable regulators to test out new rules in a low-risk and timely manner. Automated drone flight approval and remote drone IDs are also being explored and could help governments ensure new airspace entrants are incorporated safely. On a global level, the International Civil Aviation Organization (ICAO) provides standards and recommended practices for the safe introduction of new technologies into civil aviation. That organization recently published model drone regulation[177] and guidance for UAS in support of humanitarian aid and emergency response.[178]

Regulation is not a "one and done" process – it should evolve in tandem with new technologies and use cases. Governments should take an adaptive regulatory approach that accounts for many new drone activities and services. Learning from existing frameworks that have proven effective in other sectors could be an excellent first step. Solving these regulatory gaps is important and, if done correctly, a likely benefit to innovation and state economies. It seems time to get serious about solving the gaps.

“ Regulation is not a 'one and done' process – it should evolve in tandem with new technologies and use cases.

Now

1. **Greater drone use for physical distancing** would require more regulation of wide-scale drone use
2. **Drones can be used for delivery of urgent medical supplies** to offset human interaction during crises or for speed of service
3. **More drone jobs** would require more trained professionals and associated standards/licences
4. **Drone data and privacy** are expected to become more important as drones are used to complete certain tasks otherwise done by people during times of crisis
5. **Lack of data on drones** would become increasingly important as more drones operate in urban and other environments

Near

6. **Inadvertent collection of audio/video** would need to be regulated as drones serve in more functions

Next

7. **Proving drone business models** work would be necessary for the industry to flourish
8. **Lack of airworthiness standards** would need to be solved if certain drone business cases are to be developed
9. **Common use cases need drone-specific regulations** versus those imported from fixed or rotary-wing aircraft

Now gaps

1. **Greater drone use during physical distancing:** At the height of the COVID-19 pandemic, hundreds of millions of people around the world were required to isolate in their homes. As whole nations saw their workforces shelter in place, the use of drones enabled some work, such as infrastructure, inventory and environmental inspection to continue.

   The pandemic demonstrated the value of drones as a supplement to the workforce – one that will probably remain after a return to normalcy. As drones are integrated into the workforce at scale, new regulations will be important to ensure this is done safely. These regulations should address licences or permits for operators, procedures for operation in urban and other environments and integration into national airspace systems.

2. **Drones can be used for delivery of urgent medical supplies:** As the need for contactless delivery of goods and services rose during the COVID-19 pandemic, drones were increasingly used to deliver consumer goods of all sorts. Of particular need was the delivery of medical supplies and PPE. One successful example in Ghana delivered and collected COVID-19 test kits.

   These services enabled the quick and touchless sharing of needed supplies. But the hazardous nature of some of these deliveries adds an additional layer of risk should the drone crash, or otherwise fail, and land where the hazardous material can come into contact with others. Regulations should be considered to govern how such materials are delivered by drones.

3. **More drone jobs:** Whether for delivery of medical supplies, inspection of critical infrastructure or managing the data collected by drones, more skilled drone operators and drone data coordinators will likely be needed. New regulatory and accreditation processes would be needed to manage the training and employment of these new workers. Additionally, authorities responsible for approving operations would need training beyond basic flight as industrial and transportation needs begin to align.

4. **Drone data and personal privacy:** Drones have been used to monitor crowds and provide other crisis services during the COVID-19 pandemic. In some cases, drones were equipped with the ability to collect personal information, and this might raise privacy and civil liberty concerns. Regulatory oversight should ensure drone use during crises – and after – does not infringe on the rights of citizens.

   It is fundamentally important for regulators to create standards that are not too onerous, yet still align with society's expectations, to ensure long-term societal acceptance and the extension of trust among all parties.

5. **Lack of data on drones:** The civil aviation industry has a robust system of air traffic management that organizes flight paths and provides safety measures for travellers and members of the public. Similar systems are less developed for drones. The US, through an FAA and National Aeronautics and Space Administration (NASA) collaboration, is working on a system called Unmanned Aircraft SystemTraffic Management (UTM). The EU is

working on a similar system, called U-Space, with multiple stakeholders.[179]

The purpose of these systems is to collect information on UAS operations – drone ID, flight data and cargo, among other data points – to deconflict aviation participants and provide a system for safe flight across modes at scale. This data would need to be organized and standardized between cities, states and countries. The EU's U-Space service, which collects operationally relevant data to organize and inform UAS operators and governments, is one such example.[180]

Other countries are working on similar systems, but more development and uniformity between systems is needed.

Near gap

6. **Inadvertent collection of video/audio:** The proliferation of drones and their development from small hobby craft to larger commercial aircraft mean that some level of inadvertent video/audio collection from their cameras and other sensors is all but inevitable. But how to control for it? This data could represent a minor invasion of privacy or a violation of civil rights, depending on what it is and who can access it. Could law enforcement, for example, access the camera footage of a drone that accidentally filmed a drug-farming operation? Could they do so automatically, as with existing networks of CCTV or doorbell cameras? While this gap in regulation has not yet slowed the development of any technologies, significant public backlash could set back development.

Next gaps

> Infrastructure will probably need to be researched, built and certified using completely new standards and processes to accommodate new forms of aerial mobility.

7. **Proving drone business models:** Perhaps the greatest gap limiting the wider adoption of drones and electric vertical take-off and landing (eVTOL) aircraft is not one of safety or technical barriers but of economics. For smaller UAS, economic viability can hinge as much on regulations as customer base or pricing. Regulations that are uncertain or do not allow for higher-margin use cases, such as those that may require operation beyond line of sight or over people, can limit growth opportunities for businesses.

   For larger vehicles, the challenge could be more about economics and scale. Even optimistic estimates show that a future air taxi service could be viable only in highly dense areas – and could still cost up to $1,900 per trip. Additionally, such taxis would need to travel at more than 120mph to be competitive against cars.[181] These slim margins mean that emerging UAS business models are tremendously susceptible to regulation.

   For both small and large UAS, ultimate economic viability may rest on regulations that not only protect citizens but also allow for business growth. With few precedents to draw on, determining how UAS businesses should be regulated or taxed may end up driving the timeline and viability of many emerging UAS and eVTOL business models.

8. **Lack of airworthiness certification standards and infrastructure certification:** While the US and other countries have defined airworthiness standards for fixed-wing, rotary-wing and lighter-than-air aircraft, rapidly evolving aviation archetypes that combine characteristics of any of these three, such as electric vertical take-off and landing (eVTOL), do not neatly fit into any category. The result is that any passenger-carrying UAS – often using this new eVTOL form – would need entirely new airworthiness and safety standards.

