In collaboration with the Global Internet of Things Council and PwC

WORLD ECONOMIC FORUM

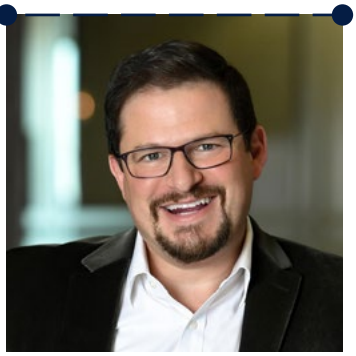
State of the Connected World
2020 Edition

INSIGHT REPORT

DECEMBER 2020

Contents

Foreword



Cristiano Amon
Co-Chair of Global Internet of Things Council; President, Qualcomm Incorporated

Stella Ndabeni-Abrahams
Co-Chair of Global Internet of Things Council; Minister of Communications and Digital Technologies, Republic of South Africa

Adrian Lovett
Co-Chair of Global Internet of Things Council; President and Chief Executive Officer, World Wide Web Foundation

Mohamed Kande
Vice-Chair, Global Advisory Leader, PwC

In January 2019, a small group of global leaders from the public and private sectors convened at the World Economic Forum's Annual Meeting in Davos to reflect on how internet-enabled devices, commonly referred to as the internet of things (IoT), were transforming and disrupting the way we live and work.

While our backgrounds and points of view were broad and varied, we were united by a shared sense of purpose to help realize the full potential and promise of these critical technologies. We acknowledged that the road ahead would not be without obstacles. Indeed, it had been 30 years since Tim Berners-Lee helped bring the internet within reach of everyone with the invention of the world wide web, yet a significant segment of the world remains unable to access these benefits.

To help build a connected world that benefits all, we established the Global IoT Council. The Council members span the public and private sectors, representing 13 countries on five continents, seven industries, an equal mix of men and women, and a combination of executive leaders and subject-matter experts. Never before has such a diverse group of leaders from business, government, civil society and academia come together to discuss the current state of IoT, let alone to chart its future direction.

At the Council's inaugural meeting in April 2019, it was clear that there was a diversity of views about the opportunity and potential risks of connected technology. Yet we all agreed that themes related to privacy, security and equitable access required greater attention. The

events of 2020 – COVID-19, climate-related natural disasters and economic instability – have raised this need for collective action from urgent to absolutely necessary.

This report is the product of a year-long effort by the World Economic Forum and Global IoT Council, in collaboration with PwC, to better understand how IoT is viewed around the world and to establish clear priorities for action. The findings of this research underscore many of the differences in perception and viewpoints that first surfaced within the Council. We see this diversity as a strength that highlights the importance of greater public-private collaboration. We also see clear areas of alignment: a shared resolve to build transparency and trust into the heart of IoT technologies, a commitment to ensure that public privacy and security is protected, a responsibility to enable equal access for all, a desire to incentivize the use of IoT to help solve humankind's biggest challenges, and a determination to bring people together to create a global consensus on these critical issues.

With the release of this report, we embark on the next phase of this shared mission to address and track the most pressing governance gaps facing the development of IoT. We look forward to sharing regular updates along the way and we invite you to join us as we chart a course towards a more connected world that benefits all.

Executive summary

Spurred by continued technological advancement, the world today is more connected than ever. This presents a tremendous opportunity to build a more sustainable and prosperous future for all, but it also introduces new risks and governance challenges in areas such as security, privacy and the fair distribution of benefits.

The global COVID-19 pandemic has made this abundantly clear. COVID-19 has highlighted the essential role the internet of things (IoT) has come to play in our lives. IoT applications such as connected thermal cameras, contact tracing devices and health-monitoring wearables are providing critical data needed to help fight the disease. while temperature sensors and parcel tracking will help ensure that sensitive COVID-19 vaccines are distributed safely. Yet the use of IoT in fighting the pandemic has also shed light on concerns about its security, privacy, interoperability and equity.

This inaugural report on the state of the connected world was initiated by the World Economic Forum and the Global IoT Council, which consists of key stakeholders from the global IoT industry in the public and private sectors and civil society. It aims to take a comprehensive look at the most pressing opportunities and challenges facing the IoT ecosystem based on extensive multistakeholder input and discussions. Our research makes clear that we are at a pivotal moment, when the development, use and governance of these technologies is rapidly changing and evolving. The main findings include, but are not limited to, the following.

1. The COVID-19 pandemic is changing the face of IoT, introducing new use cases and applications, bolstering demand in select areas such as health technology and the smart home while temporarily slowing adoption in areas such as traditional enterprise IoT.
2. The ways in which IoT is being used to help manage and respond to COVID-19 hold the potential to spur and accelerate new opportunities to boost organizational and individual resilience and flexibility, and to respond more effectively to future challenges, instability and emergencies. However, it also brings with it risks for privacy and other human rights that need to be thoroughly assessed and addressed through proper governance structures.
3. The IoT market and ecosystem is expected to grow even faster in a new post-COVID-19 business environment, thanks to the release of pent-up demand and the determination to minimize the impacts from future disruptions, especially in the enterprise and public spaces domains.
4. The maturity of IoT governance – the laws, industry standards and self-governance approaches required to mitigate potential harm – continues to lag behind the pace of technological change. The largest perceived gap in governance relates to ensuring

IoT technologies become a force for shared societal benefit, as opposed to exacerbating the digital divide and existing inequalities.

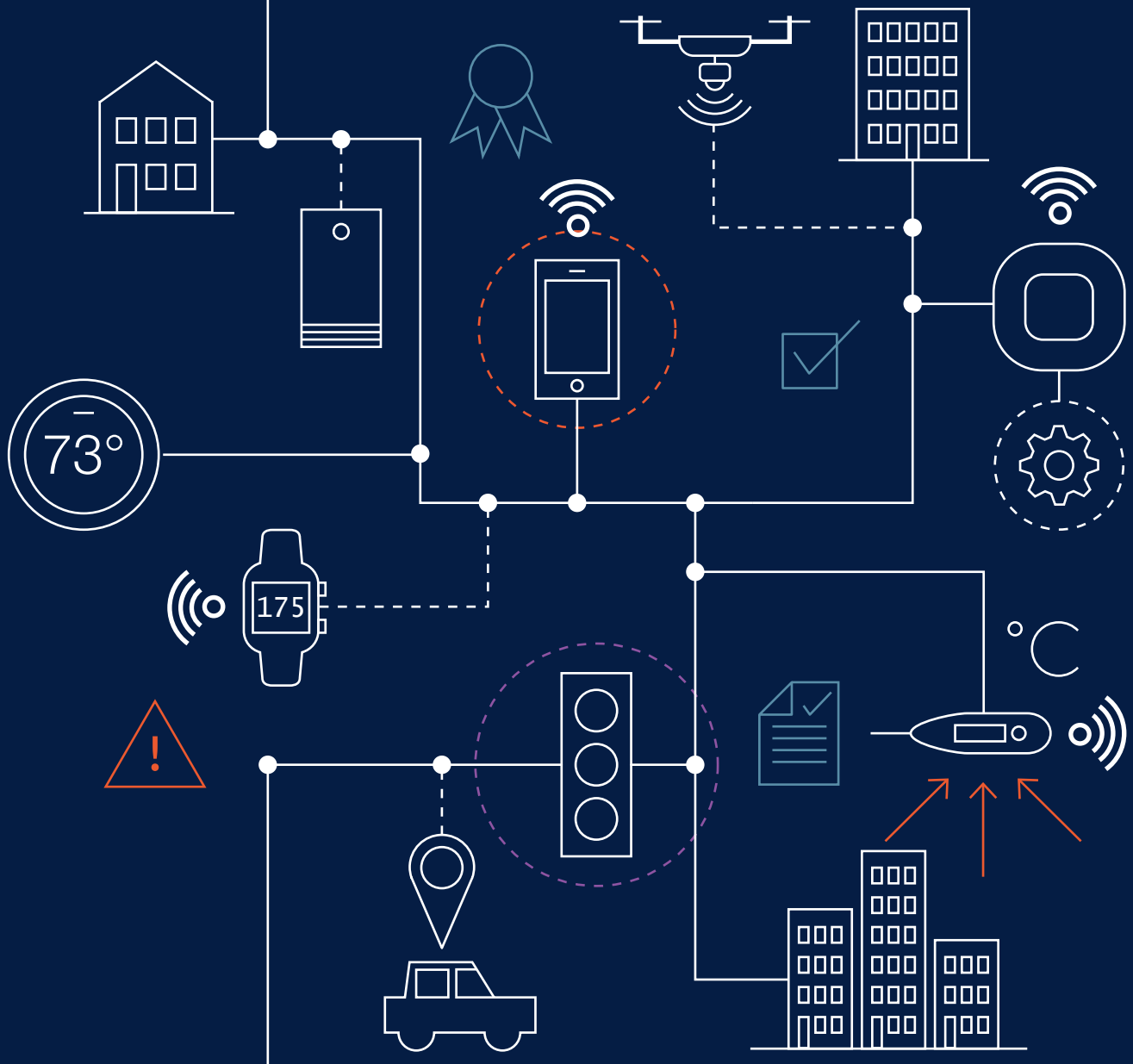
5. Over the next few years, the implementation of a variety of new technologies will likely increase the range, capabilities and analytical sophistication of IoT. These innovations have the potential to improve the governance of IoT technologies by incorporating key factors into the design of devices and systems – including privacy and security, but also human-centric considerations such as economic, civil, political and other human rights issues that could otherwise be overlooked.
6. Despite double-digit annual growth rates in the consumer IoT market, the value chain for IoT data remains opaque, undermining public trust. Privacy concerns are growing rapidly and it is becoming increasingly difficult to safeguard privacy as devices become more pervasive and embedded in people's lives, capturing personal data with greater frequency and granularity.
7. Cybersecurity threats remain a vital area of concern in the IoT ecosystem. Governments at the regional, country and state levels are beginning to address the need for better IoT security governance, but efforts so far have been globally fragmented, making compliance often confusing and costly for companies.
8. The COVID-19 pandemic has accelerated the move towards automation, a trend that some believe could affect hundreds of millions of people in the coming decade. It is important to better understand the impact that increased automation and IoT usage will likely have on regional communities and society at large now and in the future.
9. The pandemic has also shed light on how bias, implicit or explicit, and unequal access to connected devices and inequitable sharing of the benefits of IoT can have a massive societal and economic impact.
10. The interoperability of systems and advancement of global technology standards remain important priorities for the continued development and expansion of IoT.

In response to the findings of this report, the World Economic Forum, in partnership with the Global IoT Council, has developed a Global Action Plan that aims to encourage collective action on the most pressing challenges the connected world faces now. The goal of the plan is to increase public education on connected devices, encourage adoption of cybersecurity methodologies, accelerate adoption of connected systems in underserved areas and strengthen data sharing across the IoT ecosystem. Progress on these initiatives will be reported in 2021.

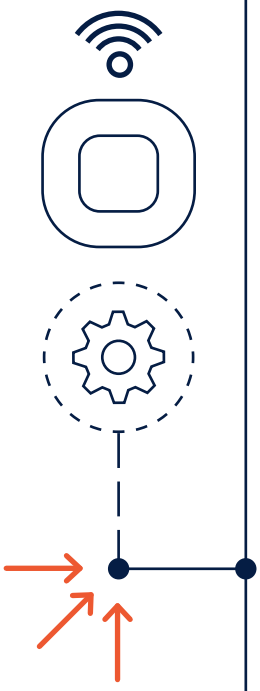
IoT is already an indispensable part of our daily lives and fundamental infrastructure. As it grows in extent and capability, we must act to ensure a connected world that is trustworthy, safe, collaborative, efficient, human-centred and generates new opportunities and benefits for all of society.

These actions address systemic challenges and therefore require the collective commitment of all stakeholders in the international community. As such, we invite you to consider how your organization might contribute to the progress of one or more of these actions. Together, we can chart a path to a future connected world that is more sustainable, resilient and prosperous for all.

Introduction: COVID-19, the Great Reset and the connected world



Introduction: COVID-19, the Great Reset and the connected world



Billions of connected devices instantly translate our physical world into the digital realm by capturing and analysing data about our surroundings in real time. Already, there are more connected devices than people in the world, and it is predicted that by 2025, 41.6 billion devices will be capturing data on how we live, work, move through our cities and operate and maintain the machines on which we depend.[1]

This vast network of devices – thermostats, speakers, beacons, cameras, sensors and other devices – is known as the internet of things (IoT). While early efforts at "connected" devices go back as far as the mid-19th century, the concept of IoT as we know it today is only about a decade old (see sidebar, "A brief history of IoT").

As it grows, IoT has the potential to transform how we live and work. Digital factories could operate with far greater efficiency and flexibility. Farms could increase productivity and improve sustainability at the same time. Cities could offer residents all kinds of new services at lower cost. Consumers could gain access to a range of applications that would make their lives more convenient and their homes safer.

Yet the networks of sensors, the data they collect, the complex software and algorithms used to analyse the data and make decisions are now combining into IoT ecosystems that challenge traditional governance approaches. The rapid growth of IoT has already raised critical concerns about its security, its effect on privacy and the fair and equal distribution of its benefits, as well as its potential for abuse and to have adverse impacts on individual rights.

COVID-19 has radically transformed the role of IoT in just a few months. Connected devices have been useful tools for monitoring and containing the disease around the world. But the situation has also highlighted the need to strike a proper balance between the public interest in protecting health in the face of future pandemics and the need to ensure the full range of human rights, such as protecting freedom of expression, association and movement.

As societies emerge from the COVID-19 crisis, a unique window of opportunity has opened to reimagine our relationship with IoT, realize new opportunities for growth and unlock a safer and more inclusive use of the technology. To do so, it is necessary to establish new governance norms to strengthen oversight and protect human rights for all.

A brief history of IoT

1969 — ARPANET, the precursor to the internet, is born

1982 — Researchers at Carnegie Mellon University develop the first connected vending machine to remotely check for cold sodas

1990 — John Romkey demonstrates the first toaster controlled via the internet

1997 — Wireless machine-to-machine (M2M) technology becomes prevalent in industry

1998 — IPv6 vastly expands the number of possible IP addresses in light of the expansion of internet usage

1999 — Kevin Ashton of the Massachusetts Institute of Technology (MIT) coins the term "internet of things"

2000 — LG announces the first smart refrigerator

2002 — Cloud technology takes hold with the launch of Amazon Web Services

2007 — The first iPhone is released

2008 — The number of connected devices exceeds the number of human beings on Earth

2008 — IBM's Smarter Planet project investigates applying sensors, networks and analytics to urban issues

2009 — Google starts testing self-driving cars

2009 — The European Union Electricity Directive requires EU states to roll out smart meters to 80% of consumers by 2020

2009 — Fitbit launches the first massively adopted fitness tracker

2010 — The price of sensors continues to drop (to present day)

2014 — The Industrial Internet Consortium (IIC) is founded by AT&T, Cisco, General Electric, IBM and Intel

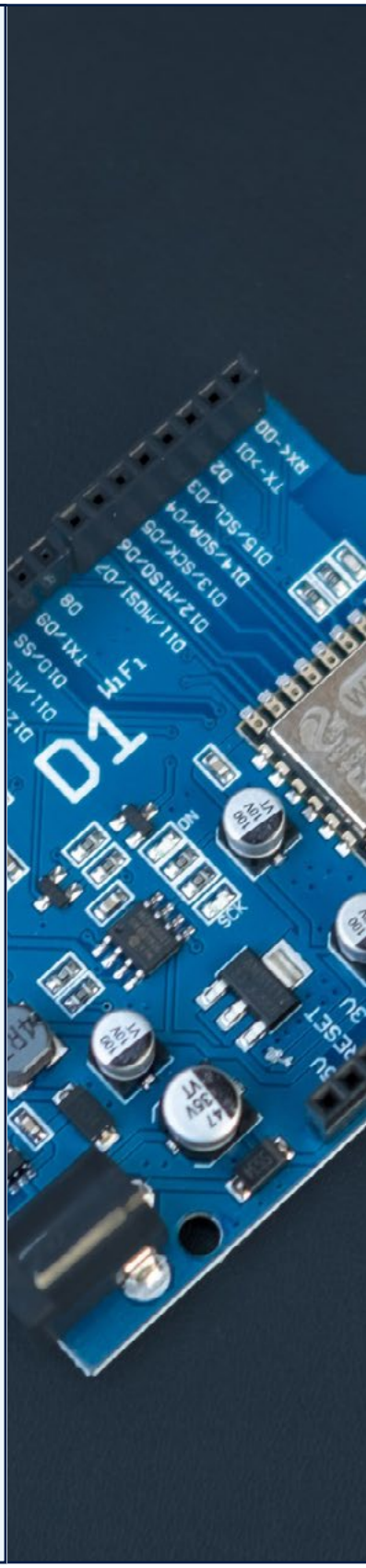
2015 — Klaus Schwab, Executive Chairman of the World Economic Forum, introduces the term "Fourth Industrial Revolution"

2016 — Mirai Botnet, the first large-scale IoT cyberattack, takes place

2018 — Toronto and Sidewalk Labs announce plan to develop smart waterfront area and receive fierce criticism over data privacy implications. The plan was eventually cancelled in May 2020

2019 — G20 nations pick World Economic Forum as secretariat for the G20 Global Smart Cities Alliance

2020 — COVID-19 hits the globe. IoT technologies such as contact tracing, health-monitoring wearables and smart thermal cameras are used by societies to contain the pandemic



Reaping the benefits

In its simplest form, IoT consists of data-collecting sensors that are connected with wireline or wirelessly to the internet, where the data transmitted by the sensors is captured, stored and analysed digitally, with little or no human intervention. The insights generated can then be used by machines, and by humans, if necessary, to adjust and modify the activity being monitored.

The range of potential IoT applications is limited only by the human imagination. IoT is already being used to monitor a diverse range of applications, from the number of steps people take daily to the rate of wear on jet turbine blades. Sensors, cameras and actuators have been embedded in everything from clothing to huge industrial machines. Recent-model cars and trucks contain hundreds of sensors that monitor the vehicle's operation, from seatbelt usage to engine condition to tyre pressure. Almost half of homes in the US now have smart speakers that answer questions, play customized music and news, take online shopping orders and monitor activities, among other things. And the analytical engines that create the insights provided are growing in sophistication. Many of them employ artificial intelligence (AI) and machine learning technologies to augment analysis of the data captured.

Most recently, IoT has been used to fight the COVID-19 pandemic. It has improved the efficiency of contact tracing by automating the process with smartphones and IoT sensors, and has enabled the use of cleaning and sterilizing robots, as well as remote monitoring of patients (see sidebar, "The good fight"). Beyond healthcare, IoT has helped make COVID-disrupted supply chains more resilient, automated activities in warehouses and on factory floors to help promote social distancing and provided safe remote access to industrial machines. IoT has also accelerated a variety of public-sector projects related to communications and transport – even robots and drones – in the fight against COVID-19. The insights gained now from IoT's essential role during the pandemic will likely translate into valuable tools for companies in their efforts to enable business continuity in the face of all kinds of natural disaster.

The good fight

Numerous IoT applications have emerged during the COVID-19 pandemic to safeguard people in their daily lives and help businesses get their workforces back on the job safely.

The two main components for containing COVID-19 are proactive prevention by practising social distancing and rapid response to identify and contain exposures. IoT applications using sensing technologies built into devices such as smartphones and wearables can help monitor social distancing and aid with contact tracing if infected cases are reported. Sensors can also help identify illness. Smart watches can monitor changes in heart rate, and thermal imaging can flag potential fevers among people in crowds.

Examples in the enterprise space include PwC's Check-In: a PwC product that uses Bluetooth and Wi-Fi technologies in its automatic contact tracing component to help enterprises rapidly identify users who may be exposed to an infected colleague in the workplace.

In the public space, Google and Apple have collaborated on software development tools to enable government and healthcare organizations to create contact tracing apps for Android and iOS devices.

Countries such as Switzerland and Japan, and state governments including North Dakota in the US, have used such tools to provide contact tracing apps to their citizens. Wearable device companies such as Fitbit and Oura are partnering with researchers to develop COVID-19 detection and monitoring algorithms.

While such applications are having a positive impact in terms of containing COVID-19, they may also pose challenges to personal privacy, which will be discussed in Chapter 5.

Opportunity knocks

In short, the economic and social benefits of IoT are far-reaching. Manufacturing companies can gather data on the factory floor to boost efficiency and capacity. The products they build can be equipped with sensors to enable predictive maintenance and provide a range of services that will provide significant added value and improve customer loyalty. Consumer-oriented companies can learn more about their current and prospective customers, enabling them to offer all kinds of new services built on need and convenience. Overall, according to the GSMA, IoT has increased productivity by as much as 0.2% of GDP already, and that number is growing.[2]

IoT's business benefits will be supplemented and enhanced through its impact on our environment and society as a whole. Connected technologies are already delivering significant progress against the United Nations' Sustainable Development Goals (SDGs). A 2018 analysis of more than 640 IoT deployments, led by the World Economic Forum in collaboration with research firm IoT Analytics, showed that 84% of existing IoT deployments address, or have the power to advance, the SDGs.[3] Examples include promoting more efficient use of natural resources, building better, fairer "smart cities", and developing clean, affordable energy alternatives.

