Deloitte.

Global Technology Governance Report 2021

Harnessing Fourth Industrial Revolution technologies in a COVID-19 world

In collaboration with the World Economic Foum

Deloitte Center *for* Government Insights

Introduction

The recovery from COVID-19 has triggered a tsunami of innovations in work, collaboration, distribution, and service delivery—and shifted many customer behaviors, habits, and expectations. Several of the emerging technologies of the Fourth Industrial Revolution (4IR), including artificial intelligence (AI), mobility (including autonomous vehicles), blockchain, drones, and the Internet of Things (IoT), have been at the center of these innovations and are likely to play an outsized role in what emerges postpandemic. These technologies power applications that are revolutionary, in turn creating a self-reinforcing cycle that spins like a flywheel, surging on its own momentum.

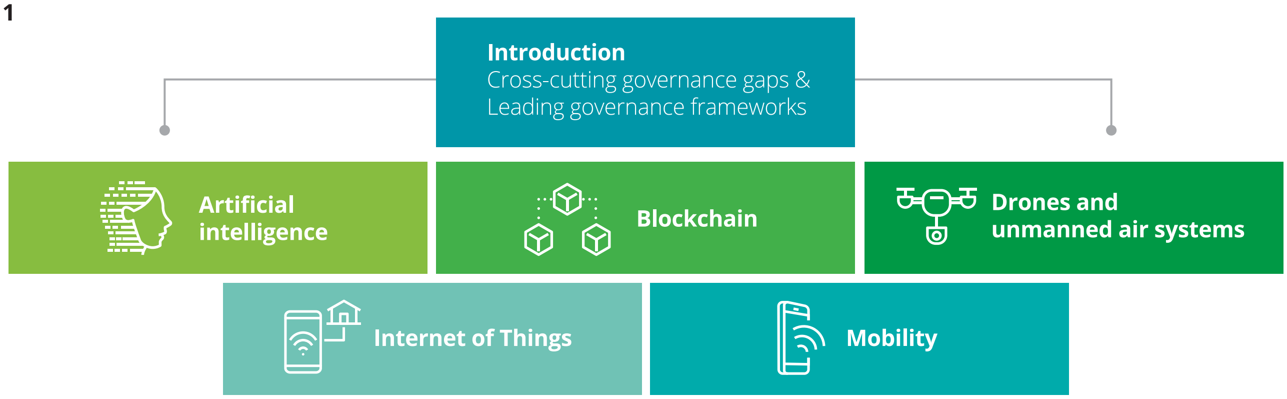
Artificial intelligence and data analytics have helped Taiwan predict the risk of infection.[1] China has used drones and robots to minimize human contact.[2] The United Arab Emirates (UAE) is leveraging blockchain to provide seamless digital services to its citizens.[3] The United States is using autonomous vehicles to deliver test samples to processing labs.[4] Many countries are using mobile apps as sensors for contact tracing.[5]

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. Artificial intelligence doesn't quite fit into existing regulatory frameworks. International blockchain ledgers may violate existing national financial laws. Drones and IoT have the potential to cause privacy concerns. Autonomous vehicles may change traditional safety risks. All of these disruptions translate into a suite of technologies and capabilities poised to slip through gaps in governance.

How governments and other stakeholders approach the governance of 4IR 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 4IR technology development while mitigating the risks of unethical or malicious uses.

With this in mind, the World Economic Forum worked with Deloitte to produce a practical handbook to examine some of the most important applications of 4IR technologies for thriving in a postpandemic world and governance challenges that should be addressed for these technologies to reach their full potential. The report is not an 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: AI, mobility (including autonomous vehicles), blockchain, drones, and IoT.[6]