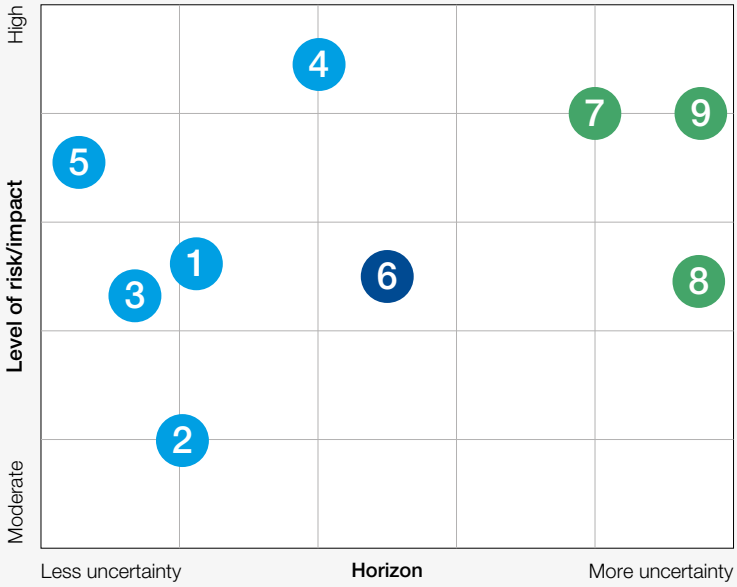
   Varied jurisdictions are currently exploring the development of new airworthiness standards, but this can be time-consuming and costly in itself. In the meantime, the lack of clarity is slowing the development of possible aircraft. Infrastructure will probably need to be researched, built and certified using completely new standards and processes to accommodate new forms of aerial mobility.

9. **Common use cases need drone-specific regulations:** Just as regulators must strike the proper balance between regulation and innovation, they should also tailor guidelines to specific use cases and their associated safety and security challenges, even as they rely on existing frameworks. For example, while regulators have permitted UAS use for health services, such as delivering COVID-19 tests or PPE in Ghana and the US, regulations are often borrowed from other similar services. This can leave regulators unprepared to address UAS-specific challenges.

   The lack of second-order regulatory ability could also affect business cases. For instance, early in the adoption of UAS by the energy industry, many operators were confused by the regulatory landscape governing proximity of flight to power lines. Without tailored standards, power-line operations stipulated no flights of any kind closer than 1,000 feet. This limitation has been well suited for helicopters, the prevailing form of flight at low altitudes, but made less sense for drones and limited their value considerably.

FIGURE 9 | **Time horizon and risk level of emerging governance gaps**

1. Greater drone use during social distancing
2. Drone delivery of urgent medical supplies
3. More drone jobs
4. Drone data and privacy
5. Lack of data on drones
6. Inadvertent collection of video/audio
7. Proving drone business models
8. Lack of airworthiness standards
9. Common use of cases need drone-specific regulations



Source: Deloitte analysis

Sample innovative governance frameworks

1. **Sandboxes for drone experiments**
   Regulatory sandboxes are one success story from drones that may be valuable to other emerging technologies as well. These sandboxes have been used around the world to offer UAS operators a testing ground to explore drone capabilities and inform regulators of regulatory gaps or challenges.

   The US, UK, Japan and Malawi are all currently employing regulatory sandboxes, which can be tailored to the needs of a given market or country. Additionally, they often prove to be as informative to the technology developers as the regulators. For example, in Malawi, where wireless network coverage is more intermittent, the sandbox was able to test connectivity.[182] In Japan's sandboxes, governmental bodies were able to review testing results to protect public safety while making it easier for innovators to navigate the government approval process.[183]

2. **Drone ID rule-making framework**
   One proposed rule, remote identification (remote ID), provides a framework for remote identification of all UAS operating in US airspace.[184] The rule would facilitate the collection and storage of certain data such as the identity, location and altitude of an unmanned aircraft and its control station.

   Remote ID was developed through a collaborative process, incorporating not only public comment on proposed rules but also input from the industry working group that helped FAA regulators to craft those rules in the first place.[185]

   Remote ID is designed to enable safe, routine drone operations across the US. This capability can enhance safety and security by allowing the FAA, law enforcement and federal security agencies to identify drones flying in their jurisdiction. Widespread adoption of UAS for uses such as package delivery or flight in densely congested airspace might be largely impossible without drone ID.

3. **Transnational collaboration on UAS regulation**
   The International Civil Aviation Organization (ICAO), a United Nations specialized agency, provides governance through the development of standards and recommended practices (SARPs). SARPs are considered a useful regulatory tool because they provide detailed measures for regulating new technology. Additionally, ICAO can develop them relatively quickly, normally within a few years.[186]

   The relative ease with which ICAO can develop SARPs, despite a broad international membership, is due in large part to the fact that states are under no legal obligation to follow SARPs – though doing so is often in member states' best interests.[187] ICAO also provides guidance through less formal reports and advisory circulars.

   ICAO has additionally produced resources concerning drone use for humanitarian aid and emergency response via its model UAS regulations, which offer a "template for member states to implement or supplement their existing UAS regulations".[188]

Through these formal and informal channels, ICAO is able to support UAS governance development. While less formal tools such as reports or advisory circulars are the most recent focus for ICAO's drone regulation, as the technology is developed further the organization may pursue more formal governance means through SARPs.

SARPs cover several issue areas, but almost all create efficiencies and greater access to air travel, which could prove useful in developing more robust UAS regulations. Regardless of the approach, ICAO is generally considered to be a well-established international organization suited to helping develop international UAS regulations.

4. **Automated drone flight approval**
The global proliferation of new systems – such as the Belgian Droneguide PRO, the Swiss Flight Management System, or the US Low Altitude Authorization and Notification Capability (LAANC) – suggest that automated request and approval of drone operations is the next step in the evolution of air traffic management.

Aided by cloud infrastructure, private UAS service providers and connections to air traffic control, automated approval systems can increase ease of use for drone operators while providing air traffic control with greater awareness and control of drones in their area. The result would probably be easier drone operations and safer travel for all of us.

Automated drone flight approval is one of the foundational steps in creating a system of UAS traffic management (UTM) that can truly integrate air traffic of all types in all environments.

Recent applications include:

- The FAA's LAANC programme seems to have been well received by both aviation and drone communities.[189]
- In 2019, skyguide and AirMap kicked off a live market trial of Swiss U-space automated authorization. More than 200 operators have joined the market trial and have used the Swiss U-space mobile application.[190]
- In the initial few months, about 18,000 drone users (unique visitors) used the Droneguide application every month.[191]

TABLE 5 **Innovative governance framework criteria**

Framework	Agile	Fit for purpose	Globally relevant	Inclusive	Innovative	Evidence-based	Produced outcomes	Currently live
1. Sandboxes for drone experiments	●	●	●		●	●	●	●
2. Drone ID rule-making framework		●	●			●		●
3. Transnational collaboration on UAS		●	●	●		●	●	●
4. Automated drone flight approval		●	●	●		●	●	●