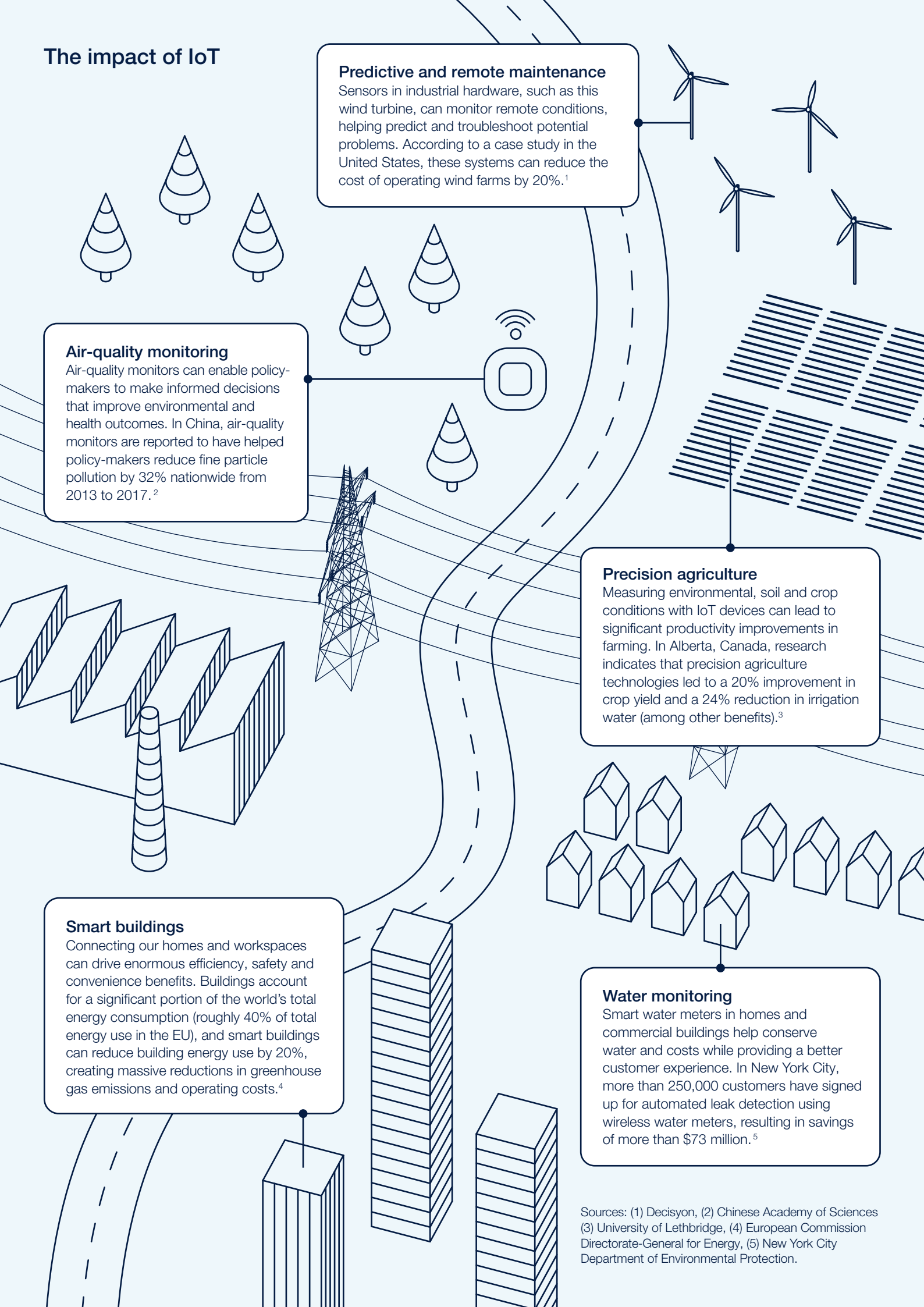
As IoT becomes more tightly incorporated into every aspect of our lives, it will provide a far deeper understanding of ourselves and the world we live in. The sheer number of connections between people and things will likely enable new kinds of economic and social interaction and creative endeavour. Ultimately, if IoT is developed and governed properly, it will expand human potential and elevate the lives of all people.

Perpetual innovation

Despite the rapidly growing presence of IoT devices, networks and analytical systems, in many ways these technologies are still in the early stages of development. Over the next few years, a variety of new technologies will be implemented that will likely increase the range, power and analytical sophistication of IoT. Super-fast 5G networks with near-zero latency are already being deployed.

Combined with fog/edge computing that enables data processing in end devices, this will likely significantly reduce the response time for mission-critical applications. This could potentially unlock transformative applications such as real-time traffic coordination for autonomous vehicles. Natural language processing (NPL) in edge devices such as smart speakers will reduce costs and improve the user experience.

The impact of IoT



Predictive and remote maintenance

Sensors in industrial hardware, such as this wind turbine, can monitor remote conditions, helping predict and troubleshoot potential problems. According to a case study in the United States, these systems can reduce the cost of operating wind farms by 20%.[1]

Air-quality monitoring

Air-quality monitors can enable policy-makers to make informed decisions that improve environmental and health outcomes. In China, air-quality monitors are reported to have helped policy-makers reduce fine particle pollution by 32% nationwide from 2013 to 2017.[2]

Precision agriculture

Measuring environmental, soil and crop conditions with IoT devices can lead to significant productivity improvements in farming. In Alberta, Canada, research indicates that precision agriculture technologies led to a 20% improvement in crop yield and a 24% reduction in irrigation water (among other benefits).[3]

Smart buildings

Connecting our homes and workspaces can drive enormous efficiency, safety and convenience benefits. Buildings account for a significant portion of the world's total energy consumption (roughly 40% of total energy use in the EU), and smart buildings can reduce building energy use by 20%, creating massive reductions in greenhouse gas emissions and operating costs.[4]

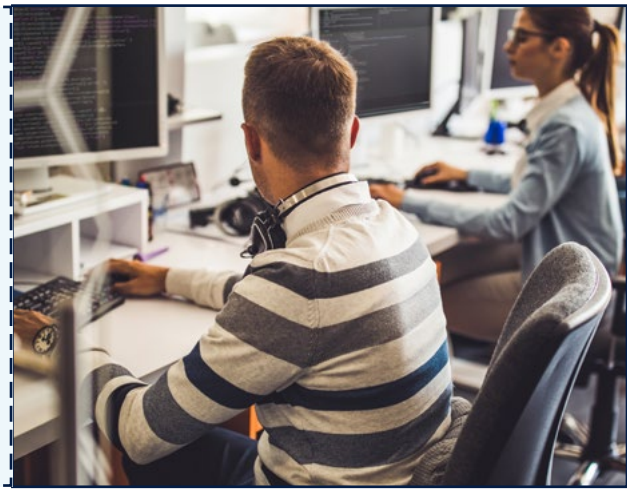
Water monitoring

Smart water meters in homes and commercial buildings help conserve water and costs while providing a better customer experience. In New York City, more than 250,000 customers have signed up for automated leak detection using wireless water meters, resulting in savings of more than $73 million.[5]

Sources: (1) Decisyon, (2) Chinese Academy of Sciences (3) University of Lethbridge, (4) European Commission Directorate-General for Energy, (5) New York City Department of Environmental Protection.

Growth across IoT's three domains

To better understand the nature of IoT and analyse the governance gaps that may limit its growth and human-centred goals, we have divided it into three primary domains.



1 Consumer IoT

This domain comprises applications designed for use by consumers, such as smart home devices, internet-connected appliances, wearables, connected health-monitoring devices and beyond.

2 Enterprise IoT

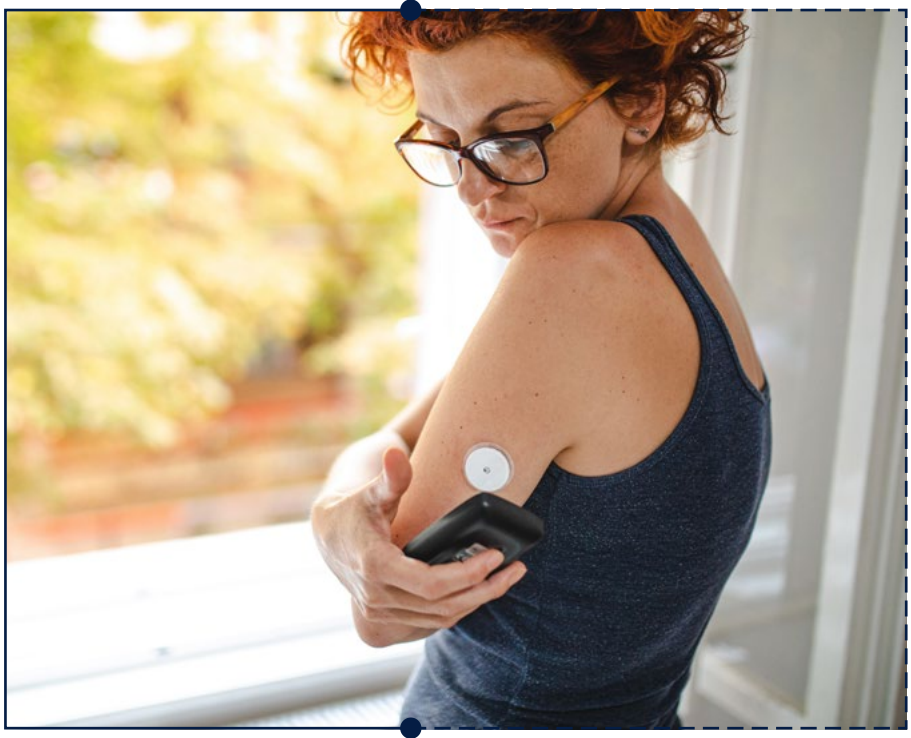
Applications in this domain include smart factories, connected supply chains, internet-enabled machinery, intelligent building management systems, precision agriculture and beyond.

3 Public spaces IoT

This category includes all applications in public spaces, such as smart city technologies for traffic and lighting management, public safety solutions, emergency notification, waste management, fleet management systems and beyond.

Overall, investment in and adoption of IoT has been growing across all three domains and in every region. Prior to the emergence of COVID-19, PwC estimated that, in 2020, IoT investments by businesses would grow to $832 billion, while consumer spending on IoT solutions would rise to $236 billion.[4] Spending on smart city initiatives worldwide in 2019 exceeded $100 billion and is projected to be around $190 billion in 2023.[5] And, according to Forrester, 41 million US households had smart speakers in 2019, for example, with sales growing in international markets as suppliers adjust for local languages and cultures.[6] Overall, spending on IoT technology was projected to grow 13% per year through to 2023, according to the International Data Corporation (IDC).[7]

The pandemic effect



These growth predictions, however, have been interrupted by COVID-19. The supply of new installations of the wide-area network connections that power IoT has slowed by 18% compared with the pre-COVID forecast, according to ABI Research; this is due to manufacturing shutdowns, supply chain interruptions, component shortages, worker unavailability and changes in the demand for connected products.[8]

The impact of COVID-19 on the demand for IoT applications has been mixed. Many enterprise and smart city projects have been put on hold as businesses cope with the pandemic-driven economic slowdown and governments reprioritize budgets in response to the health crisis. However, the use of connected thermal cameras to detect potential COVID-19 infections has grown substantially.[9,10] Demand for technologies that can help workforces get safely back to work is also likely to continue to grow. Many IoT solution providers pivoted quickly to the development of COVID-19-related apps and devices for services such as social distancing monitoring and contact tracing. The digital contact tracing market alone has a market potential of $4.3 billion according to IDC.[11]

Global consumer spending on smart home-related devices may drop to $44 billion in 2020, from $52 billion in 2019, according to Strategy Analytics.[12]

Growth in demand among consumers for connected cars, too, has slowed, to less than 2% in 2020.[13] But global shipments of voice-controlled smart home devices is expected to grow by close to 30% in 2020, driven by the dramatic increase in people working from home, according to ABI Research.[14] These disparities illustrate how the impact of COVID-19 on IoT varies widely by end market and application.

If a COVID-19 vaccine becomes available, perhaps some time in 2021, both the supply and demand of IoT devices and applications are expected to gradually bounce back as the global economy stabilizes.[15]

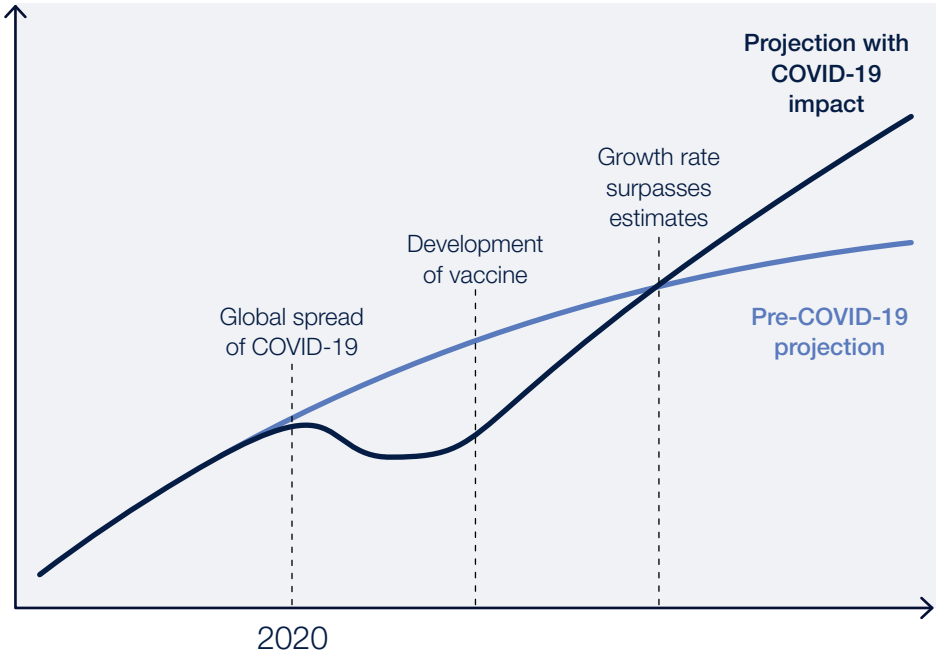
The IoT market is expected to grow even faster than expected once the world enters a new post-COVID-19 business environment, thanks to the release of pent-up demand and new investment in technology to minimize impacts from future disruptions, especially in the enterprise and public spaces domains. According to a survey by the GSMA, enterprises will increase investment in automation in the hope of improving agility in the face of future pandemics.[16] The industrial IoT market is expected to grow at a compound annual growth rate (CAGR) of 16.7% to reach $263.4 billion by 2027, driven by applications such as industrial automation and predictive maintenance.[17] Public health agencies will likely prioritize telehealth and remote patient-monitoring applications to expand the accessibility of health services. The US Centers for Disease Control and Prevention has published guidance for the use of telehealth to expand access to essential health services during the COVID-19 pandemic.[18] IDC forecasts that global IoT spending will return to double-digit growth rates in 2021 and achieve a CAGR of 11.3% through to 2024.

Figure 1 illustrates the contrast between IoT pre-pandemic market growth estimates and expectations for its current and future growth. Note that the specific dates are estimates, given the significant level of uncertainty surrounding the extent of the spread of COVID-19, as well as the development, production and distribution of a potential vaccine.

01100100
01100001
01110100
01100001

Figure 1: **IoT connections growth rate**

Once the COVID-19 pandemic subsides, IoT growth will likely accelerate beyond previous projections.



Governing IoT

Every major innovation in the long history of technology introduces new challenges and unintended impacts for society. Technologies such as cars, television, the internet and, most recently, social media all brought with them negative impacts that governments, industry stakeholders and society at large struggled to manage, despite their significant economic and social benefits.

IoT is no exception. It has the potential to fundamentally transform how we live and work – but it can also be misused. These risks are coming to light, in the form of security and privacy issues, the potential for increased cybercrime, the rise of ubiquitous surveillance at work, home or in public spaces, control of mobility and expression, and more. Confusion regarding IoT's technological standards, too, could limit its growth and benefits for society and make it more susceptible to safety issues and security breaches. Fundamentally, IoT is all about collecting the data needed to digitize the physical world and realize new benefits for society. But current policies for governing the collection and analysis of data are outdated, fragmented and incomplete.

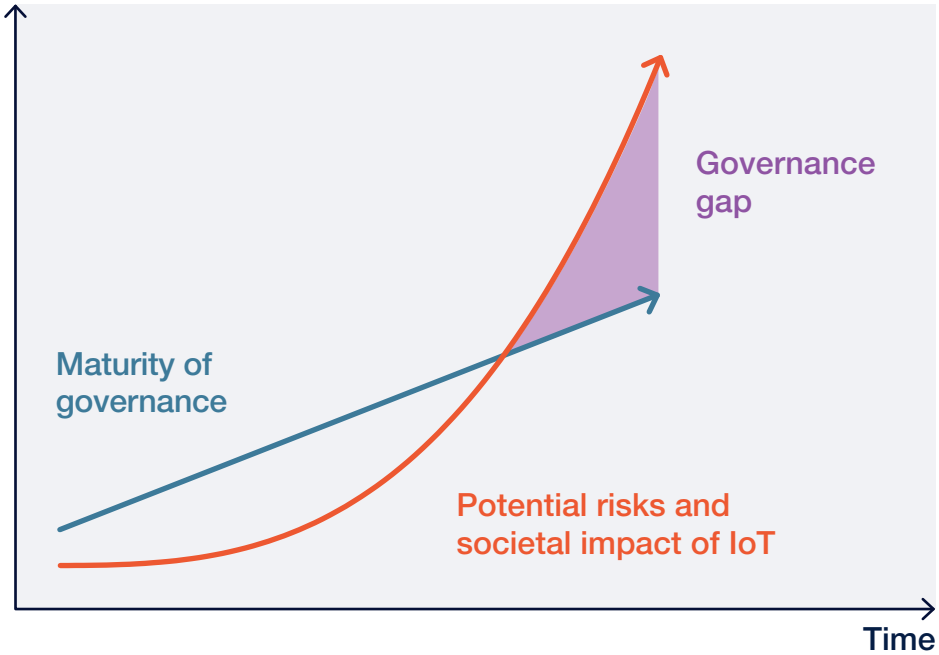
In short, for IoT, as for most new technologies, there are gaps in our ability to address and mitigate its potential negative impacts on a range of economic, political and social issues.

We define a governance gap as the difference between the potential risks posed by a technology and society's efforts to safeguard itself against these risks through laws, industry standards and self-governance approaches designed to achieve the greatest potential benefit of that technology for society as a whole. Effective technology governance mitigates risks and reduces the potential harms to society while also helping to maximize the technology's positive impacts (see Figure 2).

01100100
01100001
01110100
01100001

Figure 2: **Our guiding framework**

The gap between IoT's potential risks and the governance structures needed to mitigate them appears to be widening.



Measuring the impact

To better understand the size of the governance gap in each of the three IoT domains, we conducted a survey with more than 350 global IoT stakeholders and interviewed more than 50 IoT experts across the globe and sectors (see Appendix B for details). These contributors provided critical insights on the level of perceived risks and perceptions of the current governance level of IoT in the following five risk impact areas:

1 Privacy and trust

The ability of IoT devices and systems to safe-guard the privacy of users and ensure that personal and proprietary information will be collected, stored and used for agreed purposes in an ethical and responsible manner.

2 Safety and security

The ability of an IoT system to maintain a safe and secure development and operating environment.

3 Interoperability and system architecture

The ability of IoT devices and systems to interact effectively with one another to execute tasks in an efficient and cost-effective manner across the entire IoT ecosystem.

4 Societal benefit and equity

The ability of IoT devices and systems to fairly benefit and protect societal stakeholders irrespective of geographic, socioeconomic or other factors.