Figure 1



Introduction
Cross-cutting governance gaps &
Leading governance frameworks

Artificial intelligence

Blockchain

Drones and unmanned air systems

Internet of Things

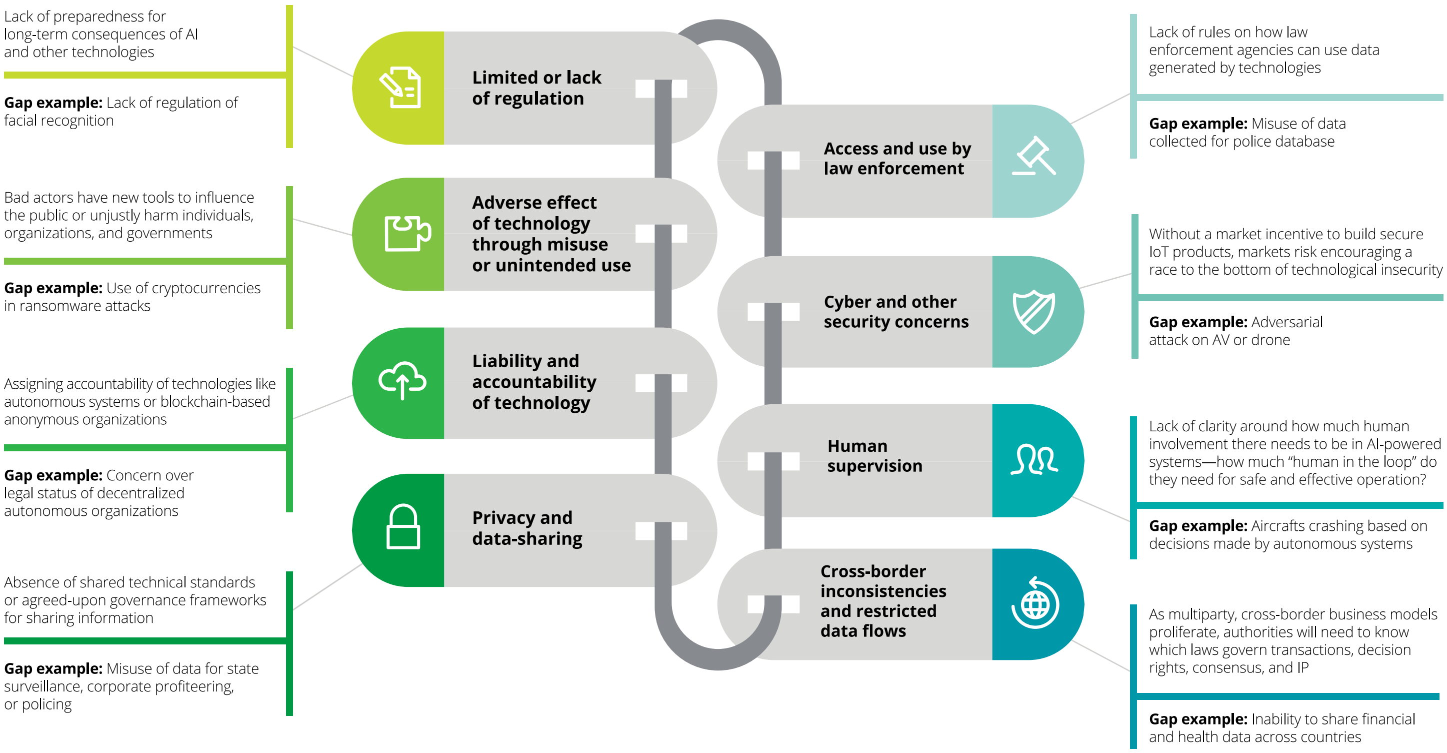
Mobility

Cross-cutting technology governance challenges

From drones to IoT, each individual technology presents its own unique set of governance challenges, many of which are detailed in the full version of this study. Our analysis also revealed a host of common challenges across the five 4IR technologies we focused on. While many predated COVID-19, the pandemic and its aftermath have accelerated the urgency of addressing them.

- Limited or lack of regulation
- Adverse effect of technology through misuse or unintended use
- Liability and accountability of 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


Limited or lack of regulation
Adverse effect of technology through misuse or unintended use
Liability and accountability of 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

Lack of preparedness for long-term consequences of AI and other technologies

Gap example: Lack of regulation of facial recognition

Bad actors have new tools to influence the public or unjustly harm individuals, organizations, and governments

Gap example: Use of cryptocurrencies in ransomware attacks

Assigning accountability of technologies like autonomous systems or blockchain-based anonymous organizations

Gap example: Concern over legal status of decentralized autonomous organizations

Absence of shared technical standards or agreed-upon governance frameworks for sharing information

Gap example: Misuse of data for state surveillance, corporate profiteering, or policing

Lack of rules on how law enforcement agencies can use data generated by technologies

Gap example: Misuse of data collected for police database

Without a market incentive to build secure IoT products, markets risk encouraging a race to the bottom of technological insecurity

Gap example: Adversarial attack on AV or drone

Lack of clarity around how much human involvement there needs to be in AI-powered systems—how much "human in the loop" do they need for safe and effective operation?