Source: Deloitte analysis

Contributors

World Economic Forum

Michelle Avary
Head of Automotive and Autonomous Mobility

Kimmy Bettinger
Project Specialist, Data Policy

Sumedha Deshmukh
Platform Curator, Blockchain and Digital Currency

Kay Firth Butterfield
Head of Artificial Intelligence and Machine Learning

Ruth Hickin
Strategy and Impact Lead

Eddan Katz
Project Lead, Artificial Intelligence and Machine Learning

Jeff Merritt
Head of Internet of Things and Urban Transformation

Conor Sanchez
Platform Specialist, Artificial Intelligence and Machine Learning

Sheila Warren
Platform Head, Blockchain and Distributed Policy

Harrison Wolf
Project Lead, Aerospace and Drones

Deloitte

Scott Corwin
Managing Director

William D. Eggers
Managing Director

Jonathan Holdowsky
Senior Manager

David Jarvis
Senior Manager

Diana Kearns-Manolatos
Senior Manager

Pankaj Kishnani
Assistant Manager

Joe Mariani
Manager

Dave Noone
Senior Manager

Derek Pankratz
Senior Manager

Adam Routh
Manager

Brenna Sniderman
Senior Manager

Endnotes

1. Matthew Beedham, "Report: Cryptocurrency Ransomware Payments up 90%, Thanks to Ryuk", TheNextWeb.com, 18 May 2019, https://thenextweb.com/hardfork/2019/04/18/cryptocurrency-ransom-increase-ryuk/ (link as of 2/11/20).
2. Katie Brigham, "The Growing Fight over Police Use of Facial Recognition", CNBC, 11 July 2020, https://www.cnbc.com/2020/07/11/why-police-usage-of-facial-recognition-has-come-under-scrutiny.html (link as of 2/11/20).
3. Government of Singapore Personal Data Protection Commission, "Model AI Governance Framework", https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework (link as of 2/11/20).
4. Japan Virtual and Crypto Assets Exchange Association, "Statistics", https://jvcea.or.jp/about/statistics/; see also Japan Virtual and Crypto Assets Exchange Association, "Main Info", 12 June 2020, https://jvcea.or.jp/news/main-info/20200612-001/ (links as of 2/11/20).
5. United Nations Economic Commission for Europe, "Safety at Core of New Framework to Guide UN Regulatory Work on Autonomous Vehicles", 4 September 2019, http://www.unece.org/info/media/presscurrent-press-h/transport/2019/safety-at-core-of-new-framework-to-guide-un-regulatory-work-on-autonomous-vehicles/doc.html (link as of 2/11/20).
6. World Economic Forum, "Centre for the Fourth Industrial Revolution: Platforms", https://www.weforum.org/centre-for-the-fourth-industrial-revolution/areas-of-focus (link as of 2/11/20).
7. Matthew Beedham, "Report: Cryptocurrency Ransomware Payments up 90%, Thanks to Ryuk", TheNextWeb.com, 18 May 2019, https://thenextweb.com/hardfork/2019/04/18/cryptocurrency-ransom-increase-ryuk/; see also Rob Lever, "Misinformation Woes Could Multiply with 'Deepfake' Videos", Phys.org, https://phys.org/news/2019-01-misinformation-woes-deepfake-videos.html (links as of 2/11/20).
8. Tiffany Fishman and Justine Bornstein, "The Rise of Mobility as a Service", Deloitte Center for Government Insights", 23 January 2017, https://www2.deloitte.com/us/en/insights/deloitte-review/issue-20/smart-transportation-technology-mobility-as-a-service.html (link as of 2/11/20).
9. New Zealand Ministry of Social Development, "The Privacy, Human Rights and Ethics (PHRaE) Framework", https://www.msd.govt.nz/documents/about-msd-and-our-work/work-programmes/initiatives/phrae/phrae-on-a-page.pdf (link as of 2/11/20).
10. Emma Morriss, "Government Launches Coronavirus Vaccine Taskforce as Human Clinical Trials Start", Pharmafield.co.uk, 22 April 2020, https://pharmafield.co.uk/pharma_news/government-launches-coronavirus-vaccine-taskforce-as-human-clinical-trials-start/ (link as of 2/11/20).
11. We Robotics, "How Delivery Drones Are Being Used to Tackle COVID-19", 25 April 2020, https://blog.werobotics.org/2020/04/25/cargo-drones-covid-19/ (link as of 2/11/20).
12. Syed Fasiuddin, "COVID-19 Outbreak Provides Test-Bed for Need-Based Insurance in India", Economic Times, 17 March 2020, https://bfsi.economictimes.indiatimes.com/news/insurance/covid-19-outbreak-provides-test-bed-for-need-based-insurance-in-india/74672696; see also Claire Woffenden, "FCA's Launches Digital Sandbox Pilot", Fintech Times, 11 May 2020, https://thefintechtimes.com/fcas-launches-digital-sandbox-pilot/ (links as of 2/11/20).
13. David Alexander Walcott, "How the Fourth Industrial Revolution can Help us Beat COVID-19," World Economic Forum, 7 May 2020, https://www.weforum.org/agenda/2020/05/how-the-fourth-industrial-revolution-can-help-us-handle-the-threat-of-covid-19/ (link as of 2/11/20).
14. Ibid.
15. Ledger Insights, "UAE Uses Blockchain, Digital Identity to Battle Covid-19", 30 March 2020, https://shuftipro.com/news/uae-adopts-digital-identity-and-blockchain-to-fight-covid-19 (link as of 2/11/20).
16. GCN, "Autonomous Vehicles Deliver COVID-19 Tests to Lab", 8 April 2020, https://gcn.com/articles/2020/04/08/avs-covid-tests-mayo-clinic-campus.aspx (link as of 2/11/20).
17. Gadgets 360, NDTV, "Coronavirus Contact Tracing Apps: Which Countries Are Doing What", 31 May 2020, https://gadgets.ndtv.com/apps/features/coronavirus-contact-tracing-apps-which-countries-are-doing-what-2237952 (link as of 2/11/20).
18. World Economic Forum, "Centre for the Fourth Industrial Revolution: Platforms", https://www.weforum.org/centre-for-the-fourth-industrial-revolution/areas-of-focus (link as of 2/11/20).
19. Kashmir Hill, "Wrongfully Accused by an Algorithm", The New York Times, 3 August 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (link as of 2/11/20).
20. Bruce Schneier, "Testimony at the US House of Representatives Joint Hearing 'Understanding the Role of Connected Devices in Recent Cyber Attacks'", Schneieronsecurity.com, 16 November 2016, https://www.schneier.com/essays/archives/2016/11/testimony_at_the_us_.html (link as of 2/11/20).
21. Matthew Beedham, "Report: Cryptocurrency Ransomware Payments up 90%, Thanks to Ryuk", TheNextWeb.com, 18 May 2019, https://thenextweb.com/hardfork/2019/04/18/cryptocurrency-ransom-increase-ryuk/ (link as of 2/11/20).