5 Economic viability

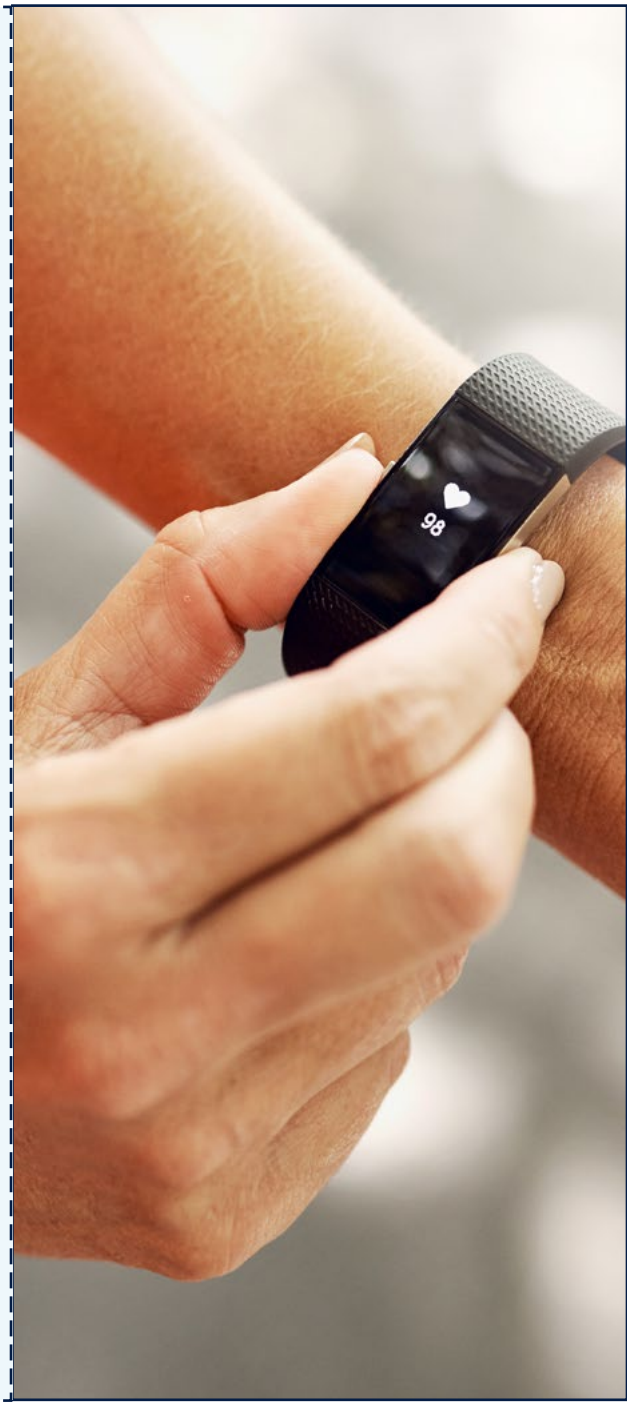
The ability of IoT devices and systems to be financially and operationally sustainable throughout their life cycles in the context of rapid technological and social changes.[19]

We assessed the governance gaps in these five areas by comparing the perceived risk level and perceptions of the current governance level measured in the survey and interviews. Using this framework, the Forum aims to help focus the efforts of business, government, academia and civil society to close the most significant governance gaps and deliver on the IoT promise of an improved quality of life for as many people as possible.

Ensuring the benefits

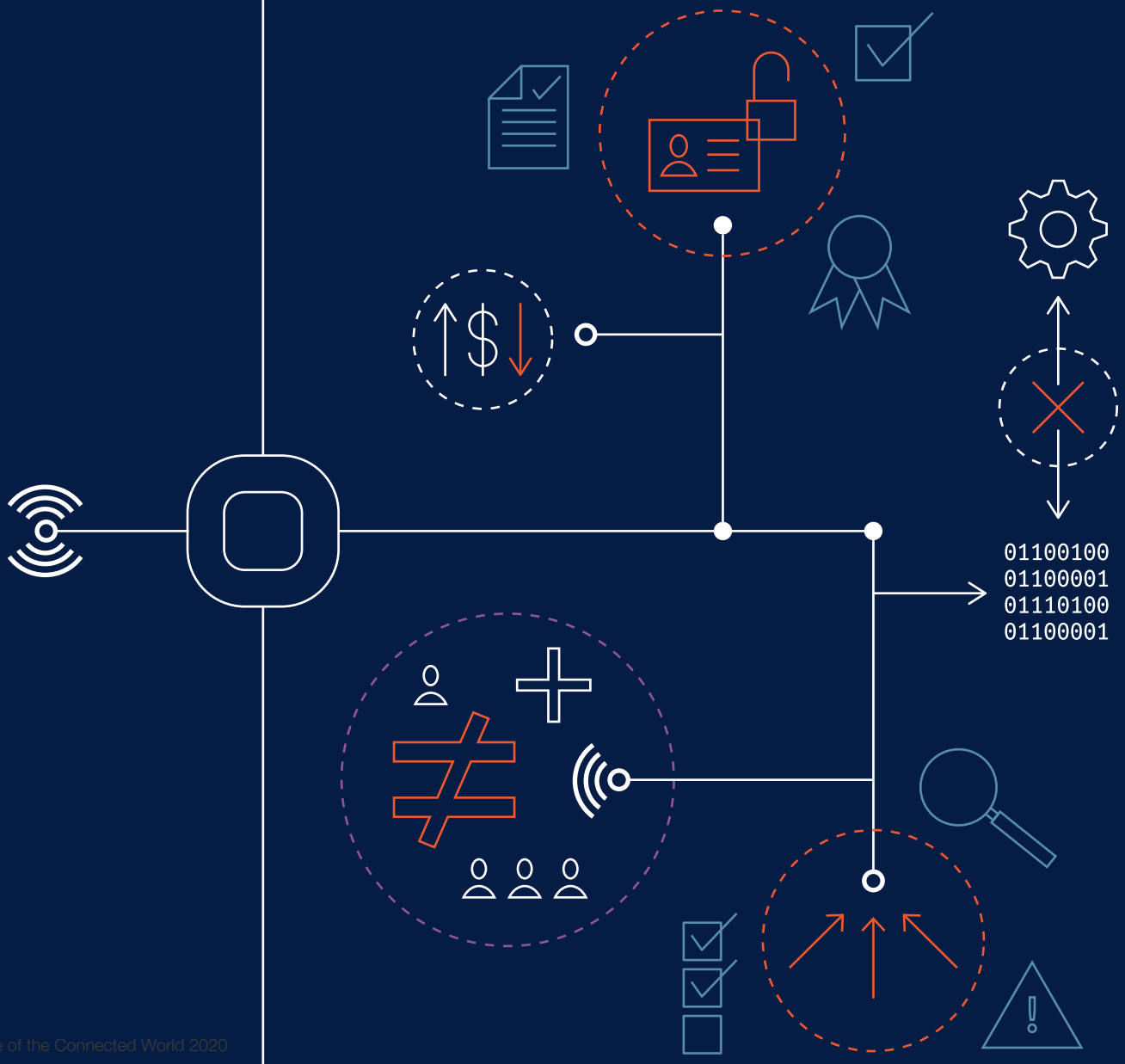
IoT is already becoming an indispensable part of people's daily lives and of the world's fundamental infrastructure. As it grows in extent and capability, the intention is that it will improve the quality of life for consumers, increase the productivity, safety and resilience of businesses, and enhance government infrastructure, operations and the provision of services.

The Forum is proud to present this innovative new framework for assessing the nature and extent of the gaps in IoT governance. With this in hand, we can work together to close these gaps and thus enable the further development of this essential technology securely, safely and fairly.



1

Recalibrating our relationship with the internet of things



The results of our survey and interviews define the nature and degree of IoT's perceived risks in each of the five impact areas and across all three IoT domains, as well as perceptions of their current level of governance. Together, these results enable us to assess the areas with the greatest gaps in governance – the first step towards developing effective governance mechanisms for IoT as a whole.

Measuring risks

The survey findings indicate that two impact areas in particular – safety and security, and privacy and trust – likely pose the greatest levels of risk, especially in the consumer IoT domain.

The survey findings indicate that two impact areas in particular – safety and security, and privacy and trust – likely pose the greatest levels of risk, especially in the consumer IoT domain (see Figure 3). Respondents pointed out that consumers have little or no transparency as to what happens to data collected by IoT devices, a problem that persists throughout the IoT value chain. Nor is there any global framework for addressing consumers' privacy concerns. To date, it has largely been the responsibility of IoT manufacturers and service providers to navigate the complex, conflicting and fragmented world of international regulations and to address and mitigate privacy risks, even as the burden of understanding how personal data is collected and used – and the risks involved – falls largely on the consumer.

In the area of safety and security, governance concerns centre on the lack of overarching mechanisms to ensure proper security management. Legislation focusing on IoT security is largely viewed as a fragmented patchwork of laws. Many current data security laws – and especially statutes requiring notification of data breaches – do not apply to IoT security issues. Moreover, IoT device manufacturers and service providers design a wide variety of security protocols into their IoT products and services, and even internal compliance with these protocols can be inconsistent. Meanwhile, consumers generally lack the awareness, knowledge and experience needed to properly manage their own exposure to IoT security risks.

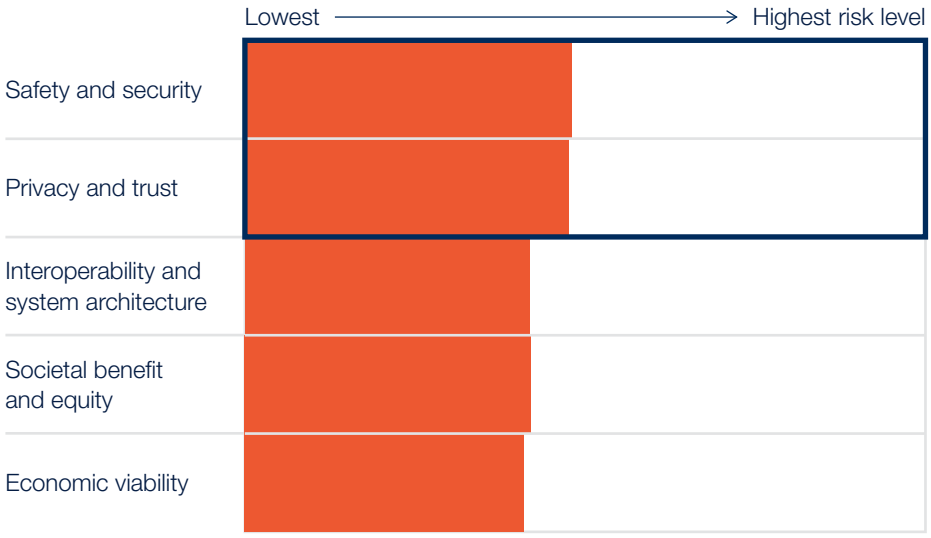
01100100
01100001
01110100
01100001

Figure 3: **Survey results summary**

Based on data from the Council's Survey of Subject Matter Experts, n = 374

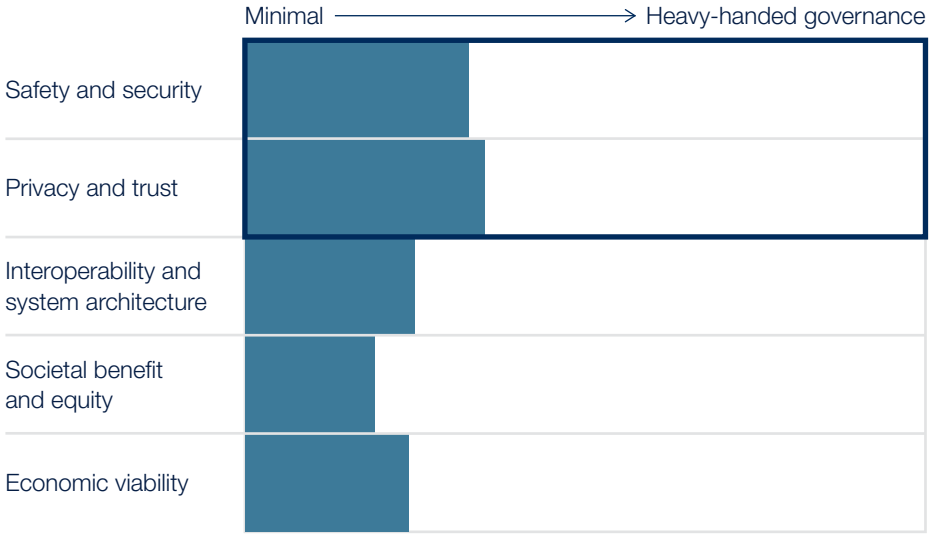
Risk

Two impact areas in particular—privacy and trust, and safety and security—pose the greatest levels of risk, especially in the consumer IoT domain.



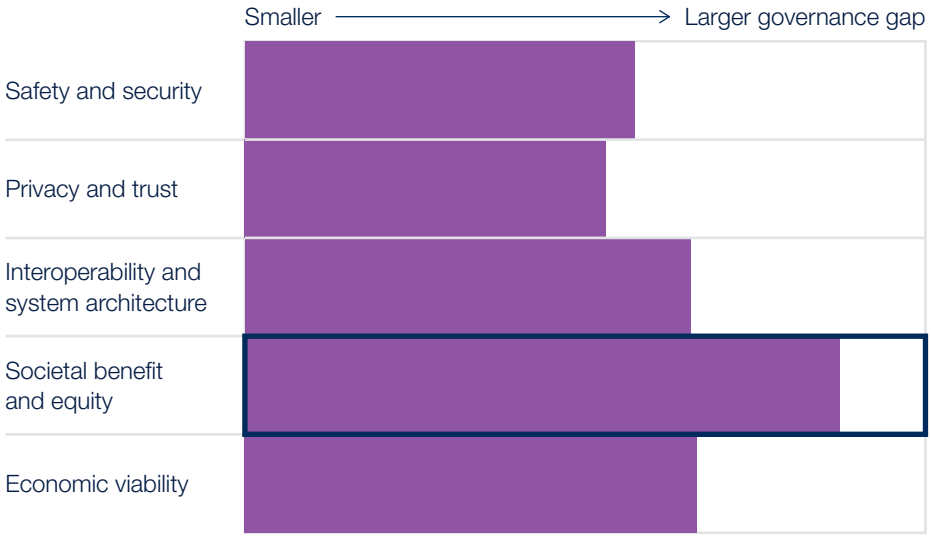
Governance

Industry and governments are working hard to respond to privacy and security risks, and governance measures are gaining traction.



Governance gaps

The largest gap in governance relates to ensuring IoT technologies become a force for shared societal benefit, as opposed to exacerbating the digital divide and existing inequalities.



Making progress

Respondents believe that industry and governments are working hard to respond to privacy and security risks and that governance measures are gaining traction. As a result, they consider the level of governance in these two areas to be higher than in the other three (see Figure 4). Respondents perceive the current gaps in governance to be highest in the area of societal benefit and equity (see Figure 4). Interviews revealed a variety of concerns as well as optimism about the future. In general, it was perceived that IoT could exacerbate the "digital divide" between digitally savvy, connected populations and those without digital access – although many also pointed out that IoT could also be a great equalizer with the right incentives. While traditional consumer protections are in place in many countries, IoT can increase the potential risk of unintended or unfair commercial practices such as discriminatory pricing. Furthermore, the opaque and complicated IoT value chain can stifle enforcement of existing regulations. The potential for job loss in the face of the greater automation enabled by IoT is also a concern.

Respondents perceive the current gaps in governance to be highest in the area of societal benefit and equity.

In the enterprise domain, interviewees noted the possibility that the positive network effects inherent in the economics of connected technologies could entrench industry oligopolies, lock users into "walled gardens", where their access to new products and services is limited, and inhibit the portability of personal data. The first companies to succeed in putting IoT to use may capture an unfair proportion of the technology's potential economic value. Interviewees also expressed concern that companies might remain unwilling to share data captured by IoT or to exchange and integrate data from different sources, limiting IoT's true potential.

Overarching governance gaps

Interviewees also brought up several more general governance issues. Many countries have imposed stringent regulations limiting the cross-border exchange of data. Such laws are causing compliance challenges and making it difficult for multinational companies to integrate the data they capture from IoT. These actions could also create barriers to international collaboration on critical IoT initiatives and suppress further innovation in the field.

In addition, IoT applications intended for the public spaces domain, such as smart cities technology, are often assessed and deployed without adequate, scaleable regulatory frameworks or the democratic participation of all stakeholders in addressing potential privacy, security and societal issues. The growing use of surveillance technologies is a case in point. Interviewees also note that the environmental impact of IoT hardware, and the e-waste this will generate, remains unaddressed.

In the following chapters, we examine more closely the gaps in IoT governance in each of the five impact areas and suggest ways in which stakeholders across all three IoT domains can collaborate in closing them.

01100100
01100001
01110100
01100001

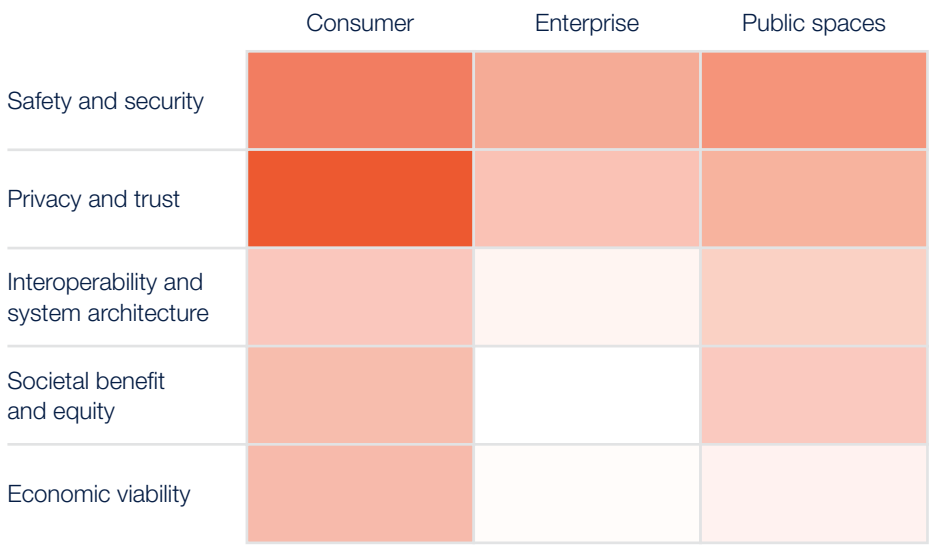
Figure 4: **Survey results**

Based on data from the Council's Survey of Subject Matter Experts, n = 374

Risk

Two impact areas in particular—privacy and trust, and safety and security—pose the greatest levels of risk, especially in the consumer IoT domain.

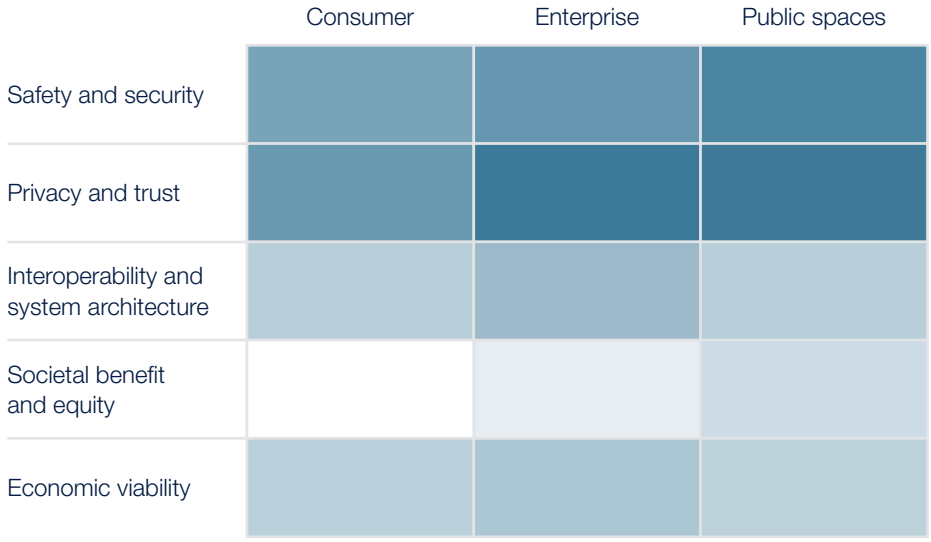
Risk level →



Governance

Despite the greater levels of risk, industry and governments are working hard to respond to privacy and security risks, and governance measures are gaining traction.