Gap example: Aircrafts crashing based on decisions made by autonomous systems

As multiparty, cross-border business models proliferate, authorities will need to know which laws govern transactions, decision rights, consensus, and IP

Gap example: Inability to share financial and health data across countries

Source: Deloitte analysis

Limited or lack of regulation

From facial recognition technology that generates false matches[7] to hackers who target IoT-enabled smart devices,[8] many regulatory bodies are unprepared for the legal consequences that could arise from the use of 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.

Adverse effect of technology through misuse or unintended use

Technology that creates opportunities for growth and innovation also often creates opportunities for misuse. Even large cities have fallen prey to bitcoin-enabled ransomware attacks, for example.[9] Algorithms and AI allow us to withdraw cash from ATMs, increase agricultural yield, prioritize environment remediation, and even save lives. However, without effective governance, such technologies can have adverse consequences. These can range from the accidental, such as a simple coding error,[10] to the nefarious, like so-called deepfake videos, in which politicians, celebrities, or news anchors can be made to appear as if they have said things they did not.

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? Medical software incorrectly diagnoses 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.[11]

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.[12]

But looking at data through only 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 technologies meet their potential. Consumers, public authorities, and private companies can all share key data in order to fully benefit from 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 shared.

Access and use by law enforcement

The issue of data-sharing and access is particularly pronounced in law enforcement, especially when it comes to technologies such as facial recognition.[13] Most governance frameworks do not currently advise law enforcement agencies on how they can use the data generated by technologies like IoT and drones. Can police interrogate personal virtual assistants? Use the inadvertent crime scene captured by a delivery drone? Use AI to scour cell phone location data?[14]

To increase trust in new technologies (and law enforcement) governments should determine how to balance the privacy of residents with lawful access to data.

Cyber and other security concerns

The more potent the technology, the more dangerous its misuse. Hackers who access AI-based systems can modify decisions or outcomes, such as by tricking a combat drone into misclassifying a crowded civilian space for an enemy or hacking autonomous vehicles to create gridlock.[15]

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

Human supervision

Should AI-powered systems be used only to augment human action and judgment, or should they also be used to power autonomous systems? There is considerable debate around 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.

Aircraft have crashed and ships have broken down due to decisions made by autonomous systems,[16] highlighting the need for a backup human driver. But while there may be a need for more human involvement in some cases, 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 less desirable than a fully autonomous system in the context of COVID-19.

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, which increases both the difficulty (of designing an effective blockchain, for example) and the risk that existing technologies will be noncompliant.

Further, many countries have restrictions around data-sharing, especially related to finance and health care.[17] However, data is a vital ingredient for technologies like AI, autonomous vehicles, and blockchain, and restricting its flow can inhibit the growth of data-dependent fields.