22. William Eggers, Mike Turley and Pankaj Kishnani, "The Future of Regulation", Deloitte Center for Government Insights, 19 June 2018, https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html; see also Edward Kelso, "New Study: 80% of ICOs are Scams, only 8% Reach an Exchange", Bitcoin.com, 28 March 2018, https://news.bitcoin.com/80-of-icos-are-scams-only-8-reach-an-exchange/ (link as of 2/11/20).
23. Colin Lecher, "What Happens When an Algorithm Cuts Your Health Care", The Verge, 2 September 2020, https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy (link as of 2/11/20).
24. Philip Koopman and Michael Wagner, "Challenges in Autonomous Vehicle Testing and Validation", SAE International Journal of Transportation Safety 4, no. 2016-01-0128 (2016): 15–24. As the authors note, "Another issue with validating machine learning is that, in general, humans cannot intuitively understand the results of the process."
25. John McKinlay, Duncan Pithouse, John McGonagle and Jessica Sanders, "Blockchain: Background, Challenges and Legal Issues", DLA Piper, 2 February 2018, https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/ (link as of 2/11/20).
26. Ibid.
27. Jack Filiba, "The History of the DAO: How a Failed Project May Still Impact the World", coinsquare.com, 28 June 2018, https://news.coinsquare.com/blockchain/the-dao-how-a-failed-project-may-still-impact-the-world/ (link as of 2/11/20). Ibid.
28. Neha Mule, "Americans Avoid to Download Contact Tracing Apps Amid Data Privacy Concerns", 19 June 2020, https://www.smartindustrynews.com/sin-article/americans-avoid-to-download-contact-tracing-apps-amid-data-privacy-concerns/ (link as of 2/11/20).
29. Telegraph reporters, "Jealous Husband Used Wall-Mounted iPad in his 'Smart Home' to Spy on Estranged Wife, Court Hears", Daily Telegraph, 10 May 2018, https://www.telegraph.co.uk/news/2018/05/10/smart-home-stalker-jealous-husband-used-wall-mounted-ipad-heating/ (link as of 2/11/20).
30. Rahul Raj, "Let's Get (Not Too) Personal; When Hyper-Personalization Turns from Cool to Creepy", Analytics India Magazine, 9 December 2019, https://analyticsindiamag.com/lets-get-not-too-personal-when-hyper-personalization-turns-from-cool-to-creepy/ (link as of 2/11/20).
31. Mark Sullivan, "Privacy Groups Want a Federal Facial-Recognition Ban, but It's a Long Shot", Fast Company, 28 January 2020, https://www.fastcompany.com/90456414/privacy-groups-want-a-national-facial-recognition-ban-but-its-a-longshot (link as of 2/11/20).
32. Mihalis Kritikos, "Ten Technologies to Fight Coronavirus", European Parliament – European Parliamentary Research Service, April 2020, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/641543/EPRS_IDA(2020)641543_EN.pdf (link as of 2/11/20).
33. Katie Brigham, "The Growing Fight over Police Use of Facial Recognition", CNBC, 11 July 2020, https://www.cnbc.com/2020/07/11/why-police-usage-of-facial-recognition-has-come-under-scrutiny.html (link as of 2/11/20).
34. Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of Machine Learning Research, 2018, http://proceedings.mlr.press/v81/buolamwini18a.html (link as of 2/11/20).
35. Bobby Hellard, "237 Police Officers Disciplined over Computer Misuse", ITPro.com, 8 November 2019, https://www.itpro.co.uk/computer-misuse-act/34783/237-police-officers-disciplined-over-computer-misuse (link as of 2/11/20).
36. Charlie Osborne, "COVID-19 Blamed for 238% Surge in Cyberattacks against Banks", ZDNET, 14 May 2020, https://www.zdnet.com/article/covid-19-blamed-for-238-surge-in-cyberattacks-against-banks/ (link as of 2/11/20).
37. Mallory Hackett, "Number of Cybersecurity Attacks Increases during COVID-19 Crisis", Healthcare Finance, 4 June 2020, https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis (link as of 2/11/20).
38. World Health Organization, "WHO Reports Fivefold Increase in Cyberattacks, Urges Vigilance", 23 April 2020, https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (link as of 2/11/20).
39. Marcus Comiter, "Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It", Harvard Belfer Center Paper, August 2019, https://www.belfercenter.org/publication/AttackingAI (link as of 2/11/20).
40. Lance Eliot, "Human In-The-Loop Vs. Out-of-The-Loop in AI Systems: The Case of AI Self-Driving Cars", AI Trends, 9 April 2019, https://www.aitrends.com/ai-insider/human-in-the-loop-vs-out-of-the-loop-in-ai-systems-the-case-of-ai-self-driving-cars/ (link as of 2/11/20).
41. Israel Aerospace Industries, "HARPY", https://www.iai.co.il/p/harpy (link as of 2/11/20).
42. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries", Information and Technology Innovation Foundation, February 2015, http://www2.itif.org/2015-cross-border-data-flows.pdf (link as of 2/11/20).
43. Branko Vlajin, "What You Need to Know About Cloud Laws and Regulations", 18 May 2018, https://www.cloudwards.net/what-you-need-to-know-about-cloud-laws-regulations/ (link as of 2/11/20).

44. New Zealand Ministry of Social Development, "The Privacy, Human Rights and Ethics (PHRaE) Framework", https://www.msd.govt.nz/documents/about-msd-and-our-work/work-programmes/initiatives/phrae/phrae-on-a-page.pdf (link as of 2/11/20).

45. New Zealand Government, "Algorithm Charter for Aotearoa New Zealand", https://data.govt.nz/use-data/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter (link as of 2/11/20).

46. UK Government Biometrics and Forensics Ethics Group Facial Recognition Working Group, "Police Use of Live Facial Recognition Technology: Ethical Issues", February 2019, https://www.gov.uk/government/publications/police-use-of-live-facial-recognition-technology-ethical-issues (link as of 2/11/20).

47. Mihalis Kritikos, "Ten Technologies to Fight Coronavirus", European Parliament – European Parliamentary Research Service, April 2020, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/641543/EPRS_IDA(2020)641543_EN.pdf (link as of 2/11/20).

48. Samburaj Das, "Japan Approves Self-Regulation for Cryptocurrency Industry", CCN, 24 October 2018, https://www.ccn.com/breaking-japan-approves-self-regulation-for-cryptocurrency-industry/ (link as of 2/11/20).

49. Japan Virtual and Crypto Assets Exchange Association, "Statistics", accessed 30 August 2020, https://jvcea.or.jp/about/statistics/; see also Japan Virtual and Crypto Assets Exchange Association, "Main Info", 12 June 2020, https://jvcea.or.jp/news/main-info/20200612-001/ (links as of 2/11/20).

50. BetterIoT, "#betteriot assessment tool", https://betteriot.wordpress.com/?s=betteriot+assessment+tool (link as of 2/11/20).

51. BetterIoT, "A Little Rebrand: Better IoT", 6 December 2018, https://betteriot.wordpress.com/2018/12/06/a-little-rebrand-better-iot/ (link as of 2/11/20).

52. The Federal Aviation Administration, "US Department of Transportation Announces Technology Partners for Remote ID Development", 5 May 2020, https://www.faa.gov/news/press_releases/news_story.cfm?newsId=24956 (link as of 2/11/20).

53. Emma Morriss, "Government Launches Coronavirus Vaccine Taskforce as Human Clinical Trials Start", 22 April 2020, https://pharmafield.co.uk/pharma_news/government-launches-coronavirus-vaccine-taskforce-as-human-clinical-trials-start/ (link as of 2/11/20).

54. William D. Eggers, Pankaj Kishnani and Shruthi Krishnamoorthy, "Transforming Government Post-COVID-19", 15 June 2020, Deloitte, https://www2.deloitte.com/us/en/insights/economy/covid-19/transforming-government-post-covid-19.html (link as of 5/11/20).

55. US Department of Transportation, "Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0", https://www.transportation.gov/av/4 (link as of 2/11/20).

56. Akanki Sharma, "Transforming Indian Healthcare via Telemedicine", Express Healthcare, 9 April 2020, https://www.expresshealthcare.in/covid19-updates/transforming-indian-healthcare-via-telemedicine/418106/ (link as of 2/11/20).

57. Drone Rules, "EU Regulations Updates", https://dronerules.eu/sl/professional/eu_regulations_updates (link as of 2/11/20).

58. "The First-Ever Corporate Mobility Pact – Catalyzing Corporate Action to Transform Mobility", World Business Council for Sustainable Development, October 2019, https://www.wbcsd.org/Programs/Cities-and-Mobility/Transforming-Mobility/News/The-first-ever-Corporate-Mobility-Pact-catalyzing-corporate-action-to-transform-mobility (link as of 2/11/20).

59. Financial Conduct Authority, "The Digital Sandbox Pilot", 4 May 2020; last updated 12 October 2020, https://www.fca.org.uk/firms/innovation/digital-sandbox (link as of 2/11/20).