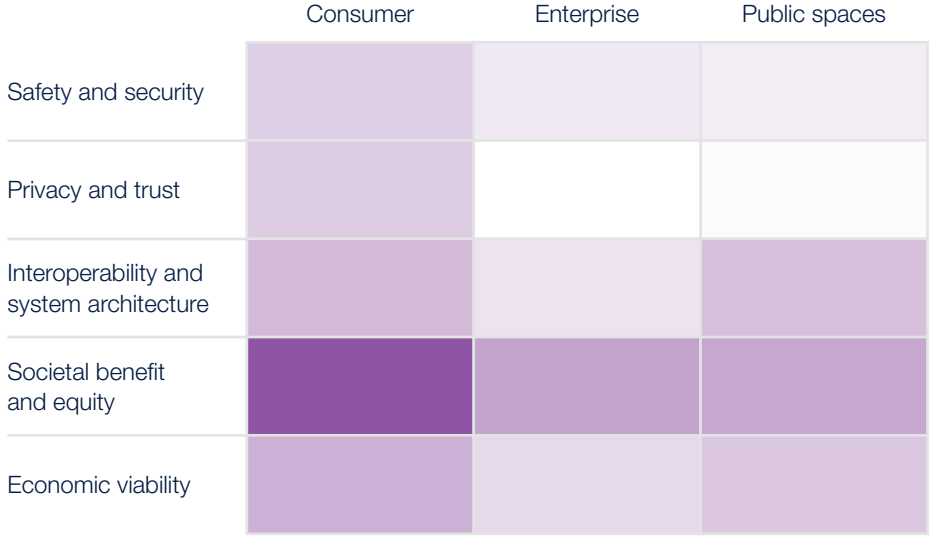
Governance level →



Governance gaps

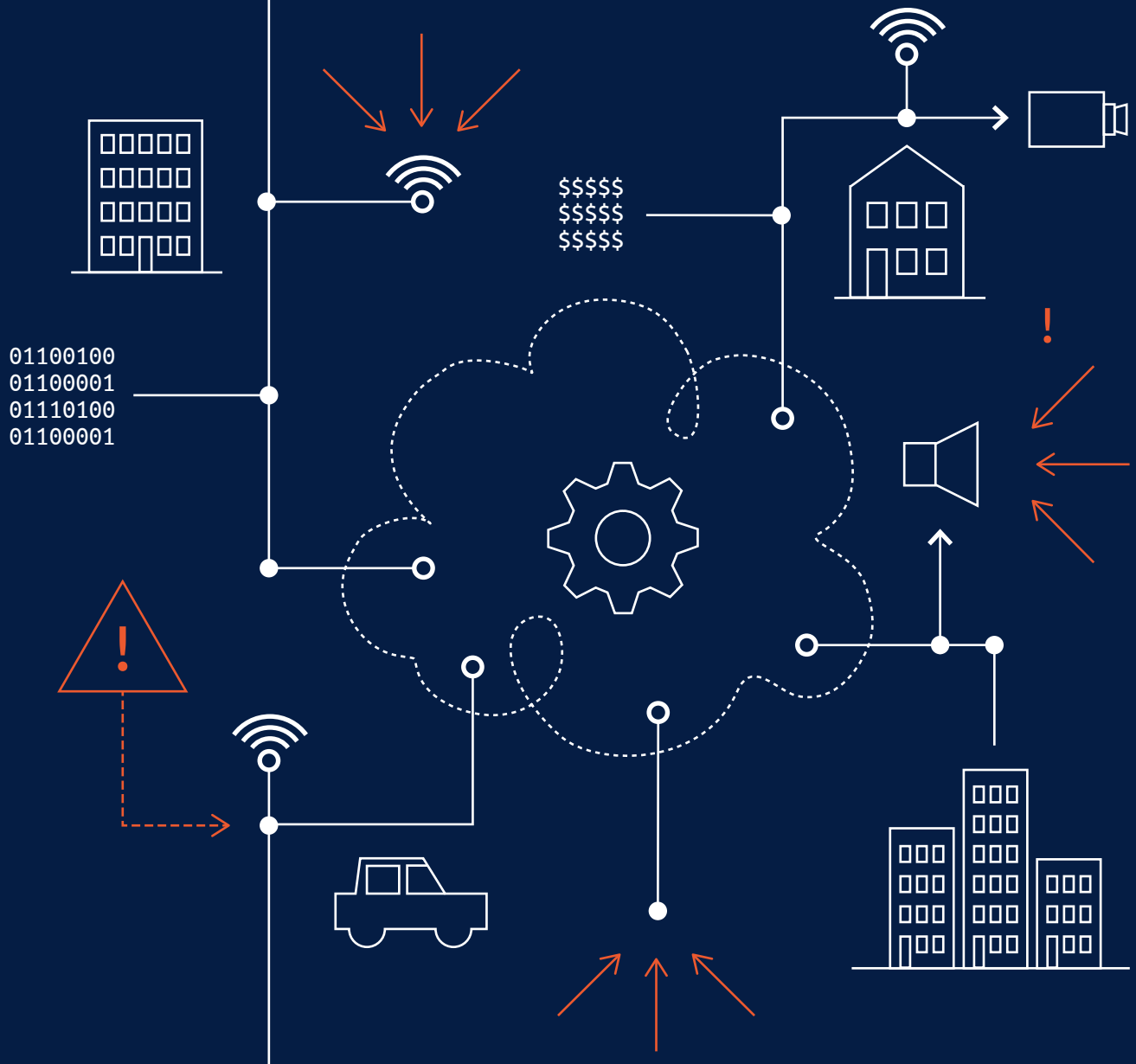
The largest gap in governance relates to ensuring IoT technologies become a force for shared societal benefit, as opposed to exacerbating the digital divide and existing inequalities.

Gap score →



2

Security and the need for standardization



No aspect of IoT has raised more concern than its safety and security. The very nature of IoT – millions of data-collecting endpoints connected wirelessly to the cloud – creates an ever-increasing number of targets attractive to bad actors. These concerns have inhibited the technology's uptake and expansion in all three domains – enterprise, consumer and public spaces. And rightly so: there have been numerous instances of hackers breaking into all kinds of IoT networks – everything from home security systems and automotive driver assistance systems to large-scale electrical grids. Research has shown that the cost of IoT hacks can represent up to 13.4% of annual revenue at companies with under $5 million in revenue. At larger businesses, the cost often rises into the tens of millions.[20] The impacts of hacks can go well beyond financial costs. IBM recently warned that hackers are targeting the refrigerated distribution systems that will distribute COVID-19 vaccines globally.

Safety and security risks are tremendous, as is the need to develop technologies and governance structures to help minimize these risks.

We define "safety and security threats" as any potential or actual cyberattack on IoT that may result in physical, psychological or economic damage or other negative consequences. This could include a wide range of motives, including attempts to spy on families at home, to steal money or personal data, to capture trade secrets, even to disrupt public infrastructure. In short, the risks are tremendous, as is the need to develop technologies and governance structures to help minimize these risks.

Risky business

"Interconnectedness comes with the risk of 'things' being intruded and reversely controlled. It may lead to significant physical safety threats to people or damage to critical infrastructure."

Yu Zhao, Chief Representative Officer of Connected Devices and Solutions, BOSCH China

In the enterprise space, notes Xiaoming Wang, a researcher at the Academy of Science of China, "enterprise intellectual property, trade secrets and operations are at stake from security risks of IoT". David Rosenberg, serial entrepreneur and Co-Founder and Chief Executive Officer of AeroFarms, a vertical farming tech company, believes that hacking presents a meaningful risk to his company and the industry. "As our farms become more and more digitally managed and connected, there are more and more bad actors trying to hack into our systems every day to take the data and we are afraid to possibly sabotage our farms. Adjustments can be made around temperature, nutrients, water, airflow, CO2 levels, the automation and other items. We always have to stay steps ahead of these potential threats."

Perhaps the best-known IoT security breach incident in public spaces is the Mirai Botnet attack. A few hackers created malware, called Mirai, that turned networked CCTV cameras into remotely controlled bots to initiate distributed denial of service (DDOS) attacks. In October 2016, it almost brought down the entire internet on the east coast of the US.[21]

Security and the need for standardization

IoT's technological vulnerability isn't the only matter of concern. The general public's lack of risk awareness and failure to adhere to security design and processes is a significant contributing factor. Breaches frequently occur due to lack of information, lack of provider-driven security updates, lack of experience and poor user behaviour. Even devices whose existing security designs can be revised and updated after they're in place can face security threats if users or companies decide that it is too complicated, confusing or expensive to continue to update them, although IoT manufacturers and service providers should make the process as easy and low cost as possible.

Security camera breaches

Security cameras are one of the most widely adopted consumer IoT products in the US. While they are designed to provide peace of mind to families, they have become a popular target for cybercriminals.

A widely known case is the Ring camera breach. In 2019, multiple families' Ring security systems were compromised. Hackers used the compromised cameras to access people's homes, harrass children and even demand ransoms.

Nest security cameras were also breached in 2019, allowing hackers to play fake warning messages that North Korea had launched missiles at the US.

That same year, Wyze Labs, a maker of affordable smart cameras, also suffered a data breach. An unsecured server resulted in the exposure of 2.4 million customers' data.

Due to the highly sensitive data produced by security cameras and other consumer IoT devices, security remains the area with the highest perceived risk from IoT.

What makes IoT different?

Security has long been a major concern for users of information technology everywhere. Despite billions of dollars being spent on efforts to secure government and corporate networks, theft of the personal data of millions of people occur regularly.

IoT is different from traditional networks in three important ways, which makes it both more vulnerable to attack and harder to defend (see Figure 5).

First, the sheer number of interconnected IoT devices and networks offer hackers millions of points of attack. In addition, edge devices such as routers that aggregate IoT data may have various security vulnerabilities. Most IoT vendors offer their own devices and network elements, with different security features, capabilities and levels of protection, making it nearly impossible to develop industry-wide security protocols. Many IoT systems are connected to sensitive corporate and government networks, offering hackers especially tempting targets.

Energy and utilities: Critical infrastructure is increasingly using IoT, such as smart meters in our electricity grids and condition monitoring technology in power plants. Each sensor or actuator that is connected via IoT creates another potential target for a security breach.

Fishing for data

In one of the strangest IoT security breaches on record, hackers ingeniously accessed a major casino's customer data through the on-site aquarium.

Modern aquariums use IoT temperature sensors connected to a local network that allow a central system to monitor and adjust the aquarium's temperature. If Wi-Fi is used, then outside attackers have an entry point. Once breached, attackers can use the sensor to potentially retrieve and transmit data from within the local network.

Using a seemingly trivial vulnerability in the smart thermometer, hackers gained access to the network, retrieved data about high-paying customers, and then extracted the data back through the temperature sensor and into the cloud. What made this attack especially troubling is that overlooking security on even the simplest device with internet access can compromise the most carefully protected networks.

"Regular products have a clearly responsible party. For IoT, you buy hardware, software and services. If there is an issue, it becomes difficult to figure out whose fault it is, since there is a series of interlocking contracts between multiple parties."

Kayleen Manwaring,
Legal Academic, University of New South Wales

The energy and utility sector provides a case in point. Many of the industry's legacy infrastructure management systems are based on closed operations technology (OT) systems not yet connected to the internet. As Colin Yu, Vice-President of Software Engineering at Envision Digital, notes: "IoT brought information technology (IT) to the OT world. It suddenly exposed the security vulnerabilities in closed OT systems via interconnectedness. It may lead to significant consequences without preparedness." As the mechanical power-generating and switching equipment that operated independently in the past is being connected via sensors and actuators to IoT, the security risks are multiplying.

Second, hackers may be especially attracted to IoT systems because of the high volume and value of personal or business data they capture and transmit. Because IoT is by its nature an interconnected web of devices, successfully hacking one IoT device can give hackers the ability to exploit other devices on the network in the absence of appropriate protections.

According to Prakash Sangam, Founder and Principal of Tantra Analyst, the extent of the potential damage is far greater than for traditional networked systems that have devices with strong processing capabilities to run sophisticated security protocols. The consequences of hacking into IoT networks, which typically have simple end devices, have the potential to be far more catastrophic. Hacking the electricity supply in a major city, he notes, could bring entire metropolitan areas to a halt and cause significant damage.

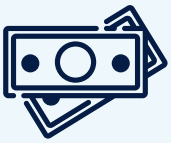
IoT systems create risks for individuals, as well. Anousheh Ansari, Chief Executive Officer of the XPRIZE Foundation, points out the risks inherent in medical device implants in patients. It is especially concerning since "there are currently not enough safety measures or security features built into these kinds of devices which could lead to major harm to one or groups of patients," she says.

Third, IoT's sheer complexity – the billions of networked sensors and actuators controlled by numerous sophisticated software programs – makes securing it and identifying the root cause of an attack exceedingly difficult. Kayleen Manwaring, a legal academic at the University of New South Wales, Sydney, Australia, says: "Regular products have a clearly responsible party. For IoT, you buy hardware, software and services. If there is an issue, it becomes difficult to figure out whose fault it is, since there is a series of interlocking contracts between multiple parties."

If a connected car is hacked, for example, causing the driver to lose control and have an accident, who is at fault? Sorting out responsibility among the driver, the car's manufacturer, the software maker and the network provider is no easy task. Assigning liability in such circumstances becomes nearly impossible; this is a major concern for the development of autonomous vehicles that the auto and insurance industries are still struggling to sort out.

Figure 5: **Key differences between IoT and traditional digital systems in safety and security**

Increased potential cyberattack points from rapidly growing number of IoT devices



More lucrative for hackers to attack due to the amount and type of data from IoT

More challenging to identify the root cause of a security breach and the part responsible due to the intertwined contracts

The state of IoT security governance

As with most new technologies, the rapid pace of IoT innovation and deployment has left the effort to govern and regulate it far behind. "It is like technology is running naked," says Lei Zheng, Director of the Lab for Digital and Mobile Governance at Fudan University. Current privacy and data security laws, as well as statutes requiring notification of data breaches, may need to be enhanced to fully address security issues from IoT.

Under most US state laws, for example, breaches exposing records containing users' names and associated biometric or sensor data do not trigger notification requirements. Most breach notification statutes govern personal information, which usually extends to a person's first and last name and any combination of their social security number, driving licence number, or bank or credit card account information.[22] Further complicating this issue, there are generally no policies governing the management of IoT data, such as requirements to periodically erase data to safeguard users while keeping law enforcement considerations in mind, so that only data that must be retained is retained. When the deletion of personal data is required, identifying all of the places where that data may be stored is a major technical challenge, especially for businesses that use numerous data-processing and storage systems. Moreover, IoT security is often addressed retroactively after an incident has occurred, rather than proactively as part of the design and throughout the life cycle of the product or service. Building security into products and solutions from the start, and finding software flaws early on, helps to proactively address security issues and prevent valuable resources from being spent later to mitigate risks or remediate damages that could have been prevented. "We are finding ways to empower companies to build security into products from the get-go, and to actively maintain security," says Gonda Lamberink, Cybersecurity Senior Business Development Manager at UL, "because what is safe today is not necessarily going to be safe tomorrow." Some measures have been taken by regulators to address the issue. For example, the UK government published the Secure by Design: Improving the Cyber Security of Consumer Internet of Things report to call for IoT industry stakeholders to take collective actions to secure consumer IoT products and associated services at every stage of the life cycle.[23] Security by Design is also part of the six Trust by Design principles launched by Consumers International to help manufacturers

"We are finding ways to empower companies to build security into products from the get-go, and to actively maintain security, because what is safe today is not necessarily going to be safe tomorrow."

Gonda Lamberink, Cybersecurity Senior Business Development Manager at UL

create safe and trusted smart devices for consumers. It encourages manufacturers to use best-in-class guidance and focuses on encryption, updates and firewalls.[24]

Governments at the regional, country and state levels are beginning to address the need for better IoT security governance, but efforts so far have been patchy and globally fragmented, making compliance both confusing and costly for companies. In the US, the National Institute of Standards and Technology (NIST) released the Foundational Cybersecurity Activities for IoT Device Manufacturers guidelines in May 2020,[25] which serve as non-binding guidance for IoT device manufacturers. Independently, the US states of California and Oregon have enacted laws requiring IoT manufacturers to outfit devices with "reasonable security features". In the EU, the European Telecommunications Standards Institute (ETSI) has released a technical specification guide on Cyber Security for Consumer Internet of Things, which also outlines leading security practices for IoT consumer devices.[26] The UK has released a code of practice[27] to end the use of default passwords; establish an end-of-life policy that explicitly states the minimum length of time for which a device will receive software updates; and require printing a support phone number for reporting vulnerabilities for consumer IoT products.

Governments at the regional, country and state levels are beginning to address the need for better IoT security governance, but efforts so far have been globally fragmented, often making compliance confusing and costly for companies.

However, as Eric Torres, Vice-President of Mobility and IoT Business at Tata Communications, notes, "We need a global IoT certification programme because the regional certifications we have today in the US, Europe, China, India, etc. are expensive and complicated, which impacts time-to-market for new products."

The technology industry, too, has made initial attempts to issue IoT security guidelines and frameworks, but there is currently no global baseline security standard for IoT. The industry-driven C2 Consensus on IoT Security Baseline Capabilities,[28] and the Cloud Security Alliance (CSA)'s IoT Security Controls Framework[29] offer guidelines to which companies can refer when building IoT systems. While both documents contain valuable information for IoT device manufacturers, these frameworks are discretionary and non-binding, with no uniform global baseline on the horizon for all to follow. While some regional efforts, such as the ioXt security certification programme, have been initiated,[30] there is no globally recognized IoT security certification programme.

As a result, current security design protocols for IoT products and services depend largely on IoT device manufacturers and service providers' internal policies and their subsequent willingness to comply with them. As Scott Jamar, former Vice-President of Industry Relations at Huawei, says: "One good way to do this would be a Consumer Reports-type model, where an independent test lab evaluates the kind of standards that may be needed."

Despite the scattered initiatives being undertaken by countries and industry organizations, governance gaps persist across the globe. IoT is poised to keep growing across industries and around the world, and the faster it grows the more

important it becomes to design and adopt stronger and more unified governance measures. To achieve this, safety and security measures should be implemented through the joint efforts of all stakeholders – governments, industry, enterprises and individuals alike (see Figure 6):

- **Consumers** should become more aware of the safety and security issues involving the IoT applications and products they purchase and use.
- **Enterprises** should put security policies, processes and controls in place and continuously monitor and update the security of their products and services and provide accurate and complete information to their customers.
- **Industry** players should collaborate on setting up global IoT security standards and security certification programmes. The IoT's global nature will require a more holistic approach that touches manufacturers and service providers across the world.
- **Governments** around the world should institute harmonized baseline IoT security regulation.

Figure 6: **Collaborating for IoT safety and security**

Domain discussions

Enterprise IoT

Safety and security for enterprise IoT applications is a critical and ongoing issue. Research conducted by the Ponemon Institute shows that a quarter of organizations surveyed experienced data breaches and cyberattacks in 2019 due to unsecured IoT devices belonging to others, up from around 15% in 2017.[31] To enable a safe and secure device environment, companies must include safety and security in their risk framework, put governance and processes in place and continuously and comprehensively monitor the risks. "There is a need for instrumenting, collecting and measuring threats and issues," says Vaibhav Parmar, a principal at PwC US. "Enterprises are still not doing a good job of IoT threat detection and analysis, in the same way they do it for traditional IT systems."

Consumer IoT

Many consumers lack the knowledge and skills needed to understand what they are buying or to maintain the security of the IoT-connected devices and services they buy. In particular, there is little knowledge of how to assess their need for any particular IoT device they wish to acquire, what kind of security features to look for when purchasing an IoT device or of how to configure and maintain the security of their IoT systems after purchase. This raises important questions, not just with respect to consumers' security but also regarding who is responsible for keeping them secure. Does this responsibility fall squarely on the consumer, or on the manufacturer, at least in part? And who is responsible for helping consumers understand how to keep their devices secure?

Further complicating things, there is an unclear standard of liability in the event of compromised IoT device security. When a security incident occurs, it is unclear whether the IoT device manufacturers would be held strictly liable for defective or insufficient security features.

From the perspective of the IoT device manufacturers, it may not always be practical to maintain and update devices indefinitely. Michele Turner, Senior Director of Google Smart Home Ecosystem, says: "Consumers expect their devices will work for a long time and manufacturers will provide software updates to these devices. However, there is a point at which these products must have an end of life. This will require a shift in consumer mindsets, and consumers will need to be comfortable purchasing another device."