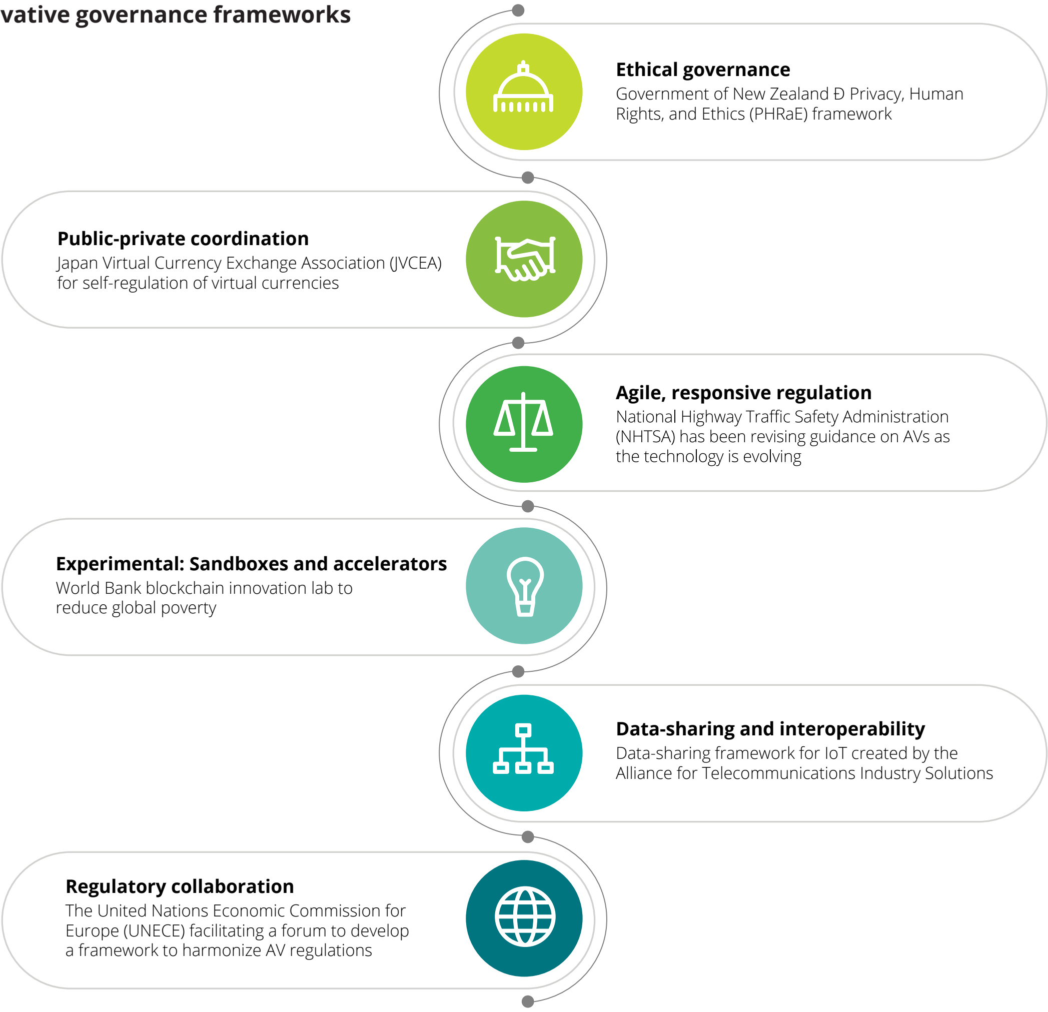
As multiparty, cross-border blockchain business models proliferate, authorities will need to be well-versed in the various laws governing transactions, decision rights, consensus, and IP.

Refer to the full report to read more about governance gaps relating to AI, mobility, blockchain, drones, and IoT.

Innovative governance frameworks

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 full report. Additionally, our analysis found a number of common themes across the areas of technology discussed in this report.

Figure 3. Innovative governance frameworks



Ethical governance
Government of New Zealand Ð Privacy, Human Rights, and Ethics (PHRaE) framework

Public-private coordination
Japan Virtual Currency Exchange Association (JVCEA) for self-regulation of virtual currencies

Agile, responsive regulation
National Highway Traffic Safety Administration (NHTSA) has been revising guidance on AVs as the technology is evolving

Experimental: Sandboxes and accelerators
World Bank blockchain innovation lab to reduce global poverty

Data-sharing and interoperability
Data-sharing framework for IoT created by the Alliance for Telecommunications Industry Solutions

Regulatory collaboration
The United Nations Economic Commission for Europe (UNECE) facilitating a forum to develop a framework to harmonize AV regulations

Source: Deloitte analysis

Ethical governance

Many countries, including New Zealand[18] and the United Kingdom,[19] have developed ethical governance frameworks that provide guidelines on how to responsibly develop emerging technologies. The European Commission, in coordination with other European agencies and member states, has also released guidelines and a toolbox for designing and developing COVID-19 contact tracing apps.[20]

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, cocreated regulation, and, where appropriate, self-regulation.