60. Maryanne Buechner, "UNICET's Ascent into the Drone Age", Unicef.org, 12 June 2018, https://www.unicefusa.org/stories/unicefs-ascent-drone-age/34436 (link as of 2/11/20).

61. Aaron Boyd, "10 Drone Programs Get Federal OK to Break the Rules", NextGov, 9 May 2017, https://www.nextgov.com/emerging-tech/2018/05/10-drone-programs-get-federal-ok-break-rules/148098/ (link as of 2/11/20).

62. Ibid.

63. AUVSI, "Skyports to Trial BVLOS Flights in Non-Segregarte Airspace after Joining UK CAA Regulatory Sandbox", 15 April 2020, https://www.auvsi.org/industry-news/skyports-trial-bvlos-flights-non-segregated-airspace-after-joining-uk-caa-regulatory (link as of 2/11/20).

64. Jonathan Wilson, "No Small Potatoes: Digital Jersey's Big Data Ambitions", 28 March 2019, https://eandt.theiet.org/content/articles/2019/03/no-small-potatoes-digital-jersey-s-big-data-ambitions/ (link as of 2/11/20).

65. Ibid.

66. Digital Jersey, "IoT Sandbox", https://www.digital.je/choose-jersey/sandbox-jersey/iot-sandbox/ (link as of 2/11/20).

67. Courtney Bjorlin, "New Framework Helps Promote IoT Data Sharing Among Smart Cities", 2 March 2018, https://www.iotworldtoday.com/2018/03/02/new-framework-helps-promote-iot-data-sharing-among-smart-cities/ (link as of 2/11/20).

68. Tiffany Fishman and Justine Bornstein, "The Rise of Mobility as a Service", January 2017, Deloitte Center for Government Insights, 23 January 2017, https://www2.deloitte.com/us/en/insights/deloitte-review/issue-20/smart-transportation-technology-mobility-as-a-service.html (link as of 2/11/20).

69. Organisation for Economic Co-operation and Development Regulatory Policy Division, "International Regulatory Co-operation: Adapting Rulemaking for an Interconnected World", OECD, October 2018, https://www.oecd.org/gov/regulatory-policy/international-regulatory-cooperation-policy-brief-2018.pdf (link as of 2/11/20).

70. Christine Horton, "Are the Fintech Bridges Working?" Raconteur, 15 December 2019, https://www.raconteur.net/finance/uk-fintech-bridges (link as of 2/11/20).

71. Financial Conduct Authority, "Global Financial Innovation Network (GFIN)", FCA.org, 31 January 2019, last updated 27 February 2020, https://www.fca.org.uk/firms/global-financial-innovation-network (link as of 2/11/20).

72. United Nations Economic Commission for Europe, "Safety at Core of New Framework to Guide UN Regulatory Work on Autonomous Vehicles", 4 September 2019, http://www.unece.org/info/media/presscurrent-press-h/transport/2019/safety-at-core-of-new-framework-to-guide-un-regulatory-work-on-autonomous-vehicles/doc.html (link as of 2/11/20).

73. TechXplore, "Countries Agree Regulations for Automated Driving", 25 June 2020, https://techxplore.com/news/2020-06-countries-automated.html (link as of 2/11/20).

74. Thomas Macaulay, "Drug Discovery Might be the Best Use of AI to Tackle the Pandemic", TNW, 1 May 2020, https://thenextweb.com/neural/2020/05/01/drug-discovery-might-be-the-best-use-of-ai-to-tackle-the-pandemic/; Jo Best, "AI and the Coronavirus Fight: How Artificial Intelligence is Taking on COVID-19", ZDNet, 9 April 2020, https://www.zdnet.com/article/ai-and-the-coronavirus-fight-how-artificial-intelligence-is-taking-on-covid-19/; Daniela Hernandez, "Coronavirus Trackers Try Out AI Tools as Eyes Turn to Reopening", Wall Street Journal, 19 April 2020, https://www.wsj.com/articles/coronavirus-trackers-try-out-ai-tools-as-eyes-turn-to-reopening-11587294000 (links as of 2/11/20).

75. Mark Maurer, "CFOs Look to Ramp Up Automation Investments Amid Pandemic", Wall Street Journal, 8 April 2020, https://www.wsj.com/articles/cfos-look-to-ramp-up-automation-investments-amid-pandemic-11586338202 (link as of 2/11/20).

76. Tomio Geron, "Manufacturers Use New Technology to Stay Running," Wall Street Journal, 15 June 2020, https://www.wsj.com/articles/manufacturers-use-new-technology-to-stay-running-11592213401; Jane Lanhee Lee, "Call Center AI Firm ASAPP Unveils Funding as COVID-19 Boosts Business", Reuters, 1 May 2020, https://www.reuters.com/article/us-asapp-funding/call-center-ai-firm-asapp-unveils-funding-as-covid-19-boosts-business-idUSKBN22D559 (link as of 2/11/20).

77. John McCormick, "Chatbots Help Texas Officials Cope with Flood of Coronavirus Unemployment Claims", Wall Street Journal, 23 April 2020, https://www.wsj.com/articles/chatbots-help-texas-officials-cope-with-flood-of-coronavirus-unemployment-claims-11587634202 (link as of 2/11/20).

78. Jeff Loucks et al., Thriving in the Era of Pervasive AI, Deloitte's State of AI in the Enterprise, 3rd edition, Deloitte Insights, 2020, https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/about-deloitte/deloitte-cn-dtt-thriving-in-the-era-of-persuasive-ai-en-200819.pdf (link as of 2/11/20).

79. Executive Committee of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, "Statement Regarding the Ethical Implementation of Artificial Intelligence Systems (AIS) for Addressing the COVID-19 Pandemic", IEEE Spectrum, 7 May 2020, https://spectrum.ieee.org/the-institute/ieee-news/statement-regarding-the-ethical-implementation-of-artificial-intelligence-systems-ais-for-addressing-the-covid19-pandemic#.XrXYiLrc1Ws.twitter; see also Ayanna Howard and Jason Borenstein, "AI, Robots, and Ethics in the Age of COVID-19", MIT Sloan Management Review, 12 May 2020, https://sloanreview.mit.edu/article/ai-robots-and-ethics-in-the-age-of-covid-19/ (links as of 2/11/20).

80. Innovation, Science and Economic Development Canada, "Joint Statement from Founding Members of the Global Partnership on Artificial Intelligence", Government of Canada, last updated 15 June 2020, https://www.canada.ca/en/innovation-science-economic-development/news/2020/06/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence.html; European Commission, "Ethics Guidelines for Trustworthy AI", 8 April 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai; Vatican, "Rome Call for AI Ethics", 28 February 2020, http://www.academyforlife.va/content/dam/pav/documenti%20pdf/2020/Assemblea/comunicati%20stampa/01_CS_Rome%20Call%20for%20AI%20Ethics_ENG_10_02_2020.pdf (links as of 2/11/20).

81. Deloitte Center for Technology, Media and Telecommunications, "COVID-19 Outlook for the US Technology Industry", May 2020, https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/covid-19/covid-19-outlook-on-technology-industry.html..html (link as of 2/11/20).

82. Casy Ross, "Hospitals Are Using AI to Predict the Decline of Covid-19 Patients", Stat News, 24 April 2020, https://www.statnews.com/2020/04/24/coronavirus-hospitals-use-ai-to-predict-patient-decline-before-knowing-it-works/ (link as of 2/11/20).