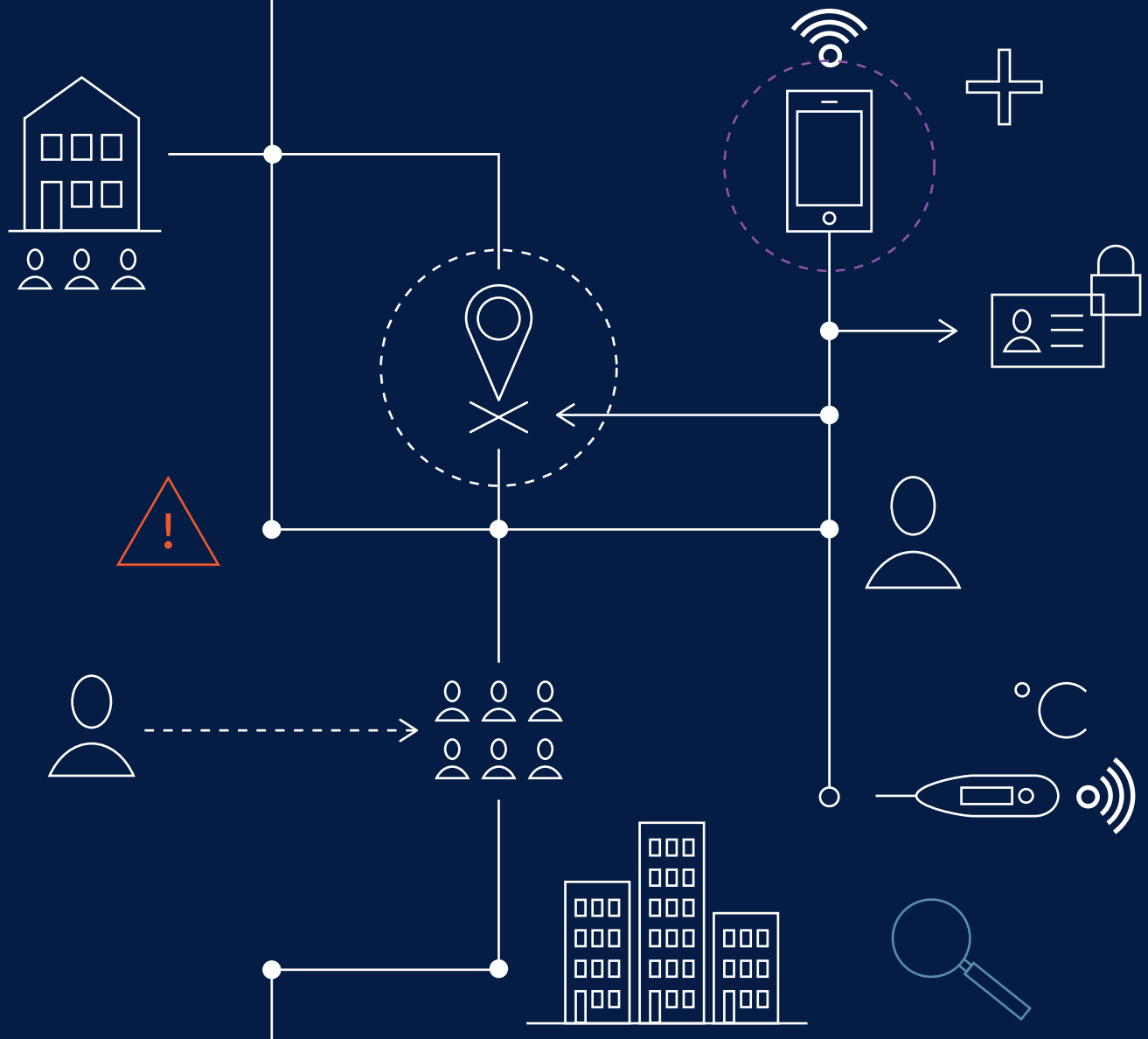
Public spaces IoT

Throughout the public sphere, there is inadequate cybersecurity awareness, resources, and training to properly protect IoT systems from cyberattacks. A 2018 study by researchers at IBM and Threatcare demonstrated that many smart city devices are vulnerable to hacking and cyberattacks, potentially enabling attackers to cause widespread public panic. The team uncovered 17 specific vulnerabilities in four smart city systems from three different vendors, eight of which left cities open to false attacks meant to cause panic or real attacks such as flooding, radiation, gunshot reports or transport and transit-system gridlock.[32]

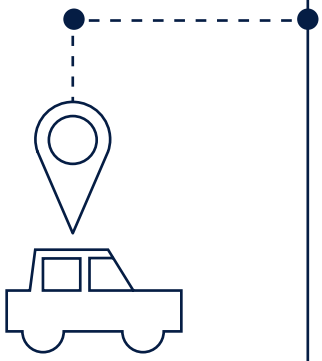
To thwart other similar cyber breaches in public spaces, it is critical that safety and security measures be built in throughout the life cycle of IoT projects, from procurement to deployment to post-deployment operations and maintenance. To achieve this, funding should be secured not only for deployment of IoT applications but also for their long-term maintenance. Public entities should also make a careful analysis of the need or appropriateness of a particular IoT solution in light of the problem it is intended to solve.

3

Pandemics, privacy and the public interest



Pandemics, privacy and the public interest



Perhaps the single most important feature of IoT is its rapidly growing ability to digitize, collect and analyse all kinds of data about the physical world in which we live, work and play. The increasing number of sensors, cameras and microphones planted in our homes and workplaces and in outdoor spaces is already upending traditional norms of privacy in both the physical and the digital realms. Privacy is no longer a simple matter of closing the blinds and locking the door, or of using an online search engine in "incognito" mode and refusing to consent to cookies.

In the connected world, maintaining privacy requires people to delve purposefully into cyberspace to understand what information is being collected in the physical world and how it may be used. However, research by Consumers International illustrates that only 50% of IoT consumers are aware of the settings on their IoT devices that control data collection.[33] Yet even that knowledge will not protect consumers if unscrupulous or negligent companies and governments allow IoT to be used to capture and potentially misuse their personal information.

The COVID-19 pandemic has cast a new light on the issue of privacy in the context of IoT. Maintaining the privacy of personal data on health remains, as always, a matter of security. Contact tracing apps and devices and other measures designed to promote public safety, however, are another matter entirely, and they have already raised alarm bells among privacy advocates. The pandemic will require everyone – governments, enterprises and people alike – to carefully consider the proper balance between the need to control the spread of the pandemic without disproportionally putting at risk the exercise of other human rights enabled by privacy protections.

So far, efforts to protect privacy in IoT have led to an international patchwork of government regulations and industry principles that has failed to establish adequate privacy rights or consistently guarantee people's privacy. While there are real-time databases on privacy laws and policies that can help businesses check compliance status, and respondents to our survey deemed the current state of IoT governance in this area to be moderate, a significant governance gap remains given the severity of the threat posed by privacy risks.

Inherent risks

We define privacy and trust in the context of IoT as the ability of IoT devices and systems to safeguard the personal activities and data of their users against surveillance, misuse and theft, with the goal of engendering confidence among users that their personal activities will not be monitored and their personal information will be collected, stored and used in an appropriate and responsible manner. This, however, is no easy task, given the very nature of IoT. Survey respondents pointed to privacy and trust as the area with the greatest level of risk, while interviews with IoT specialists suggested four important differences between IoT and other digital systems that make the task so difficult:

1 Pervasiveness

With the rapid adoption of IoT applications in every sphere of life, IoT devices have become increasingly pervasive. According to NCTA – the Internet and Television Association, there were about eight networked devices per person in the US in 2018, and the number is projected to climb to 13.6 per person by 2022.[34] Deployment of IoT sensors in public spaces is also growing quickly and invisibly, with little understanding of what they are used for or why they are in use.[35]

2 Proximity

The sheer scale of deployment isn't the only issue: IoT devices are also becoming more intimately and indispensably entwined in people's lives. In the US, more than 20% of people use smart "wearables" today.[36] Globally, the smart wearable market is projected to grow at a CAGR of 19% from 2020 to 2025.[37] Smart speakers and home security cameras have also been widely adopted. Fewer and fewer aspects of our lives are incapable of being monitored.

3 Granularity

Sensor technology is advancing quickly, and IoT devices are able to collect information from the physical world with increasingly granularity. Precise, detailed data is critical for applications such as autonomous vehicles, but the sheer level of detail also exacerbates privacy concerns. Lei Zheng of Fudan University says: "With more and more cameras being installed in recent years, they are getting increasingly close to people and capturing people's behaviour with higher granularity, which leads to lots of privacy concerns."

4 Real-time data

Much of the data captured by IoT devices is transmitted and analysed in real time, which poses a further challenge to privacy protection. "With static data, we have time to review and ensure that the data doesn't refer to personal or sensitive information. When we move towards real-time data streams, we lose the chance to perform privacy checks," says Anders Raahauge, Project Lead and Executive Advisor at Denmark's Agency for Data Supply and Efficiency.

Data demand

The complex value chain leading from the sensors, microphones and cameras collecting that data to its use and monetization is often invisible to end users. Any given IoT application consists of a plurality of services, hardware and software, which may muddy the visibility of how information is collected and used and who controls it.

Technology companies have traditionally been encouraged to collect as much user data as possible in order to extract valuable behavioural insights that go well beyond the need to maintain proper service levels. Most end-user licence agreements (EULA) and terms of service (ToS) permit device data to be shared with third parties for product functionality, security and service improvements. In many cases, however, the data may also be used for additional commercial purposes, including the sale of personal data to third parties, essentially creating secondary markets for data.[38] "Large companies collect a massive amount of data about everyone and each person's behaviour," says Anousheh Ansari of the XPRIZE Foundation. "This presents a big risk as currently there is no real oversight of how data is used or monetized, which may create an opportunity for influencing people's behaviour without anyone noticing it."

One academic study found that the manufacturers of 72 out of total of 81 consumer IoT devices studied shared the data they collected with third parties, and the data shared went far beyond basic information about the physical device being used.[39] "The biggest gap is the notion that companies can police themselves," says Mokena Makeka, Creative and Managing Director of Designworks. "This results in no accountability to the public, because companies end up just being accountable to themselves."

To address privacy concerns, IoT service providers typically use a so-called "release and forget" model. The technique involves de-identifying the data they collect before releasing it to third parties by removing names, dates of birth and other identifiers. Once released, service providers then "forget" how third parties use the data. However, a paper published in July 2019 in Nature Communications demonstrated that 99.98% of Americans included in an anonymized tranche of data could be reidentified using common demographic characteristics such as age, gender and marital status. Even anonymized and heavily sampled datasets are unlikely to satisfy the privacy standards set forth by the EU's General Data Protection Regulation (GDPR), bringing into question whether the de-identification release-and-forget model is technically or legally adequate.[40, 41]

The COVID-19 pandemic has raised a further issue: the need to balance individual privacy with the ability to effectively trace and control the disease. To contain the spread of the disease, countries such as South Korea, Singapore and China are using a variety of devices, some of them "wearable", and smartphone apps to trace the contacts of people infected with the disease. Geolocation and person-specific data collected is, by its nature, deemed personal data. While cultural and legal norms relating to privacy differ among countries, many would view the explicit collection of such data as a potential violation of personal privacy rights.

A Harris Poll survey found widespread public support for aggressive measures such as government mobile phone tracking and mandatory health screenings in public places to curb the spread of COVID-19 in the US, even when they might adversely affect privacy and civil liberties.[42] The World Health Organization (WHO) has released guidelines on how to ethically deploy contact tracing technology while balancing privacy protection and other rights.[43]

Researchers at MIT have developed an opt-in geolocation tracking app for smartphones that de-identifies the data collected and stores it with an independent third party.[44] Yet the adoption rate for apps like that developed at MIT remains low. As Roberto Zambrana from Bolivia's Gobierno Autónomo Municipal de La Paz points out, the boundary between privacy and the public good during an emergency is unlikely to be determined to everyone's satisfaction.

"The biggest gap is the notion that companies can police themselves."

Mokena Makeka,
Creative and Managing
Director of Designworks

Heightened risk

"Different standards across countries are inefficient and unsustainable, since people will be confused and IoT may end up being both over-regulated and unregulated at the same time."

Anders Raahauge, Project Lead and Executive Advisor at Denmark's Agency for Data Supply and Efficiency

Despite the potential risks to privacy and loss of trust inherent in IoT, the good news is that the public and private sectors, and society as a whole, are actively engaged in sorting out the complex issues involved. For example, the UK government published the Code of Practice for Consumer IoT Security.[45] Our survey indicates that the perceived governance maturity level of governance in the privacy and trust area is "moderate" – the highest among the five impact areas. Still, there remains a significant governance gap to be closed.

Today, privacy regulations are largely a global patchwork. The fundamental challenge is that there is no global consensus on the definition of personal data. Jocelyn Aqua, Principal of the Cybersecurity and Privacy Practice at PwC US, says: "A global IoT privacy framework that creates consensus on fundamental privacy principles can be very helpful for IoT businesses. It can form a solid base for these businesses' privacy practice before they address regional privacy regulation differences." Moreover, the effort to govern matters of privacy and trust can take many forms, including international, national and regional privacy regulations, industry-specific privacy standards and self-governance approaches regulated by contract law.

Currently, the EU's General Data Protection Regulation (GDPR) is the most substantial international framework covering EU countries and is being used as a foundation or reference by other countries on privacy regulations.[46] Regional regulations include the California Consumer Privacy Act (CCPA) and Illinois Biometric Information Privacy Act.

Attempts to regulate privacy issues vary in their approach to the problem. The GDPR, for example, focuses on building privacy protections into products and services as part of the engineering process – while the CCPA emphasizes protecting consumers from the "sale of their personal information".[47] According to the GDPR, consumers must opt in to the storage and sharing of their personal data, while the CCPA requires that users be given the right to opt out, a considerably more business-friendly requirement.[48] "We need a regulation that works globally," says Anders Raahauge of Denmark's Agency for Data Supply and Efficiency. "Different standards across countries are inefficient and unsustainable, since people will be confused and IoT may end up being both over-regulated and unregulated at the same time."

There are also emerging global multistakeholder efforts in relation to these problems. The Contract for the Web is a global plan of action to make the online world safe and empowering for everyone. It was written by representatives from more than 80 organizations, representing governments, companies and civil society, and sets out commitments to guide digital policy agendas. "Privacy is central to our freedom, dignity and safety. The Contract for the Web lays out guidance for how Governments can respect and protect people's fundamental online privacy and data rights and how companies can regain consumers' trust by respecting and promoting privacy rights," says Adrian Lovett, President and Chief Executive Officer of the World Wide Web Foundation.

IoT industry players have had mixed reactions to the piecemeal legislative approach and recognize the need for greater clarity. Some stakeholders have argued that government regulations mandating the type of acceptable IoT technology have the potential to chill or slow future industry innovation.[49] Maria Paz Canales, Executive Director of Chile's Derechos Digitales, says that technology does not necessarily need to be regulated, and instead we could perhaps regulate and codify the rights of the people using it. On the other hand, Sanjeet Pandit, Head of Smart Cities at Qualcomm, notes, "In order to reap the full benefits of intelligent, connected systems, we must ensure that there are proper regulations and industry standards in place to protect users' privacy, safety and security." The EU Alliance for Internet of Things Innovation (AIOTI) rated the right balance between protecting consumers and increasing innovation as being IoT's biggest challenge. For Joao Gonçalves, Industrial Policy Executive Manager at Brazil's National Industry Confederation (CNI), the solution lies in incentivizing good practices among service providers. "Brazil enacted the Brazilian General Data Protection Law," he says. "It is not only

"If we cannot gain the trust of the data source – the citizens – public projects will not succeed."

Nakamura Shojiro, Co-Lead of Accenture Innovation Center Fukushima, Japan

focused on penalties, but also incentives for companies with good privacy policies."

Meanwhile, industry standards and government-issued recommendations are emerging as an important tool in guiding the data and risk management practices of IoT technology companies. In the US, the National Institute of Standards and Technology (NIST) has issued its Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, for example, generating considerable interest in the North American market, although it is too early to measure the impact of the framework.[50] In fact, the risk of allowing third-party access to sensitive user data has been a contributing factor in some technology companies' efforts to restrict their IoT ecosystems further in order to create safer and more controlled environments for users.[51] In response to evolving privacy laws and increasing consumer awareness about privacy and tracking, the technology industry is also moving towards collecting data solely on a "need-to-know" basis.[52]

In addition, the privacy-by-design principle[53] is emerging as one of the more prevalent methods of industry self-regulation. A Carnegie Mellon University project, for example, has created a plug-in tool to help developers design privacy-friendly apps.[54]

Trust and transparency

Respecting user privacy is only one element of engendering trust, albeit an important one. Fostering transparency in the entire data value chain is also critical. "In data-driven smart city projects, data validity and freedom regarding data usage is imperative," says Nakamura Shojiro, Co-Lead of Accenture Innovation Center Fukushima in Japan, "If we cannot gain the trust of the data source – the citizens – public projects will not succeed."

A number of transparency-related governance initiatives are already under way across the IoT landscape. Sidewalk Labs' Designing for Digital Transparency in the Public Realm programme, for example, offers guidance on how IoT app developers can "advance digital transparency and enable agency" in public spaces.[55]

Truly engendering trust in IoT, however, depends not just on improving privacy, security and transparency practices. The public should also come to feel that it can influence how its data is being gathered and used, whether by businesses or by governments. "The big question is how we are ensuring that people have a voice in how their data is being used and how we can create trust in the decision-making process," says Dan Wu, Privacy Counsel and Legal Engineer at Immuta USA. "As data collection continues to expand, so too will public distrust unless new governance initiatives can empower the public to feel that they have agency over their own data."

And as the number of IoT devices grows, there will be more pressure for individuals to consent to IoT data collection. Concerns about facial recognition systems are on the increase; even the fast-growing popularity of smart speakers that listen in, whether or not permission is granted, has faced opposition. Efforts to raise awareness on the part of the public, however, are also on the rise. For example, Jason Hong, a professor at the Human Computer Interaction Institute at Carnegie Mellon University's School of Computer Science, has explored design options to make potentially unnoticeable IoT devices such as cameras and microphones more easily identified by people entering a new environment.[56]

Indeed, it is ultimately up to companies to engender trust among consumers. "Companies should try to do more than the norm and more than what is expected," says Jerry Power, Founding Member of the Intelligent IoT Integrator (I3) Consortium and Chairman of I3 Systems. "As people spend more time online, companies will begin to compete on trustworthiness in order to win customers."

Domain discussions

Enterprise IoT

For the most part, issues involving the impact of IoT on privacy and trust are primarily the concerns of the consumer and public spaces domains. Still, protecting the privacy and determining ownership of the data generated from enterprise IoT applications has also emerged as a potential risk. "There is a gap in data ownership for industrial IoT applications. While raw data generated from IoT applications usually belongs to enterprises, who owns the processed data? Enterprises, IoT solution providers or both? It has not been clearly defined yet," notes Johnny Zhang, Vice-President of Digital Services at Schneider Electric China. The effort to ensure the privacy of enterprise data may suffer from the same lack of transparency in the data value chain as consumer IoT data does. "For the short term, it might be good to let the industries explore viable models," Zhang concludes, "but for the long term, there needs to be some clear definition and regulation here."

Consumer IoT

Full transparency in the data value chain is critical to establish trust with end users of consumer IoT applications, and the gap between company practices and consumer expectations remains wide. Still, some organizations are working in the right direction. Amazon's smart speakers and Alexa system, for example, initially raised major concerns about the data collected as it listened. To assuage these concerns, Amazon allowed users to log in to see what data was collected and delete it when desired – essentially putting control back into the hands of consumers. Anita Woolley, Associate Professor of Organizational Behaviour and Theory at the Tepper School of Business, Carnegie Mellon University, concedes that this was a step in the right direction. "But it could have been better if Amazon had done it initially, instead of as a response to pushback," she points out.

A number of governance bodies are working on a further initiative to develop "trustmarks" and privacy "nutrition labels" for consumer IoT devices to provide more transparency and help consumers assess the trade-offs involved in their purchasing decisions.[57, 58, 59]

Adrian Lovett, President and Chief Executive Officer of the World Wide Web Foundation, agrees that a vital principle for governments and companies is to respect and protect people's fundamental right to privacy. He notes, however, that "privacy concerns are not sufficiently far upstream in the process of designing and building IoT devices. Privacy is not a sufficiently high priority in the overall priorities of the companies developing them, or the government's overseeing of those companies."

Public spaces IoT

The main governance challenge for IoT applications in public spaces lies in ensuring that governments can justify the use and benefits of those systems and in enabling people to agree to being monitored.[60] "There may be some misunderstanding about the technology and a lack of trust for citizens being asked to share their data as well as a lack of awareness of the potential benefits," says Deborah Colville of Belfast City Council in the UK. Indeed, while it is a relatively simple exercise to review one's browser history and clear cookies, trying to find out what data is being collected in public on a pervasive smart city network is far more opaque – if not impossible. Companies and governments alike are already using facial-recognition technologies to collect and store the face-prints of millions of people, creating an enormous potential for misuse. This lack of transparency has already led many consumers to view public IoT systems as "creepy" and "untrustworthy".[61]

In the absence of adequate transparency in the entire life cycle of these technologies, from the decision to deploy them to their use and oversight, concerns about how to get the general public to trust that IoT devices in public spaces will not invade their privacy and abuse their data are growing. The only solution may be greater transparency and accountability. "Trust is not the same thing as faith," one survey respondent noted. "To accelerate IoT adoption while avoiding threats, the key is to be transparent with the information, and to avoid endless privacy statements that only convince users that something is being hidden behind all of the legalese." External independent oversight and some form of participatory model in the governance of the system could help to gain the trust of people affected by these technologies.

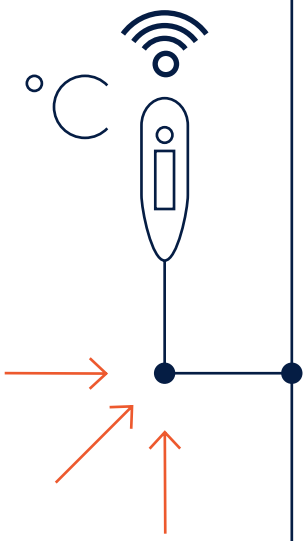
4

A connected world for everyone

The growing ubiquity of IoT devices and the increasing variety of applications may mean that IoT is beginning to touch virtually every aspect of people's lives. In an effort to monitor, measure and control everything from city traffic to the contents of our refrigerators to our individual heartbeats, IoT sensors are being integrated into almost every corner of our lives. The societal benefits are real – IoT apps and devices have already made major contributions to the ongoing battle against COVID-19, for example. But so is the potential risk that the benefits may be distributed unequally, that data will be collected selectively and that IoT will be used in ways that unfairly exclude or burden certain groups of people.

We define social equity and benefits as the ability of IoT devices and systems to fairly benefit and protect all societal stakeholders equally, irrespective of geographic or socioeconomic factors, availability of connectivity or other aspects. Promoting fairness in this realm, and making people aware of the risks involved, is a key challenge for two reasons. First, these risks are often slow to reveal themselves and deeply interwoven into the convoluted and largely invisible IoT data value chain, making them hidden and hard to identify. And second, while some stakeholders enjoy the majority of the benefits from IoT applications, others may be excluded from the landscape or have to bear the adverse impacts on their human rights, which can be overlooked entirely.