Japan's Financial Services Agency (FSA), for example, has empowered the country's cryptocurrency industry to self-regulate and police domestic exchanges. The public-private body is authorized to establish binding guidelines on behalf of the cryptocurrency industry[21] and periodically releases data on trading volume and the value of cryptocurrencies for transparency's sake.[22]

Public-private coordination has also become more evident than before in various governments' response to COVID-19. For example, the United Kingdom formed a task force of pharmaceutical companies, regulators, and academics to facilitate the rapid development of vaccines for COVID-19.[23]

Agile, responsive regulation

Typically, regulations aren't "future-proof." They tend to be prescriptive in nature, take months or years to enact, 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.

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

This could mean regulation that checks its effectiveness against user feedback. For example, the National Highway Traffic Safety Administration has revised its guidelines for autonomous vehicles four times in as many years based on feedback from industry participants.[24] Meanwhile, India's Ministry of Health and Family Welfare announced guidelines in response to COVID-19 that allow registered medical practitioners to deliver services via telemedicine.[25]

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), for instance, has divided drone regulations into three categories based on the risks they pose and adjusted regulations accordingly,[26] while the city of Lisbon has done the same for new transit technologies.[27]

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 allows firms to test their models and develop proofs of concept.

The United Kingdom employed a sandbox model to encourage financial organizations to innovate during the pandemic.[28] Meanwhile, many countries are piloting sandbox approaches for drones as the role they can play in moving medical supplies, minimizing human contact, and supplying essentials to remote areas becomes apparent. [29]

Data-sharing and interoperability

Since many technologies rely on data to refine their operations, more data should mean better results. But the data employed by 4IR technologies is often sensitive information, which is hampered by differing rules across borders and sometimes stored in formats that are incompatible.

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 while maintaining ethical guardrails.[30]

Meanwhile, Finland revised its Transport Code to make public transit data available via open APIs, allowing commuters to plan, book, and pay for multimodal trips via single application interface.[31]

Regulatory collaboration

Because emerging technologies permeate national boundaries, regulating them calls for collaboration across agencies within a country, as well as cross-border collaboration.[32]

To operate effectively on a global scale, companies need a standard framework and guidelines at the international level, such as the regulatory convergence seen in the fintech sector over the past few years.[33]

International bodies also have a vital role to play in setting global standards. For instance, the United Nations Economic Commission for Europe (UNECE) facilitated a forum where China, the European Union, Japan, and the United States came together to develop a framework for harmonizing autonomous vehicle regulations.[34]

When faced with rapidly adapting technologies, regulators must also learn to rapidly adapt, nurturing 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.

You can read the full report on the World Economic Forum website. The report also contains summaries of governance gaps and emerging governance frameworks specific to the 4IR technologies listed below.