83. Facebook Artificial Intelligence, "Using AI to Detect COVID-19 Misinformation and Exploitative Content", 12 May 2020, https://ai.facebook.com/blog/using-ai-to-detect-covid-19-misinformation-and-exploitative-content (link as of 2/11/20).

84. Danny Palmer, "The Dark Web's Latest Offering: Disinformation as a Service," ZDNet, 1 October 2019 (link as of 2/11/20).

85. Vatican, "Rome Call for AI Ethics", 28 February 2020, http://www.academyforlife.va/content/dam/pav/documenti%20pdf/2020/Assemblea/comunicati%20stampa/01_CS_Rome%20Call%20for%20AI%20Ethics_ENG_10_02_2020.pdf (link as of 2/11/20).

86. Jonah M. Kessel, "Killer Robots Aren't Regulated. Yet.", New York Times, 13 December 2019 (link as of 2/11/20).

87. Kathleen Walch, "Why the Race for AI Dominance Is More Global than You Think", Forbes, 9 February 2020 (link as of 2/11/20).

88. Abishur Prakash, "The Geopolitics of Artificial Intelligence", Scientific American, 11 July 2019 (link as of 2/11/20).

89. Charlotte Jee, "A New US Bill Would Ban the Police Use of Facial Recognition", MIT Technology Review, 26 June 2020; Taylor Hatmaker, "Portland Passes Expansive City Ban on Facial Recognition Tech", TechCrunch, 10 September 2020 (links as of 2/11/20).

90. For example, programmes such as the Technovation Families & AI World Championships, an MIT-designed curriculum to teach middle-school students about AI concepts, and Microsoft's Girls in AI hackathon.

91. Government of Canada, "Directive on Automated Decision Making"; Isabelle Kirkwood, "New Federal Directive Looks to Increase Automated Decision-Making in Government", Betakit, 5 March 2019 (links as of 2/11/20).

92. Unicef, "Generation AI"; Human Rights Center at UC Berkeley School of Law, "Memorandum on Artificial Intelligence and Child Rights" (links as of 2/11/20).

93. New Zealand Ministry of Social Development, "The Privacy, Human Rights and Ethics (PHRaE) Framework" (link as of 2/11/20).

94. Lofred Madzou, Michael Costigan and Kate MacDonald, "Reimagining Regulation for the Age of AI: New Zealand Pilot Project", World Economic Forum, June 2020 (link as of 2/11/20).

95. Université de Montréal, "Montréal Declaration for Responsible Development of Artificial Intelligence", 2018, https://docs.wixstatic.com/ugd/ebc3a3_bfd718945e0945718910cef164f97427.pdf (link as of 2/11/20).

96. University of Helsinki, "Finland Is Challenging the Entire World to Understand AI by Offering a Completely Free Online Course – Initiative Got 1% of the Finnish Population to Study the Basics", 6 September 2018; Silicon Republic, "Finland is Offering a Free Crash Course in AI to Everyone in the EU", 18 December 2019 (links as of 2/11/20).

97. US Food and Drug Administration, "Artificial Intelligence and Machine Learning in Software as a Medical Device", last updated 5 October 2020 (link as of 2/11/20).

98. Government of Singapore, Personal Data Protection Commission, "Model AI Governance Framework", https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework (link as of 2/11/20).

99. IEEE, "IEEE P7011 – News Site Trustworthiness Working Group" (link as of 2/11/20).

100. UK Government Biometrics and Forensics Ethics Group Facial Recognition Working Group, "Ethical Issues Arising from the Police Use of Live Facial Recognition Technology" (link as of 2/11/20).

101. World Economic Forum, "Guidelines for AI Procurement", September 2019; World Economic Forum News Release, "UK Government First to Pilot AI Procurement Guidelines Co-Designed with World Economic Forum", 20 September 2019 (links as of 2/11/20).

102. Port News, "BunkerTrace Secures First Commercial Partnership with Marfin Management", 22 January 2020 (link as of 2/11/20).

103. Nadia Hewett et al, "Redesigning Trust: Blockchain Deployment Toolkit – Ecosystem Overview", World Economic Forum, April 2020.

104. Andrey Shevchenko, "Mastercard Launches Virtual Testing Environment for Central Bank Currencies", Cointelegraph, 9 September 2020 (link as of 2/11/20).

105. Marshall Hayner, "Central Bank Digital Currencies and their Role in the Financial System", Cointelegraph, 22 August 2020 (link as of 2/11/20).

106. Migration Policy Institute, "Global Remittances Guide" (link as of 2/11/20).

107. Mohammad Musharraf, "Bangladesh to Get its First Blockchain Remittance Service", Cointelegraph, 9 September 2020 (link as of 2/11/20).

108. Ibid.

109. Sebastian Sinclair, "Ethereum Classic Suffers Second 51% Attack in a Week", Coindesk, 6 August 2020; see also Felipe Erazo, "Argentinean Gov't Blockchain Hacked to Spread Fake News on Coronavirus", Cointelegraph, 16 March 2020 (links as of 2/11/20).

110. Linda Pawczuk, Jonathan Holdowsky, Rob Massey and Brian Hansen, "Deloitte's 2020 Global Blockchain Survey: From Promise to Reality", Deloitte Insights, 2020 (link as of 2/11/20).

111. European Commission, "Questions and Answers – Commission Steps up Fight against Money Laundering and Terrorist Financing", 7 May 2020; see also Rachel Wolfson, "What the 5th Anti-Money Laundering Directive Means for Crypto Businesses", Cointelegraph, 10 January 2020 (links as of 2/11/20).

112. Kirill Bryanov, "US Federal Government: Confusing Regulation for Crypto, Full Clearance for Blockchain", Cointelegraph, 16 December 2018 (link as of 2/11/20).

113. Kelly Phillips Erb, "IRS Issues New Guidance on the Tax Treatment of Cryptocurrency", Forbes, 9 October 2020 (link as of 2/11/20).

114. Ibid.

115. Scott Schiefelbein and Tyler Greaves, "Uncharted Territory – The State Income Tax Implications of Blockchain Technology and Cryptocurrency", Deloitte (link as of 2/11/20).

116. GS1 US, GS1 Global, "Bridging Blockchains – Interoperability Is Essential to the Future of Data Sharing"(link as of 2/11/20).

117. Emily Perryman, "Blockchain Interoperability Will be Key to Successful Projects this Year", Yahoo Finance, 26 January 2020 (link as of 2/11/20).

118. Linda Pawczuk, Jonathan Holdowsky, Rob Massey and Brian Hansen, "Deloitte's 2020 Global Blockchain Survey: From Promise to Reality", Deloitte Insights, 2020 (link as of 2/11/20).

119. Deloitte, "CFO Insights – Getting Smart about Smart Contracts", June 2016 (link as 2/11/20).

120. Zachary L. Catanzaro and Robert Kain, "The Revolution Will be Memorialized: Selected Blockchain-Based Smart Contract Use Cases", Florida Bar Journal, October 2020 (link as of 2/11/20).

121. John McKinlay, Duncan Pithouse, John McGonagle and Jessica Sanders, "Blockchain: Background, Challenges and Legal Issues", DLA Piper, 2 February 2018; see also Zachary L. Catanzaro and Robert Kain, "The Revolution Will be Memorialized: Selected Blockchain-Based Smart Contract Use Cases", Florida Bar Journal, October 2020 (links as of 2/11/20).