Economic risks



Differences in economic development, income, age, gender, education level, internet access and other factors on both a national and a global scale have created a "digital divide" that prevents people from enjoying equal access to the benefits of the digital world. Today, only 54% of the global population is connected,[62] with people in poorer regions far less likely to be online, along with women, elderly people and those living in remote and rural areas.[63] "It is crucial to ensure that there's digital equality, and that there is fundamentally universal access to the tools that the internet can bring. We need to be ambitious, going beyond basic access to embrace meaningful connectivity so that people have the data, speeds and devices they need to use the full power of the web," says Adrian Lovett of the World Wide Web Foundation.

Many fear that the rise of IoT may deepen the digital divide. An IoT application as straightforward as water-quality monitoring, for example, might be made available only in developed areas where it is most economically efficient, even though underdeveloped areas are far more likely to benefit from it. "Economic disparities are relevant in all new technologies," says Swarun Kumar, Assistant Professor of Electrical and Computer Engineering at Carnegie Mellon University. "We need to be careful about their public and private deployment, because low-income neighbourhoods might not get the same support [as high-income neighbourhoods]. For example, a luxury high rise might have air-quality sensors, leak detectors and security sensors, whereas none of these features would be found in a low-income housing project."

The IoT digital divide may exacerbate economic disparities, as well. CNI's Joao Gonçalves says, "A few years ago, disparities in connectivity between cities and rural regions was just a social problem. However, today, with the development of IoT, it is also an economic problem. Farmers are missing opportunities to improve productivity in agriculture." Around the world, IoT has enabled farmers to introduce precision farming applications such as remote monitoring and control of irrigation, sensor-based applications of fertilizer and pesticides, and self-driving tractors. Together, these are revolutionizing agriculture – if farmers can gain access to these tools.

On the other hand, if deployed properly, IoT can help bridge the digital divide. For example, IoT applications for remote patient monitoring for chronic diseases as well as COVID-19 have been rolled out in the UAE.[64, 65] Sofana Dahlan, a social entrepreneur and the first female lawyer in Saudi Arabia, notes that: "New technologies may help to bridge the gender gap. When information is presented digitally rather than in person, the gender bias may be eliminated." Gonçalves points out that broadband is widely available in Brazilian cities, but not in rural areas, and this presents a risk to its social benefits and equity. "Perhaps more access to connectivity will help people living in rural areas to reach the benefits associated with the IoT."

Enabling objective analysis

How data collected through IoT devices is used may present a further societal risk, if people face discrimination based on the analysis of data collected about them – whether or not the data is accurate. Among the adverse effects are service rejections, price hikes and unequal payment from work. According to an IERC position paper, "[IoT] and big data raise important concerns with regard to the privacy of the individuals and civil rights, protections against discriminatory outcomes and infringements of the right to equal treatment."[66]

How can we confirm, for example, that insurance companies will not abuse access to sensitive data gleaned or inferred from IoT devices, such as fitness trackers or automotive navigation systems? Should consumers be rewarded for good behaviour? Does the potential for predatory pricing or refusal of service outweigh the potential benefits of additional data? "At present, you cannot be sure that decisions made by algorithm are totally non-discriminatory," says Kristian Møller, Director General of Denmark's Agency for Data Supply and Efficiency. "We require a regulatory framework that is top down and ensures the ethical and inclusive use of data. We need to set the rules for the entire playing field." Alicia Asín, Co-Founder and Chief Executive Officer of Libelium, points out that the quality of input data massively affects the results of algorithms. "Algorithms are only as good as the data that goes into them," she notes. "Having multiple sources of data on the same platform increases the quality and reliability of the data."

Differences in the ability to benefit from IoT pose further risks. Ahmad Alabdulkareem, Director of the Center for Complex Systems (CCS) at the King Abdulaziz City for Science and Technology (KACST) and MIT, notes the example of potential unequal effect from usage of the power consumption data from smart meters. "If a utility company implements dynamic utility pricing based on the data, consumers at a higher socioeconomic scale can install solar panels to offset the impact from these pricing mechanisms, while consumers at a lower socioeconomic scale may not be able to do so."

It is the threat of job replacement through automation enabled by technologies such as IoT, AI and robotics, however, that presents perhaps the most significant societal risk. Companies in both the industrial and service sectors are rapidly adopting IoT technologies to streamline their operations and reduce costs. And concerns about the effect on employment are already widespread. "The bottom 30–40% of the population, in terms of income, already feel stressed about new technologies, and they fear that technology is going to take their jobs," says Carina Lopes, Head of the Digital Future Society Think Tank at Mobile World Capital in Barcelona. "Governments, both in Spain and in other countries around the world, have found that reskilling people for new jobs is very challenging, as many of these people have been working in the same jobs and repeating the same tasks for 30 or 40 years."

"The bottom 30–40% of the population, in terms of income, already feel stressed about new technologies, and they fear that technology is going to take their jobs."

Carina Lopes, Head of the Digital Future Society Think Tank at Mobile World Capital in Barcelona

Bridging the gap

These critical societal issues will only increase in importance as more IoT devices are deployed and more powerful software is used to analyse the data they generate. According to our survey, respondents did not perceive societal benefit and equity as a top risk of IoT. But they also judged it to have the largest governance gap across the three impact domains, and it has the potential for significant long-term implications if the gap is not addressed.

Currently, there are no formal overarching governance mechanisms for reducing the risk of the unfair or unequal distribution of societal benefits through IoT. Some local municipalities, however, have adopted effective methodologies to try and combat these. Joyce Edson, Deputy Chief Information Officer of the City of Los Angeles, says, "The city is taking active steps to ensure that new technologies will be rolled out citywide instead of only to specific areas to prevent a digital divide."

Such efforts, however, are only a start. The need to mitigate societal risks remains great.

Domain discussions

Enterprise IoT

Implementing enterprise IoT is often perceived to be complex and costly. Generally, larger companies have the appetite, knowledge and capital available to implement advanced IoT. This could further widen the gap between large incumbents and small, local and minority-owned businesses. According to the World Economic Forum's research, larger businesses (those with more than 500 employees) are six times more likely to use industrial IoT than small and medium-sized businesses.[67] New regulations designed to govern IoT more fairly may only exacerbate inequalities by increasing the compliance burden and creating barriers to entry into new sectors for such companies.

Consumer IoT

Examples of societal inequities in the consumer domain abound. So-called "free" services such as Gmail and Google Maps, for example, are not truly free. Users pay for them with the personal data they allow Google to monetize. Similarly, consumers pay for wearable wristbands that track physical activity and other data. While the apps that capture and analyse the data being tracked are free, the trade-off is that your data can be monetized by selling it to third parties. As a result, online services are already springing up that allow users to pay extra to confirm that their data is not collected and sold to third parties. People who are unwilling – or unable – to pay the extra fee could thus be relegated to a second class of privacy citizenship.

A further risk is the potential for excluding from the provision of services those who are not connected and monitored through sensors. Excluding them in the making of business and policy decisions may further marginalize these already vulnerable groups.

Such inequities could lead to all kinds of unintended negative consequences, including the unfair distribution of healthcare services based on inaccurate or biased analysis of data collected from wearable exercise devices.

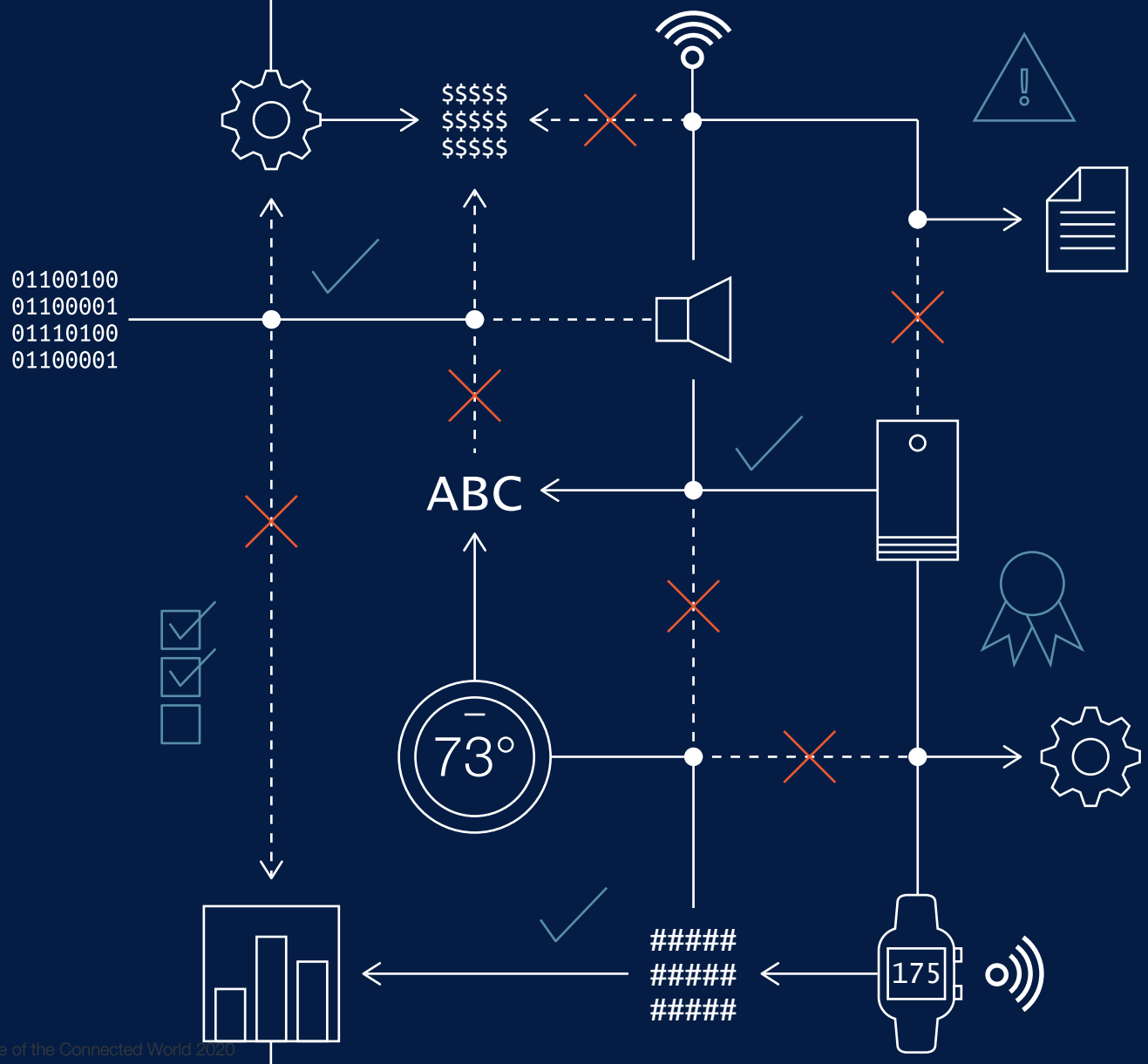
Public spaces IoT

The gathering of data from IoT applications in public spaces has the potential to generate considerable societal benefit. Already, there are numerous government initiatives to collect and make "smart city" data, such as air-quality and traffic-flow data, publicly available. The Danish government recently conducted a study[68] demonstrating the societal benefits of opening up data to the public and private sectors. Geospatial data collected by the Danish government has been used to optimize real estate tax determinations and to create noise maps to help people make real estate purchasing decisions.

At the same time, it is critical that the public is involved in decisions regarding the use of public funds for public IoT projects. "France and Estonia are building digital platforms where citizens can contribute their ideas for city initiatives," says Dan Wu of Immuta USA. "The goal is to democratize decision-making power and to use technologies to make it easier."

5

Creating a shared language for connected things



IoT is a fast-growing, many-layered and enormously complex set of technologies. Unlike the internet, however, which is built on a single set of internet protocol technologies, every IoT environment operates on its own data, communications and platform standards. Just as one provider's connected home thermostat device will not work with another provider's home system, so one service provider's industrial IoT tools will not work with another's without proper integration.

The added complexity and cost brought about by IoT's lack of interoperability can create a range of risks. It can prevent IoT devices and systems from effectively operating with each other to execute tasks in an efficient and cost-effective manner. It can slow the implementation of IoT while possibly increasing security and privacy risks. And it can even hinder the fair distribution of the technology's benefits throughout society. Efforts to encourage interoperability, however, have been fragmented and regional, at best. Overcoming the hurdle of interoperability is essential if our society is to reap more benefits of IoT.

Layers of complexity

Any particular IoT ecosystem can be designed and implemented using a wide variety of components, applications and communications standards from different vendors based on different system architectures. To enable them to work together within a particular ecosystem, however, they should be interoperable. At present, though, every layer of IoT offers a wide variety of incompatible options.

1 Data layer

IoT's many components, products and systems use different data structures, data interface standards and messaging formats for communication, which can lead to compatibility issues when data is exchanged between systems. Even when the data generated by different IoT components shares the same data format, the data and information models can still differ, making it impossible for them to "understand" each other.

2 Communication layer

There are numerous standards and proprietary technologies available for connecting IoT devices to networks, such as NB-IOT, LTE-M, Wi-Fi, ZigBee, SigFox and LoRa etc. Due to cost limitations and design complexities, most IoT devices typically support just one of these many communications technologies.

3 Platform layer

Many different operating systems have been developed specifically for IoT devices, including Contiki,[69] RIOT,[70] TinyOS[71] and OpenWSN.[72] In addition, IoT platforms such as Apple HomeKit, Google Brillo, Amazon AWS IoT and IBM Watson each depend on incompatible operating systems, programming languages and data structures. The many options available make it virtually impossible for developers to create cross-platform and cross-domain IoT applications.

The lack of interoperability across IoT's complex structure makes it difficult for end users in every domain to streamline their operations and protect their investments in the technology or move among providers. But enabling interoperability is no easy task. A 2016 paper from the Industrial Internet Consortium (IIC) puts the problem this way: "It is not a matter of agreeing on a small set of standards to rule the industrial IoT world, but about carefully orchestrating complex and partially competing protocols and standards on multiple levels."[73] Adrian Slatcher, Principal Resource and Programmes Officer at Manchester City Council in the UK, concurs: "Interoperability cannot be simply imposed. Rather, interoperability needs to exist at the right point of the system. Ten different companies may have ten different data models. It is important to identify the point for interoperability that makes the most sense by looking at the data value chain."

Why interoperability matters

Interoperability issues and the lack of global standards are undermining progress and creating barriers for the further development of IoT. It is difficult to gain economies of scale if IoT solution providers have to create, test and support multiple versions of the same device in order to ensure interoperability across different communications protocols and platforms. "We cannot create economic viability with lots of silos," says Juan Pablo Cosentino, Dean of the School of Engineering at Argentina's Austral University. "Why do we need to include five technologies in a device? Can we use only two? Silos prevent scale." Charlotte Roule, Chief Executive Officer of ENGIE China, echoes this view: "Interoperability creates the ability for market players such as ENGIE to develop efficient solutions. It also preserves some room for competition, hence secures affordability for the customer and mitigates the risk which could be borne by having one single solution." There is a further barrier to IoT adoption: Companies and individuals may hesitate to implement an IoT solution if its particular device or communications standards will soon become obsolete or cannot be integrated with other initiatives.

The lack of interoperability also makes it far more complicated and expensive to replace legacy IoT systems or build new capabilities on to older ones. Ryan Kurtzman, Smart City Program Manager of the City of Long Beach, California, notes that the lack of interoperability can also mean projects are stuck with certain vendors, inhibiting flexibility. And what happens if a particular vendor goes out of business or is acquired? The average IoT device lifespan is expected to be 10 years. Some legacy sensors that have been used for a long period of time may not be retired any time soon. If interoperability is not implemented and maintained from the beginning, the downstream cost could be significant. As Mads Bjørn-Møldrup, Director of PwC Denmark, notes: "Currently there is no standard data model to exchange data. When governments buy sensors from different vendors, they cannot merge the data together, and there is no government agency that is taking the lead to identify which global standard should be adopted in Denmark right now."

Finally, the lack of interoperability can also harm fair competition. As large-incumbent IoT device and service providers scale up "walled gardens", new players may struggle, suppressing competition, hindering innovation and increasing costs to the consumer. "There are lots of excellent solutions from small companies, but they don't have scale and cannot connect with solutions from big companies," says Cosentino of Austral University.

"Why do we need to include five technologies in a device? Can we use only two? Silos prevent scale."

Juan Pablo Cosentino, Dean of the School of Engineering at Argentina's Austral University

Fragmented governance

“It is a matter of coordination. There are so many people trying to do the same thing, but they need to make sure that the right hand knows what the left hand is doing.”

Joyce Edson, Deputy Chief Information Officer, City of Los Angeles

At present, the effort to design governance mechanisms and standards to promote IoT interoperability are fragmented and largely regional in nature. Several industrial organizations have offered their own frameworks, such as OneM2M,[74] Alljoyn,[75] IoTivity[76] and OMA LWM2M.[77] Regional government entities, too, have been trying to promote IoT interoperability, especially for the industrial IoT (IIOT) and smart cities. The China Electronics Standardization Institute published an Industrial IoT Interoperability White Paper.[78] ETSI, a European standards bureau, has published specifications for information exchange in smart cities,[79] while the EU has published Baseline Security Recommendations[80] for IoT in the context of critical information infrastructures in the hope of achieving a consensus for interoperability across the IoT ecosystem. Still, there is no de facto global standard for use in either the enterprise, public spaces or consumer domains. “It is a matter of coordination,” says Joyce Edson of the City of Los Angeles. “There are so many people trying to do the same thing, but they need to make sure that the right hand knows what the left hand is doing.”

Mohammad Ismail, Management Consultant, AI, IoT and Financial Crimes, for IBM Watson, points out the importance of collaboration in working towards IoT interoperability. Consortiums, he says, are imperative: “Consortiums and partnerships truly help everyone; on the vendor side it is a cost-savings opportunity, for consumers it is about better tools, and on the governance side it means multiple stakeholders providing input and keeping an eye out on the entire IoT ecosystem.”

Ultimately, market forces may drive the need for interoperability standards. “The push for interoperability must come from larger projects,” says Adrian Slatcher of Manchester City Council. “It is hard to make a business case for interoperability for small projects. IT teams in government are usually small, and small projects have no incentives to make sure interoperability is implemented.”

Domain discussions

Enterprise IoT

IoT systems designed for enterprises are largely limited to specific industries; some industries have standard protocols, while others don't. And even when standards are available, challenges remain in ensuring compatibility among components from different vendors. Colin Yu of Envision Digital points out that a significant number of industry standards exist in the energy sector, for example. But different companies may have different interpretations of the same standard. "We have to do the dirty work of collecting and implementing 1,000 or more variations of standards in a single platform in order to interconnect with equipment from different companies," he says. In his view, industry consortiums should be formed to define industrial standards and enforce compliance with them.

However, as Johnny Zhang of Schneider Electric China points out, "It may be challenging for incumbent large vendors to open their hardware interfaces and conform to industry standards because these are the anchor for their profits."

This may increase costs for customers. First, they may become locked into a specific ecosystem. Second, complicated additional solutions often need to be deployed to enable communication across different platforms and with business partners and supply chains.

As important as it is to promote interoperability among IIoT applications, there is a potential risk that simplistic, overarching governance models could hinder IoT adoption. "Governance should be defined by experts in each industry," says Yu Zhao of BOSCH China. "One-size-fits-all governance is going to restrict IoT industry development. In general, governance with a lighter touch is more suitable at this stage." Richard Zhang, Chief Technology Officer of IoT, Intel China, agrees: "Governance should not always mean restriction but also facilitation," he says. "Right now, it is important to foster the IoT market and encourage industries to embrace this new technology as well as putting proper restrictions on it."

Consumer IoT

Among consumer IoT players, the current trend is for large tech companies such as Google, Apple and Amazon to build their own IoT ecosystems and prevent or limit their IoT devices' functionality across platforms. In August 2019, for example, Google shut down its "Work with Nest" programme, which allowed Nest smart home devices to connect with other smart home platforms such as Amazon's. "Consumers are really suffering from conglomerates that operate in silos," says Burak Demirtaş, Project Manager at Arcelik Global, Turkey. "They should be able to buy what they desire without these restrictions, and these smart devices should work collaboratively without needing to be from the same platform."