- **AI**
- **Mobility**
- **Blockchain**
- **Drones**
- **IoT**

Endnotes

1. David Alexander Walcot, "How the Fourth Industrial Revolution can help us beat COVID-19," World Economic Forum, May 7, 2020.
2. Ibid.
3. Wilbur Rodgers, "UAE adopts digital identity and blockchain to fight COVID-19," March 30, 2020.
4. GCN, "Autonomous vehicles deliver COVID-19 tests to lab," April 8, 2020.
5. Gadgets 360, NDTV, "Coronavirus contact tracing apps: which countries are doing what," May 31, 2020.
6. World Economic Forum, "Centre for the Fourth Industrial Revolution: Platforms," accessed October 5, 2020.
7. Kashmir Hill, "Wrongfully Accused by an Algorithm," *New York Times*, August 3, 2020.
8. Bruce Schneier, "Testimony at the US House of Representatives Joint Hearing 'Understanding the Role of Connected Devices in Recent Cyber Attacks'," Schneireronsecurity.com, November 16, 2016.
9. Matthew Beedham, "Report: Cryptocurrency ransomware payments up 90%, thanks to Ryuk," Thenextweb.com, April 18, 2019.
10. Colin Lecher, "What happens when an algorithm cuts your health care," Verge, March 21, 2018.
11. Philip Koopman and Michael Wagner, "Challenges in autonomous vehicle testing and validation," *SAE International Journal of Transportation Safety* 4, no. 2016-01-0128 (2016): pp. 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."
12. Neha Mule, "Americans avoid to download contact tracing apps amid data privacy concerns," *Smart Industry News*, June 19, 2020.
13. Mark Sullivan, "Privacy groups want a federal facial-recognition ban, but it's a long shot," *Fast Company*, January 28, 2020.
14. Mihalis Kritikos, *Ten technologies to fight coronavirus*, European Parliament, April 2020.
15. Marcus Comiter, Attacking artificial intelligence: AI's security vulnerability and what policymakers can do about it, harvard belfer center, August 2019.
16. Lance Eliot, "Human in-the-loop vs. out-of-the-loop in AI systems: The case of AI self-driving cars," *AI Trends*, April 9, 2019, accessed February 28, 2020.
17. Daniel Castro and Alan McQuinn, *Cross-border data flows enable growth in all industries, information and technology innovation foundation*, February 2015.
18. New Zealand Ministry of Social Development, The Privacy, Human Rights and Ethics (PHRaE) Framework.
19. Biometrics and Forensics Ethics Group, Facial Recognition Working Group, United Kingdom, *Ethical issues arising from the police use of live facial recognition technology*, 2019
20. Mihalis Kritikos, *Ten technologies to fight coronavirus*, European Parliament, April 2020.
21. Samburaj Das, "Japan approves self-regulation for cryptocurrency industry," CCN, October 24, 2018, last modified January 24, 2020.
22. Japan Virtual and Crypto Assets Exchange Association, "Statistics," accessed August 30, 2020; also see Japan Virtual and Crypto Assets Exchange Association, "Main info," June 12, 2020.

Endnotes

23. Emma Morriss, “Government launches coronavirus vaccine taskforce as human clinical trials start,” *Pharmafield*, April 22, 2020.

24. US Department of Transportation, *Ensuring American leadership in automated vehicle technologies: Automated vehicles 4.0*, January 8, 2020, accessed March 9, 2020.

25. Akanki Sharma, “Transforming Indian healthcare via telemedicine,” *Express Healthcare*, April 9, 2020; William D. Eggers et al., “How governments can navigate a disrupted world: Foresight, agility, and resilience,” Deloitte Insights.

26. Drone Rules, “EU Regulations Updates,” accessed March 9, 2020.

27. “The first-ever Corporate Mobility Pact—catalyzing corporate action to transform mobility,” World Business Council for Sustainable Development, October 15, 2019.

28. Financial Conduct Authority, “Digital sandbox – coronavirus pilot,” July 16, 2020.

29. Maryanne Buechner, “UNICEF’s ascent into the drone age,” UNICEF.org, June 12, 2018.

29. Aaron Boyd, “10 drone programs get federal OK to break the rules,” NextGov, May 9, 2018.

29. Ibid.

29. AUVSI, “Skyports to trial BVLOS flights in non-segregated airspace after joining uk caa regulatory sandbox,” April 15, 2020.

30. Courtney Bjorlin, “new framework helps promote IoT data sharing among smart cities,” IoT World Today, March 2, 2018.

31. Warwick Goodall et al., “The rise of mobility as a service,” Deloitte Center for Government Insights, January 23, 2017.

32. Organisation for Economic Co-operation and Development, International Regulatory Co-operation: Adapting rulemaking for an interconnected world, October 2018.

33. Christine Horton, “Are the fintech bridges working?” *Raconteur*, December 15, 2019.

34. United Nations Economic Commission for Europe, “Safety at core of new Framework to guide UN regulatory work on autonomous vehicles,” September 4, 2019.

Contacts

William D. Eggers

Executive Director, Deloitte Center for Government Insights - US

weggers@deloitte.com

Matt Gracie

Solution Leader - US

magracie@deloitte.com

Keith Davis

Solution Leader - Canada

keidavis@deloitte.ca

Michael Theill

Solution Leader - Denmark

mtheill@deloitte.dk

Ursula Brennan

Solution Leader - Australia

ubrennan@deloitte.com.au

Hans Verheggen

Solution Leader - EU

hverheggen@deloitte.com

Walter Carlton

Solution Leader - UK

wcarlton@deloitte.co.uk

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States, and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Copyright © 2020 Deloitte Development LLC. All rights reserved.