122. Gabrielle Olya, "Food Recalls Cost Millions – and Companies Aren't the Only Ones Paying the Price", Yahoo Finance, 7 December 2018 (link as of 2/11/20).

123. Gary Wollenhaupt, "Why Humans Are Blockchain's Weakest Link", Supply Chain Dive, 29 February 2019 (link as of 2/11/20).

124. Library of Congress, "Regulation of Cryptocurrency Around the World" (link as of 2/11/20).

125. Branko Vlajin, "What You Need to Know about Cloud Laws and Regulations", Cloudwards, 18 May 2018 (link as of 2/11/20).

126. Heather Morton, "Blockchain 2019 Legislation", National Conference of State Legislation, 23 July 2019, https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2019-legislation.aspx; Kirill Bryanov, "US Federal Government: Confusing Regulation for Crypto, Full Clearance for Blockchain", Cointelegraph, 16 December 2018 (links as of 2/11/20).

127. Information Commissioner's Office, "Right to Erasure" (link as of 2/11/20).

128. Mike Miliard, "As Blockchain Proves Its Worth for Healthcare, Regulatory Questions Remain", Healthcare IT News, 11 December 2018 (link as of 2/11/20).

129. Internal Revenue Service, "Virtual Currency: IRS Issues Additional Guidance on Tax Treatment and Reminds Taxpayers of Reporting Obligations", 9 October 2019; and Anna Baydakova, "The IRS Just Issued Its First Cryptocurrency Tax Guidance in 5 Years", Coindesk, 9 October 2019 (links as of 2/11/20).

130. HM Revenue & Customs, "Cryptoassets: Tax for Individuals", 20 December 2019 (link as of 2/11/20).

131. Digiconomist, "Bitcoin Energy Consumption Index" (link as of 2/11/20).

132. Ibid.

133. Corrie E. Clark and Heather L. Greenley, "Bitcoin, Blockchain and the Energy Sector", Congressional Research Service, 9 August 2019 (link as of 2/11/20).

134. Indiana Lee, "Renewable Energy and Blockchain", Energy Central, 3 April 2020.

135. Fernando Sanchez, "How Blockchain Can Uphold Creators' Rights and Copyright Law", Blockchain News, 14 March 2020 (link as of 2/11/20).

136. Jonathan M. Holdowsky, Aureen Mandal, Michael Severin, Amin Bensadok, Imran Khan, Kshitish Balhotra, Utsavi Pathak and Jordan Eng, "Libra: Shaping the Evolution of Financial Infrastructure", Deloitte Insights (link as of 2/11/20).

137. World Economic Forum, "Platform for Good Digital Identity" (link as of 2/11/20).

138. Columbia Business School, "Regulatory Sandboxes" (link as of 2/11/20).

139. Paul Muir, "Singapore Firm Graduates from Regulatory Sandbox", Asia Times, 4 February 2020 (link as of 2/11/20).

140. Felipe Erazo, "South Korea's Fintech Sandbox Creates 380 New Blockchain Jobs", Cointelegraph, 15 May 2020 (link as of 2/11/20).

141. Financial Conduct Authority, "Regulatory Sandbox – Cohort 6", 14 October 2020 (link as of 2/11/20).

142. Japan Virtual and Crypto Assets Exchange Association, "Statistics", https://jvcea.or.jp/about/statistics/; see also Japan Virtual and Crypto Assets Exchange Association, "Main Info", 12 June 2020, https://jvcea.or.jp/news/main-info/20200612-001/; and David Hamilton, "Japan FSA Approves 2 New Blockchain Associations", Securities, 4 May 2020 (links as of 2/11/20).

143. Olga Kharif, "Bermuda Dives Deeper into Crypto with Stimulus Coin Test Program", Bloomberg, 1 September 2020 (link as of 2/11/20).

144. Sandali Handagama, "Government of Bermuda Pilots Stimulus Token in Response to COVID-19 Crisis", Coindesk, 1 September 2020 (link as of 2/11/20).

145. FTS Newsdeck, "Government of Bermuda Pilots Digital Stimulus Token in Collaboration with Stablehouse", Global Fintech series, 2 September 2020 (link as of 2/11/20).

146. Digital Monetary Institute, "Asia Takes Off", August 2020; see also Bank of Thailand, "Enhancing Bond Lifecycle Functionalities & Programmable Compliance Using Distributed Ledger Technology"; and Hong Kong Monetary Authority, "Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments" (links as of 2/11/20).

147. Binance Research, "First Look: China's Central Bank Digital Currency", 28 August 2019; see also Veta Chan, "An Absolute Necessity: Why this Expert Says China Desperately Needs a Digital Currency", Fortune, 30 July 2020; and Robert Murray, "Understanding China's Digital Yuan", Foreign Research Policy Institute (links of as 2/11/20).

148. Martin Neil Bailey et al., "The Origins of the Financial Crisis", Initiative on Business and Public Policy at Brookings, the Brookings Institution, November 2008.

149. Bruce Schneier, "Testimony at the US House of Representatives Joint Hearing 'Understanding the Role of Connected Devices in Recent Cyber Attacks'", Schneireronsecurity.com, 16 November 2016, https://www.schneier.com/essays/archives/2016/11/testimony_at_the_us_.html (link as of 2/11/20).

150. "About UL", https://www.ul.com/about (link as of 5/11/12).

151. For Finland's IoT labeling effort, see Sarah Coble, "Finns Label Cyber-Secure IoT Devices", Infosecurity-magazine.com, November 2019, https://www.infosecurity-magazine.com/news/finns-label-cybersecure-iot-devices/; and for the UK's related effort, see Sooraj Shah, "UK Government Proposes IoT Security and Device Labelling Scheme", internetofbusiness.com, March 2018, https://internetofbusiness.com/uk-government-proposes-iot-security-measures-and-device-labelling-scheme/ (links as of 2/11/20).

152. Better IoT, "Making Good Design Actionable", https://betteriot.wordpress.com/ (link as of 2/11/20).

153. FATF Recommendations, "FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High-Level Principles and Procedures", Financial Action Task Force, 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html (link as of 2/11/20).

154. While progress has been slow for grey list countries such as Pakistan, simply appearing on the list seems to have been a motivator to reform for others such as Iceland and Malta (links as of 2/11/20).

155. Robert Puentes, "COVID's Differing Impact on Transit Ridership", Eno Center for Transportation, 24 April 2020 (link as of 2/11/20).

156. "COVID-19 Transportation Trends", INRIX (link as of 2/11/20).

157. Christina Goldbaum, "Thinking of Buying a Bike? Get Ready for a Long Wait", The New York Times, 18 May 2020 (link as of 2/11/20).

158. Kelly Yamanouchi, "UPS Grapples with Christmas-like Shipping Surge amid Coronavirus", Atlanta Journal-Constitution, 8 June 2020.

159. Scott Corwin et al. "The Futures of Mobility after COVID-19", Deloitte Insights, 21 May 2020, https://www2.deloitte.com/content/dam/insights/us/articles/6739_fom-covid/DI_FoM-COVID.pdf (link as of 2/11/20).

160. Jonathan I. Dingel and Brent Neiman, "How Many Jobs Can Be Done at Home?" no. w26948, National Bureau of Economic Research, 2020, https://www.nber.org/papers/w26948 (link as of 2/11/20).