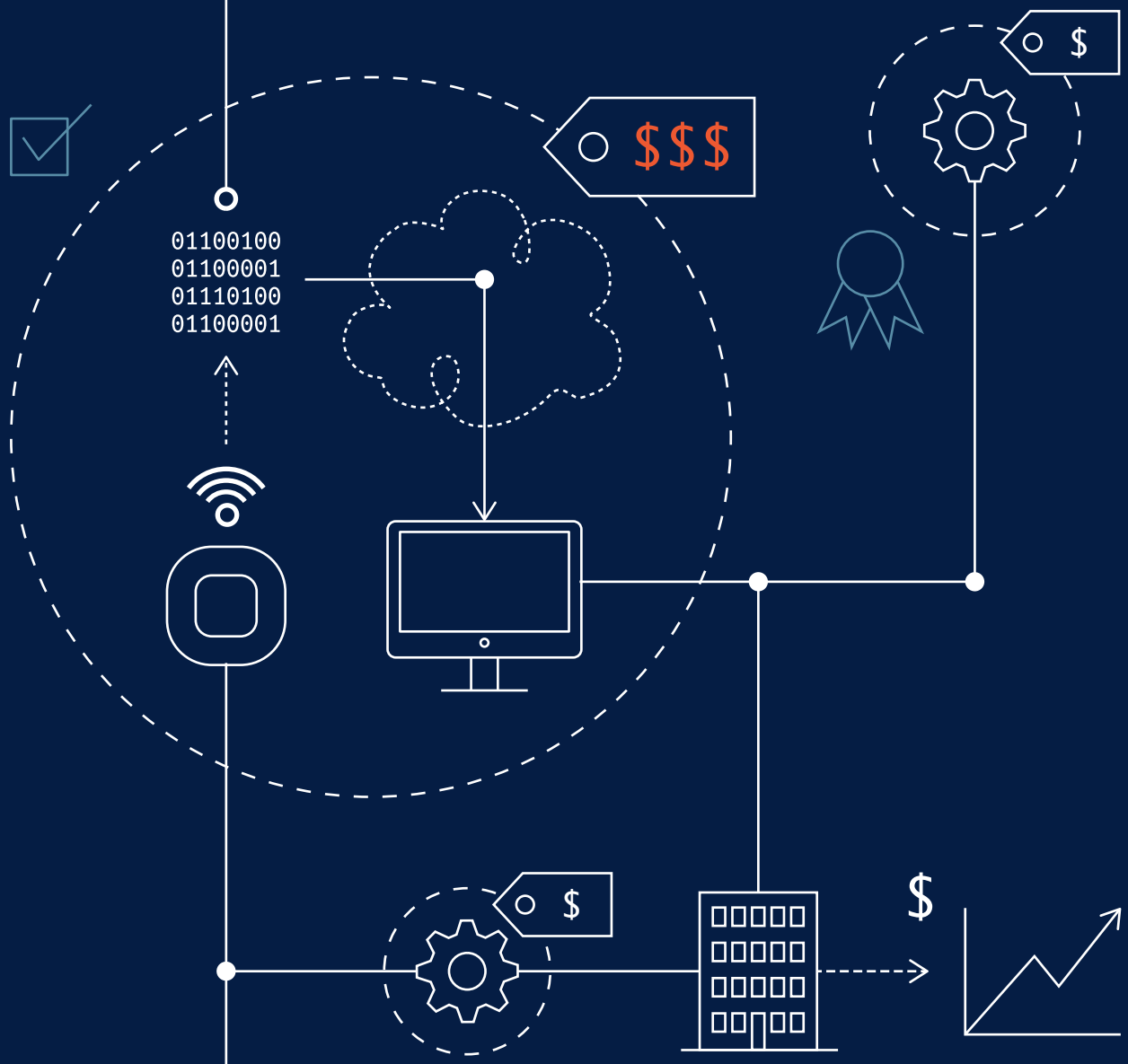
Public spaces IoT

Governments looking to implement IoT-based smart city projects face two significant risks in particular. The first is vendor lock-in. Some government entities have set up policies in the hope of avoiding this problem. "The City of Los Angeles is working on standardizing the basic terms for IoT systems in all our requests for proposals," says Joyce Edson, the city's Deputy Chief Information Officer. "The city will not go for proprietary systems."

The second is data interoperability. As Jesper Weng Haar, Head of the Data Department at the Danish Agency for Data Supply and Efficiency, says, "Due to data format differences, data generated from similar projects in different cities cannot be integrated and exchanged." This significantly undermines the value of publicly funded projects, he concludes.

6

Enabling economic viability



Few new technologies come without some degree of economic risk, no matter the domain for which they are intended. The history of technology in the enterprise and public spheres is littered with enormously expensive technology implementations that failed to deliver on the promised functionality and benefits. In an age of rapid innovation, consumers can find themselves stuck with "the latest thing" that soon becomes outmoded.

In many ways, IoT is no different. Like all technologies, potential risks to economic and operational viability could prevent IoT devices, applications and systems from being financially and operationally sustainable, both in the planning stages and throughout their life cycles. Yet due to its sheer scope, its transformative potential and the nature of its goals and potential benefits, the economic risks of IoT are worth addressing.

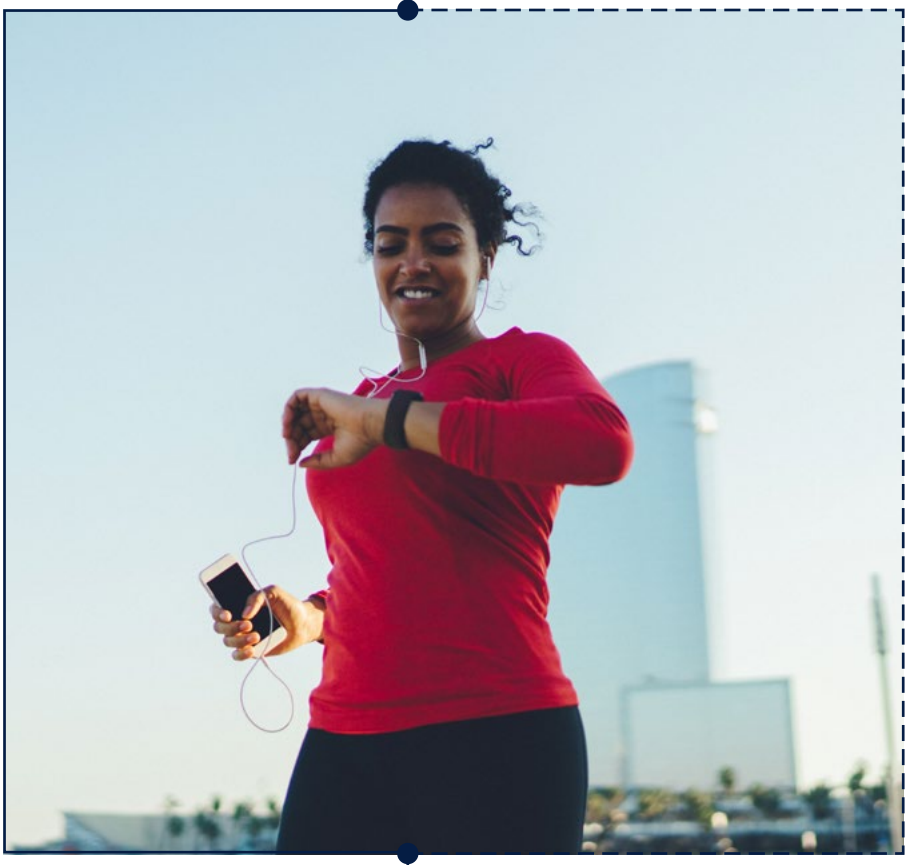
Devising governance mechanisms for mitigating economic risk is especially difficult, given that such potential risks are often self-imposed, whether by businesses, public entities or consumers. Still, efforts to help offset these potential risks are ongoing, especially in the public spaces and consumer domains.

"Some smart city systems have been abandoned after initial deployments due to lack of maintenance funding and resources."

Lei Zheng, Director of the Lab for Digital and Mobile Governance at Fudan University

Risk assessment

Most enterprises calculate the value of a new technology implementation in terms of return on investment (ROI) – how much will a particular investment contribute in terms of lower costs, increased efficiency, higher revenues, greater customer satisfaction or some other metric. Public entities, too, should take such considerations into account, though the pay-off will often come in the form of social benefits that may be harder to calculate.



Certainly, many IoT projects will be subject to such an analysis. And as with any major investment, the economic risks are considerable. Generally speaking, building a reasonable business case for transformative IoT investment in enterprise or public spaces can be difficult, given the potential complexity and lengthy time to achieve a reasonable ROI. Companies looking to test the waters should consider starting small, perhaps implementing a pilot programme to test the value of a suite of IoT applications for a particular factory operation or supply-chain mechanism, before making large-scale investments in a wholesale transformation programme.

Once implemented, IoT projects can suffer from poor ROI for several reasons. Poor data quality, for example, can reduce their financial returns or other benefits. Colin Yu of Envision Digital concurs: "Some building management systems have incorrect initial configurations, which leads to the collection of incorrect data and loss of effectiveness for smart-building applications."

Another challenge is that ROI for IoT is often measured in isolation. "Some IoT use cases may not individually fully showcase the full value of IoT, but if you aggregate them together to create a data ecosystem that enables you to make better decisions, the ROI becomes much more substantial and evident," says Anil Khurana, Global Leader of PwC's Industrial Manufacturing and Automotive practice.

Meanwhile, the ongoing cost of maintenance is often underestimated. Securing the funding and resources needed to maintain a project's long-term financial sustainability and viability is critical. "Some smart city systems have been abandoned after initial deployments due to lack of maintenance funding and resources," says Lei Zheng of Fudan University. "It's a big waste for the public investment."

Public spaces IoT projects can also suffer from sponsors' reluctance to promote the projects' benefits. Eldar Tuzmukhametov, former Head of the Smart City Lab at the City of Moscow IT Department, notes, "A number of Russian cities have citizen engagement initiatives through digital applications, but there is no investment in PR or marketing. Because nobody planned this investment, there were not enough users of the application."

Finally, enterprises and cities frequently fail to capture the value of the data they collect. Most IoT solutions today are designed for specific purposes, and the data collected is typically not shared or monetized. But data is more valuable in the presence of other data. Data captured by IoT sensors deployed by utility companies to capture climate information, for example, could also be packaged and sold to farmers needing to monitor local weather conditions. Developing innovative uses for the data collected and merging it with data from other sources can generate considerable value and improve projects' long-term financial sustainability.

Beyond ROI

Given these challenges, it's a wonder that any organization is willing to embark on a major IoT implementation. And, indeed, anecdotal evidence suggests that many companies making investment decisions based on ROI are holding off, preferring to wait until the technology is more mature and the business case is more clear-cut. This, however, may be a mistake, for several reasons.

First, IoT's benefits are not necessarily subject to a standard cost-benefit analysis. At the tactical level, an application such as preventive maintenance will likely bring measurable returns in terms of lower costs and higher customer satisfaction. But the value of IoT must also be considered strategically. Will the digital factory's greater efficiency improve efficiency to the point where a company can shutter excess capacity? Will greater insight into supply-chain operations improve its overall agility and resilience in times of stress?

Second, companies should also take into account the range of new business models IoT could enable. Rather than selling a range of specific products, might IoT allow companies to build a portfolio of services connected to those products that would bring in a consistent ongoing revenue stream? And what risks might a service-oriented business model entail in terms of the greater operational responsibility a company might take on?

Finally, companies need to consider their competitive environment. Do they operate in an industry, such as industrial manufacturing or mining, where the tactical and strategic advantages of IoT are likely to be felt first? If so, then perhaps the biggest economic risk is to be late to the game.

Governing, economically

"Public data management platforms have the potential to dramatically reduce the overhead associated with management of IOT data streams."

Jerry Power, I3 Consortium

Most efforts to improve the financial viability of IoT projects are primarily regional or local in nature. Some countries have set up policies to encourage and drive investment in IoT. For example, Saudi Arabia's government provides tax breaks and grants to inspire companies to invest in IoT. Brazil's national IoT plan aims to ensure the development of public policies for the technology sector, and members of the country's parliament have presented legislation[81] looking to eliminate tax on IoT products.

At the local level, some cities are trying to build data marketplaces to unleash the potential value of IoT data. The City of Los Angeles, for example, is working with the Intelligent IoT Integration Consortium (I3), a platform built in collaboration with the University of Southern California, to enable data collected by different sensors from the public and private sectors to be integrated with built-in security and privacy measures. According to Jerry Power of I3 Consortium: "Public data management platforms have the potential to dramatically reduce the overhead associated with management of IOT data streams, freeing them to focus on the value-added nature of their specific application."

Still, efforts to educate the public and industry stakeholders on the business potential of IoT are lagging. As Juan Pablo Cosentino of Austral University notes: "Owners of dairy farms in Argentina do not want to use another technology if they do not see real potential for business improvement. A lack of incentives and education on the value of IoT prevents people from seeing the return on investment that applications can offer."

Domain discussions

Enterprise IoT

There are two key economic viability risks and impacts specific to enterprise. The first is enabling an adequate ROI. Enterprise projects usually require relatively fast returns, while it can take a long time to collect the data needed to train the algorithms employed in certain IoT applications such as predictive maintenance. As a result, enterprises can struggle to build attractive business cases for IoT projects.

Second, there is still a significant knowledge gap between enterprise users' expectations for IoT and the ability of IoT solution providers to meet them. To bridge this gap, Yu Zhao of BOSCH China suggests working with industrial clients "to create and implement IoT-based predictive maintenance systems, for example, in an incremental approach, starting with small applications to rapidly demonstrate some benefits of the application and then introducing applications that provide additional benefits but require longer periods of investment".

Lastly, many enterprises lack a cohesive IoT strategy and roadmap. This often leads to different departments building out redundant and incompatible IoT systems, creating interoperability challenges and adding costs.

To alleviate such problems, respondents to our survey point out that enterprises should collaborate to develop industry-specific techniques on which they can then rely to manage their IoT operations. In addition, they suggest that corporate decision-makers need to gain a better understanding of the range of business models suitable for enterprise IoT applications.

Consumer IoT

Unlike most enterprise IoT applications, which usually demand clear business outcomes, consumer IoT applications are focused on end-user needs such as safety, convenience, quality of life and other personal issues. Building trust is crucial in tapping the potential of the consumer IoT as a source of economic growth and innovation.[82] From the consumer's point of view, enabling better interoperability of consumer IoT devices may also improve their economic sustainability.

Public spaces IoT

Implementations of IoT in public spaces face several critical economic risks. The first is the financial stability of vendors. Joyce Edson provides an example: "We worked on a robotics-based project to teach kids in school that sensors are not dangerous," she says. "The vendor for the project went out of business right before the rollout of the project. Luckily, the city had not invested a considerable amount of funding in the project, but we are always watchful of investments of public funds."

Second, public entities may be at a considerable disadvantage when evaluating and selecting IoT vendors. There is significant asymmetry between the information and expertise available to government officials who have to assess options and the information held by potential providers. This also makes it difficult for public officials to accurately calculate the ROI for public investments, which all too often may result in the projects' failure.

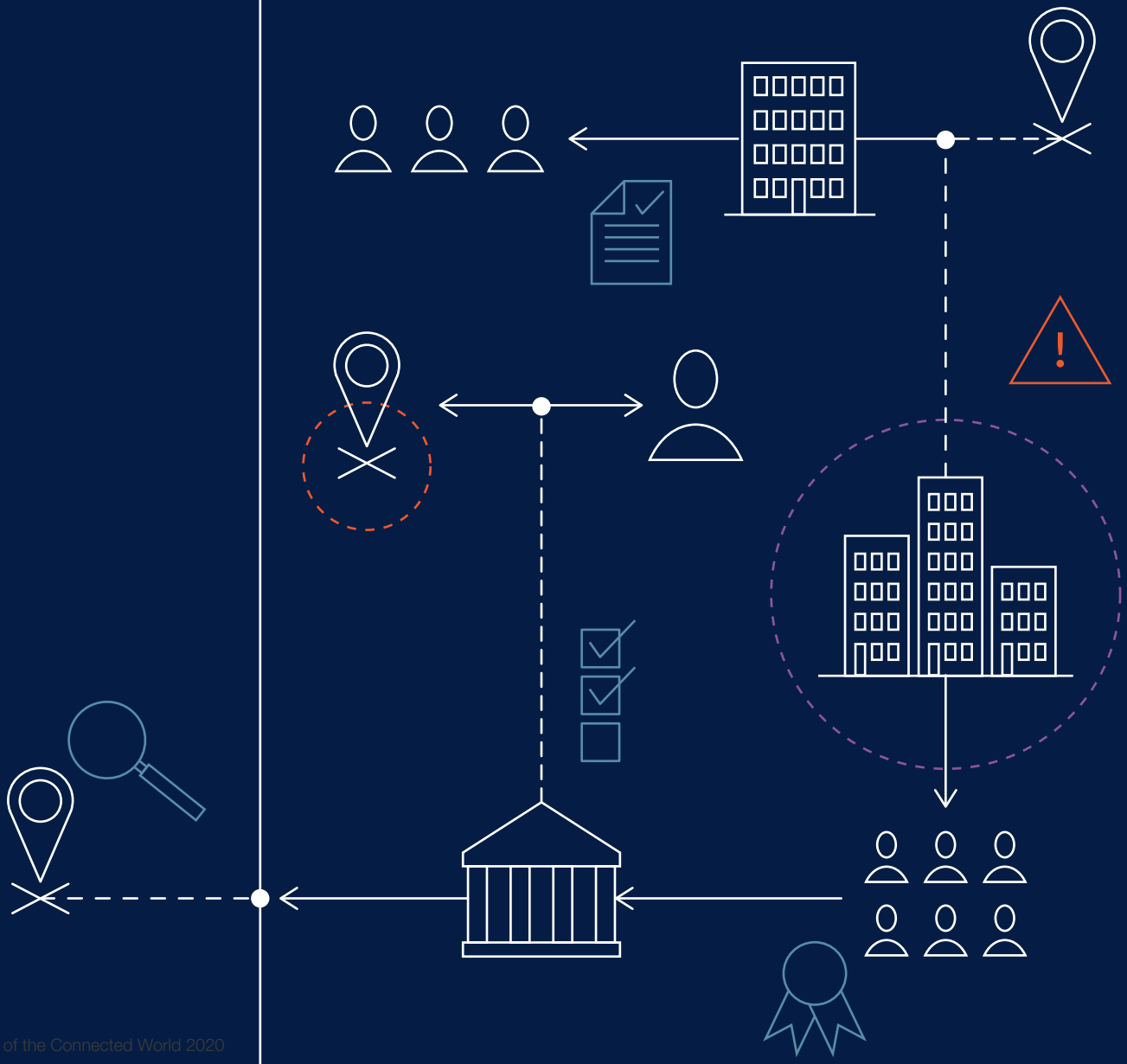
Third, managerial and process failures often prevent IoT data from being used effectively. The City of Moscow's former Head of Smart City Lab, Eldar Tuzmukhametov, says: "Citizens in Moscow were unsure whether utilities were accurately tracking usage. So the city put a data platform in place to measure utility consumption. However, it took more than six months to enact the legislation needed to allow the city to use the data it was gathering to settle disputes between utility providers and citizens."

Finally, cities struggle to monetize their smart city applications. "To enable and scale smart cities and smart connected spaces across multiple verticals, city leaders must ensure that their IoT solutions are easily upgradeable with the latest technology and innovations and there are ways to monetize these new systems. While some of this will come from increased efficiencies in city management, it will require offering end-to-end platforms and 'IoT as a service' solutions, thus providing a new structured approach to monetization, as there is no one-size-fits-all model across all global cities," says Sanjeet Pandit of Qualcomm. Like many smart city ecosystem stakeholders, Qualcomm has set up a Smart Cities Accelerator Program to connect the public sector with a variety of carefully vetted business partners and providers to deliver greater efficiencies, cost savings, and improved safety and sustainability from unique solutions that are targeted to each city's specific needs.

To alleviate some of the economic pressure on new IoT projects, some cities are working on ensuring continuous investment in their IoT projects. For example, the City of Long Beach's Ryan Kurtzman says he is exploring ways to budget and integrate IoT into every capital-planning project in order to secure their financial sustainability and long-term viability. Indeed, survey respondents agreed that risks to smart city projects can be reduced by establishing a sustainability plan throughout a project's life cycle, including vendor management, marketing, implementation and maintenance.

7

Governing complex systems



In addition to enabling us to analyse the level of potential risks and governance gaps in IoT across the five impact areas, our survey of global IoT stakeholders across the public and private sectors provided data on their extent in specific geographies and among three key groups of stakeholders.

Geographic differences

The heatmaps in Figure 7, Figure 8 and Figure 9 illustrate the degree of risk and the size of governance gap within the enterprise, public spaces and consumer domains both globally and across six key geographic regions.

01100100
01100001
01110100
01100001

Figure 7: **Survey results: risk by region**

Based on data from the Council's Survey of Subject Matter Experts, n = 374

Figure 8: **Survey results: governance by region**

Based on data from the Council's Survey of Subject Matter Experts, n = 374

Governance		Respondent region						
Domain	Impact area	**Global**	North America	Asia Pacific	Europe	Latin America	Africa	Middle East
Consumer	Safety and security							
	Privacy and trust							
	Interoperability and system architecture							
	Societal benefit and equity							
	Economic viability							
Enterprise	Safety and security							
	Privacy and trust							
	Interoperability and system architecture							
	Societal benefit and equity							
	Economic viability							
Public spaces	Safety and security							
	Privacy and trust							
	Interoperability and system architecture							
	Societal benefit and equity							
	Economic viability							

Governance level ⟶

01100100
01100001
01110100
01100001

Figure 9: **Survey results: governance gap by region**

Based on data from the Council's Survey of Subject Matter Experts, n = 374

Domain discussions

Consumer IoT

Survey respondents from Latin America perceive the risks from IoT to be the highest among all regions. This is likely because consumer IoT applications such as smart homes and connected cars have not been widely adopted in most Latin America countries,[83] and this in turn may reflect consumers' concerns and lack of knowledge about them. Lack of updated and enforceable data and consumer protection frameworks that provide adequate governance and security for consumers in the region may also exacerbate the perceived risks of IoT.