161. Hugh M. Clark, "Who Rides Public Transportation?", American Public Transportation Association, January 2017.

162. Janette Sadik-Khan and Seth Solomonow, "Fear of Public Transit Got Ahead of the Evidence", The Atlantic, 14 June 2020 (link as of 2/11/20).

163. Scott Corwin et al. "The Futures of Mobility after COVID-19", Deloitte Insights, 21 May 2020, https://www2.deloitte.com/content/dam/insights/us/articles/6739_fom-covid/DI_FoM-COVID.pdf (link as of 2/11/20).

164. Christina Goldbaum, "NY Subway, Facing a $16 Billion Deficit, Plans for Deep Cuts", The New York Times, 21 July 2020 (link as of 2/11/20).

165. World Economic Forum, "Designing a Seamless Integrated Mobility System (SIMSystem)", January 2018, http://www3.weforum.org/docs/Designing_SIMSystem_Manifesto_Transforming_Passenger_Goods_Mobility.pdf (link as of 2/11/20).

166. Adapted from World Economic Forum, "Activating a Seamless Integrated Mobility System (SIMSystem)", January 2020 (link as of 2/11/20).

167. Chris Teale, "Officials: Federal AV Law Should Not Stop Cities from Regulating Tech", Smart Cities Dive, 12 February 2020 (link as of 2/11/20).

168. Philip Koopman and Michael Wagner, "Challenges in Autonomous Vehicle Testing and Validation", SAE International Journal of Transportation Safety 4, no. 2016-01-0128 (2016): 15–24. As the authors note, "Another issue with validating machine learning is that, in general, humans cannot intuitively understand the results of the process."

169. World Business Council for Sustainable Development, "The First-Ever Corporate Mobility Pact – Catalyzing Corporate Action to Transform Mobility", World Business Council for Sustainable Development, October 2019, https://www.wbcsd.org/Programs/Cities-and-Mobility/Transforming-Mobility/News/The-first-ever-Corporate-Mobility-Pact-catalyzing-corporate-action-to-transform-mobility (link as of 2/11/20).

170. Transport for London, "TfL's Free Open Data Boosts London's Economy", 13 October 2017, https://tfl.gov.uk/info-for/media/press-releases/2017/october/tfl-s-free-open-data-boosts-london-s-economy (link as of 2/11/20).

171. Ibid.

172. Kyle Wiggers, "Nuro's R2 Receives First Autonomous Vehicle Exemption from the US Department of Transportation", Venture Beat, 6 February 2020 (link as of 2/11/20).

173. Joseph Kolly and Tim Czapp, "Partnership for Analytics Research in Traffic Safety (PARTS): Demonstrating the Value of the Partnership", SAE International Government Industry Meeting, 3–5 April 2019 (link as of 2/11/20).

174. US Department of Transportation, "US Transportation Secretary Elaine L. Chao Announces New Initiatives to Improve Safety on America's Roads", press release, 15 January 2020 (link as of 2/11/20).

175. Bryan Walsh, "Coronavirus Brings the Age of Drones Closer", axios.com, 30 May 2020, https://www.axios.com/coronavirus-drones-pandemic-surveillance-cbd80f98-4b86-49bd-806f-8e86ec42e3aa.html; see also Harrison Wolf, "We're about to see the Golden Age of Drone Delivery – Here's Why", weforum.org, July 2020, https://www.weforum.org/agenda/2020/07/golden-age-drone-delivery-covid-19-coronavirus-pandemic-technology/ (links as of 2/11/20).

176. Bryan Walsh, "Coronavirus Brings the Age of Drones Closer", axios.com, May 2020, https://www.axios.com/coronavirus-drones-pandemic-surveillance-cbd80f98-4b86-49bd-806f-8e86ec42e3aa.html (link as of 2/11/20).

177. International Civil Aviation Organization, "Introduction to ICAO Model UAS Regulations and Advisory Circulars", https://www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx (link as of 2/11/20).

178. International Civil Aviation Organization, "Unmanned Aircraft Systems (UAS) for Humanitarian Aid and Emergency Response Guidance", https://www.icao.int/safety/UA/UAID/Documents/ICAO%20U-AID%20Guidance%20Material.pdf (link as of 2/11/20).

179. Federal Aviation Administration, "Unmanned Aircraft System Traffic Management (UTM)", https://www.faa.gov/uas/research_development/traffic_management/; see also SESAR, "U-space", sesarju.eu, https://www.sesarju.eu/U-space (links as of 2/11/20).

180. SESAR, "U-space", sesarju.eu, https://www.sesarju.eu/U-space (link as of 2/11/20).

181. NASA Urban Air Mobility, "Urban Air Mobility (UAM) Market Study", Nasa.gov, November 2018, https://www.nasa.gov/sites/default/files/atoms/files/uam-market-study-executive-summary-v2.pdf (link as of 2/11/20).

182. Maryanne Buechner, "UNICET's Ascent into the Drone Age", Unicef.org, 12 June 2018, https://www.unicefusa.org/stories/unicefs-ascent-drone-age/34436 (link as of 2/11/20).

183. Tech Wire Asia, "Japan May Set up Regulatory Sandboxes to Test Drones, Self-Driving Vehicles", techwireasia.com, October 2017, https://techwireasia.com/2017/10/japan-may-set-regulatory-sandboxes-test-drones-self-driving-vehicles/ (link as of 2/11/20).

184. Federal Aviation Administration, "UAS Remote Identification", March 2020, https://www.faa.gov/uas/research_development/remote_id/ (link as of 2/11/20).

185. Ibid.

186. International Civil Aviation Organization, "Making an ICAO Standard", November 2011, https://www.icao.int/safety/airnavigation/Pages/standard.aspx (link as of 2/11/20).

187. For more on ICAO SARPs, including how they influence ICAO members, see "Convention on International Civil Aviation", 7 December 1944, UNTS 15, 295, Article 37–38; and David Mackenzie, ICAO: A History of the International Civil Aviation Organization, Toronto: University of Toronto Press, 2010, 193–194.

188. International Civil Aviation Organization, "Unmanned Aircraft Systems (UAS) for Humanitarian Aid and Emergency Response Guidance", https://www.icao.int/safety/UA/UAID/Documents/ICAO%20U-AID%20Guidance%20Material.pdf; and International Civil Aviation Organization, "Introduction to ICAO Model UAS Regulations and Advisory Circulars", https://www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx (links as of 2/11/20).

189. Drone Pilot Ground School, "How to Get Drone Flights Approved in Controlled Airspace With LAANC", dronepilotgroundschool.com, July 2019, https://www.dronepilotgroundschool.com/faa-laanc-authorization/ (link as on 2/11/20).

190. Miriam McNabb, "Switzerland's U-Space: Enabling a 'Safe and Open Drone Economy' with Aviation Data Exchange Hub", dronelife.com, August 2019, https://dronelife.com/2019/08/06/switzerlands-u-space-enabling-a-safe-and-open-drone-economy-with-aviation-data-exchange-hub/ (link as of 2/11/20).

191. Andre Orban, "The New Droneguide App Version, Compulsory for Professionals in Belgium, is a World-First", aviation24.be, September 2019, https://www.aviation24.be/air-traffic-control/skeyes/the-new-droneguide-app-version-compulsory-for-professionals-in-belgium-is-a-world-first/ (link as of 2/11/20).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org