In contrast, African respondents generally perceive the risks from consumer IoT applications to be lower than respondents from other regions. Since Africa is still lagging behind the rest of the world in internet penetration,[84] it may take some time for the general public to familiarize themselves with consumer IoT applications and gather enough information to assess their associated risks.

Enterprise IoT

Respondents across all regions align on the perceived risk and governance gap levels of enterprise IoT, although respondents from North America believe that the risks and governance gaps associated with safety and security are especially high. PwC's 2019 IoT survey suggests why: Almost half of US-based respondents to that survey admitted that cybersecurity issues have slowed or thwarted their progress in implementing IoT applications.[85]

Moreover, North America is subject to more cyberattacks than other regions, since businesses there rely more on internet-connected devices in their daily operations. While national cybersecurity regulations and enterprise security policies are in place in North America, enterprises there still consider the current governance level to be insufficient.

Public spaces IoT

Respondents from developed regions such as North America and Europe perceive the societal- and equity-related risks and governance gaps to be significantly higher than respondents from other regions. This may be a result of the relatively early development and deployment of public spaces IoT applications in these regions, which has led to a better understanding of their societal implications and both the positive and negative societal consequences of their implementations. While some countries in the Asia-Pacific region have also been early adopters of public spaces IoT, stakeholders there do not perceive the societal risks and governance gaps to be as high. This may be due to cultural differences and societal paradigms between the West and the East.[86]

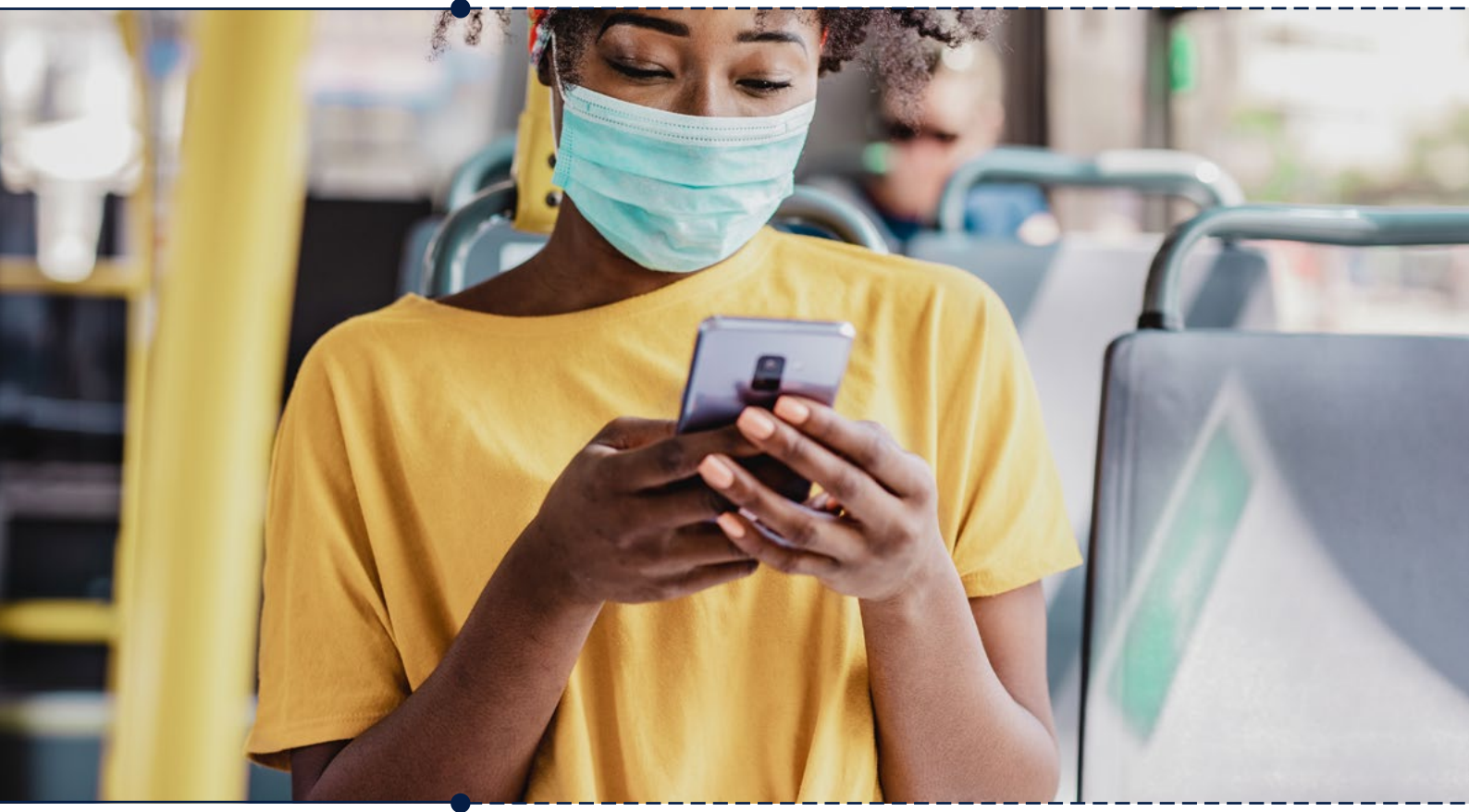
On the other hand, respondents in Asia Pacific perceive the impact and governance gap associated with IoT interoperability to be much higher than respondents from other regions. This is likely a result of the lessons learned in overcoming the challenges of large-scale public spaces IoT application deployments there, such as smart lighting, smart transportation and surveillance cameras.

Stakeholder differences

The heatmaps in Figure 10, Figure 11 and Figure 12 illustrate the degree of risk and the size of gap within the enterprise, public spaces and consumer domains as perceived by respondents across three different sectors.

Enterprise players see the risks from IoT in the consumer and public spaces domains as being significantly lower than respondents from government and the public sector across all five risk areas. This divergence reflects the different views from different parts of the IoT ecosystem. Private-sector players, which include IoT manufacturers and service providers, usually prefer less governance, making it easier and more cost efficient for them to develop and take their products and services to market. On the other hand, because governments and public-sector entities are responsible for overseeing and protecting the interests of consumers and individuals, they tend to perceive both higher risks and greater governance gaps. Civil society's view seems to be more aligned with governments and the public sector than with the private sector, suggesting the overall immaturity of the state of IoT governance.

In contrast to their views on consumer and public spaces IoT applications, respondents from the public sector perceive the risks and governance gap levels in enterprise IoT applications to be the lowest. This is likely due to the fact that private-sector players are both providers and users of enterprise IoT solutions.



01100100
01100001
01110100
01100001

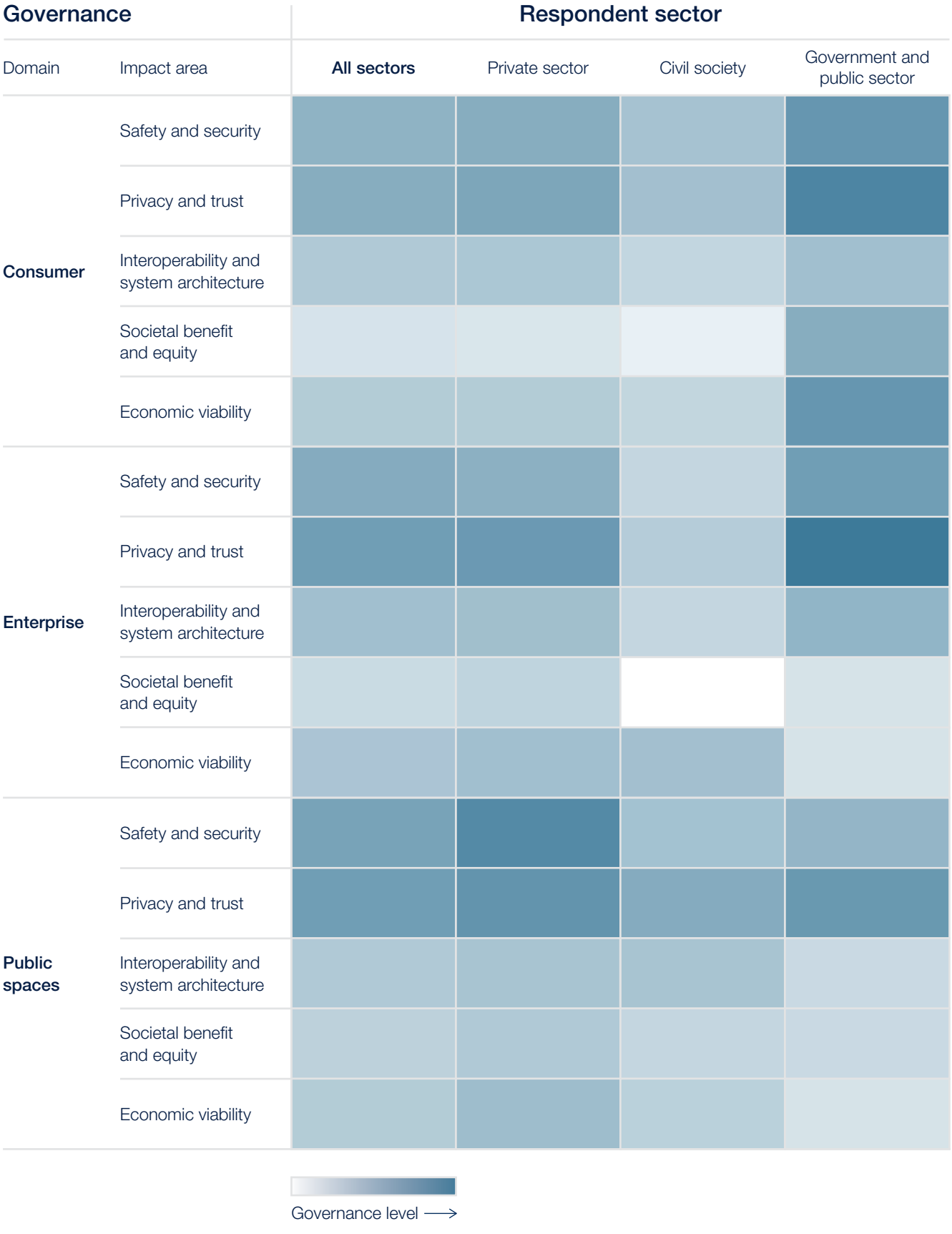
Figure 10: **Survey results: risk by sector**

Based on data from the Council's Survey of Subject Matter Experts, n = 374

01100100
01100001
01110100
01100001

Figure 11: **Survey results: governance by sector**

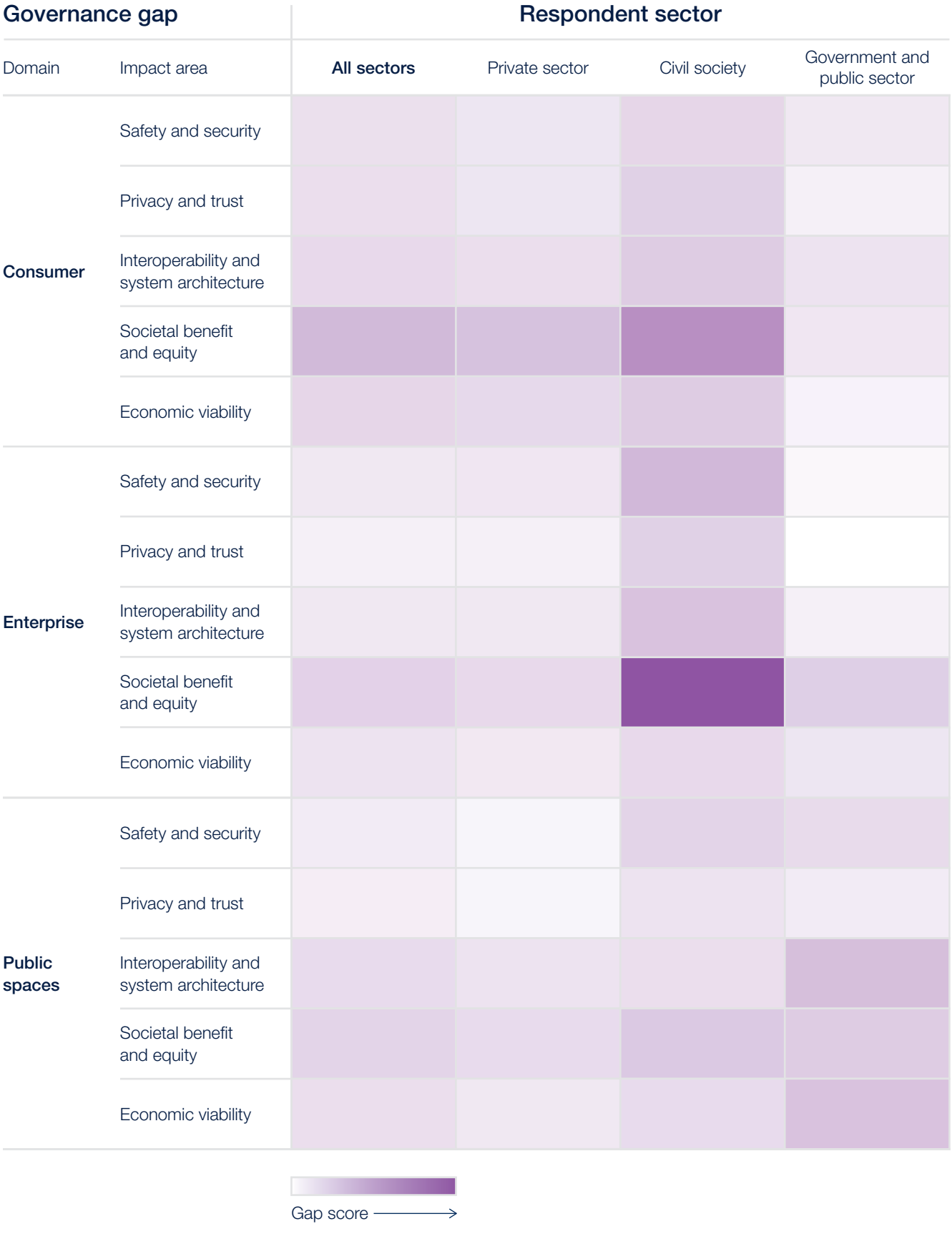
Based on data from the Council's Survey of Subject Matter Experts, n = 374



01100100
01100001
01110100
01100001

Figure 12: **Survey results: governance gap by sector**

Based on data from the Council's Survey of Subject Matter Experts, n = 374



Overarching issues and themes

Our analysis of the survey results, together with the extensive interviews we conducted with stakeholders, brought out several issues related to perceptions of IoT risk and governance that cut across every impact area and domain.

Flexible approach to governance

As the previous chapters have made clear, the many risks inherent in IoT have not yet been effectively mitigated, and the state of IoT governance remains immature. At the same time, however, the effort to manage these risks can lead, in some cases, to inappropriate regulation, which in turn can threaten the value and effectiveness of many kinds of IoT applications.

"There are cross-border data exchanges that should happen but [are] not happening today. Policy-makers should work together to find a balance between facilitation and protection."

Lei Zheng, Fudan University

The issue of cross-border data exchange is a case in point. With the digitization of the physical world, data is becoming a critical asset for countries and companies alike, thanks both to its economic value and to its importance in maintaining national security and protecting personal data. Yet countries around the world are beginning to put stringent restrictions on the movement of data across borders. Some, such as Russia, require that all data gathered there must also be stored and processed locally; other countries allow international data transfers only under certain conditions.[87]

Restrictions on cross-border data transfers can pose tremendous challenges to multinational companies in particular. Stringent data transfer measures can prevent them from using data from around the globe to enhance operational efficiencies. As Charlotte Roule of ENGIE China notes: "For ENGIE, as for any market player, cross-border data transfer is key to make the most of the experience it gained worldwide on similar projects or assets, for its customers' benefit." Restrictions on cross-border data exchange can also stymie innovation. "The value from data is lowered when cross-border data exchange is prohibited," says Xiaodong Lee, Founder and Chief Executive Officer of the Fuxi Institution in China. "There are some over-protections here because nobody knows where the appropriate boundary is. We need a global platform to discuss and define the boundary and facilitate cross-border data index and exchange with appropriate protection." This view is echoed by Lei Zheng of Fudan University. "There are cross-border data exchanges that should happen but [are] not happening today," he says. "Policy-makers should work together to find a balance between facilitation and protection." While reaching full alignment across the globe could be extremely challenging, better mechanisms could be worked out for the policy and technical communities to discuss the issue in a constructive way.

Some efforts are being made to facilitate the global conversation on cross-border transfer. For example, Japan's former prime minister, Shinzo Abe, announced the launch of the "Osaka Track" during the G20 summit in January 2019 with the goal of promoting an overarching framework for "Data Free Flow with Trust".[88] However, no significant progress has yet been made.

This issue is becoming even more important in light of the COVID-19 pandemic. If governments and global healthcare organizations cannot efficiently share data on the virus, it may hinder the global effort to fight the disease.

Fears of the societal risks of IoT are also leading to another kind of regulatory challenge – the banning of some IoT technologies outright. In the US, for example, the city of Cambridge, Massachusetts, has banned the public use of facial recognition technology.[89] According to Taskin Padir, Director of Experiential Robotics at Northeastern University, "We sometimes choose to ban emerging technologies because we don't know how to regulate them yet. As we understand the benefits of a specific technology for the society, its use in our daily lives becomes ubiquitous."

Fragmentation

As important as it is to govern the use of many types of IoT applications, privacy and cybersecurity regulations remain fragmented across the globe. "In California alone, there are over 150 privacy- and security-related regulations already on the books," notes Jerry Power of I3 Consortium, "It makes enforcement challenging." Sector-specific privacy and cybersecurity regulations for industries such as banking and healthcare, for example, make compliance complex and expensive, especially for start-ups with limited resources. Many survey and interview respondents acknowledged the desire for a single streamlined, sector-neutral regulatory framework issued by industry bodies or governments.

Besides the patchwork regulations for privacy and cybersecurity, most current regulations are general and not focused on IoT risks. "People need to understand IoT before incorporating those devices into existing governance measures," says Swarun Kumar of Carnegie Mellon University. "It would be a mistake to deploy IoT devices (and networks) and start using them for critical applications without properly understanding and addressing the security risks, as retroactively securing them is going to be extremely hard and expensive, as well as time consuming, and sometimes it may not even be possible at all." Adds Prakash Sangam, Founder and Principal of Tantra Analyst, "Governments and industry leaders should set up mandatory minimum security requirements for any IoT device being brought online."

Opacity of business models

Trust in IoT is essential if it is to be adopted at scale, and full transparency into the data collected and how it is processed is critical to engendering that trust. End users should be able to understand, control and consent to the types of data generated and shared through IoT, and it is up to IoT device vendors and service providers to be transparent about how the data they collect is being used. Jocelyn Aqua of PwC US says, "Companies always have room to improve their transparency efforts. It is important for companies to include information on data sales and transfers in their terms and conditions of use."

The talent gap

Together with other technologies, such as AI and robotics, IoT is enabling the so-called "Fourth Industrial Revolution", which will involve further automating all kinds of processes in many industries. According to a 2019 survey conducted by PwC, more than half of workers believe automation will significantly change how they work or make their jobs obsolete within the next 10 years.[90] "Jobs that are repetitive and can be replaced by automated workflows will be significantly changing or diminishing in the near future," says IBM Watson's Mohammad Ismail. "However, there will be a greater need for domain experts to assist with digital technologies."

Already, societies are scrambling to adapt to the change. According to LinkedIn, demand for data scientists in the US has grown exponentially. Besides the shortage of technology-sector talent, "the skills required to create good policy around IoT are still developing," says Yalena Coleman, Solution Architect of Applied Data and Technology at Connected Places Catapult in London, UK. Without the talent needed to understand IoT and its use in both the

enterprise and public spaces domains and to create proper mechanisms for governing it, IoT's growth will likely be slowed considerably.

As IoT technologies and applications continue to evolve at an accelerated pace, the need for education to equip our next generation of experts with critical skills to fill the talent gap becomes paramount. It is critical for everyone to understand the emerging technology trends and how they may affect our society.

At the same time, employers are likely to face resistance in their efforts to replace workers through automation. "One of the preconditions before a large automotive manufacturer could start a plant modernization project here in South Africa is that there must be no job loss," says IoT practitioner George Kaleibela. While governments and enterprises are aware of the needs to retrain and upskill workers in the age of automation, "public spending on labour-force training and support has fallen steadily for years in most member countries of the Organisation for Economic Co-operation and Development (OECD)," according to consultancy firm McKinsey. "Nor do corporate-training budgets appear to be on any kind of upswing."[91]

"The waste being produced is enormous, and there is no global solution on recycling the huge amount of electronics, most of which have relatively short lives."

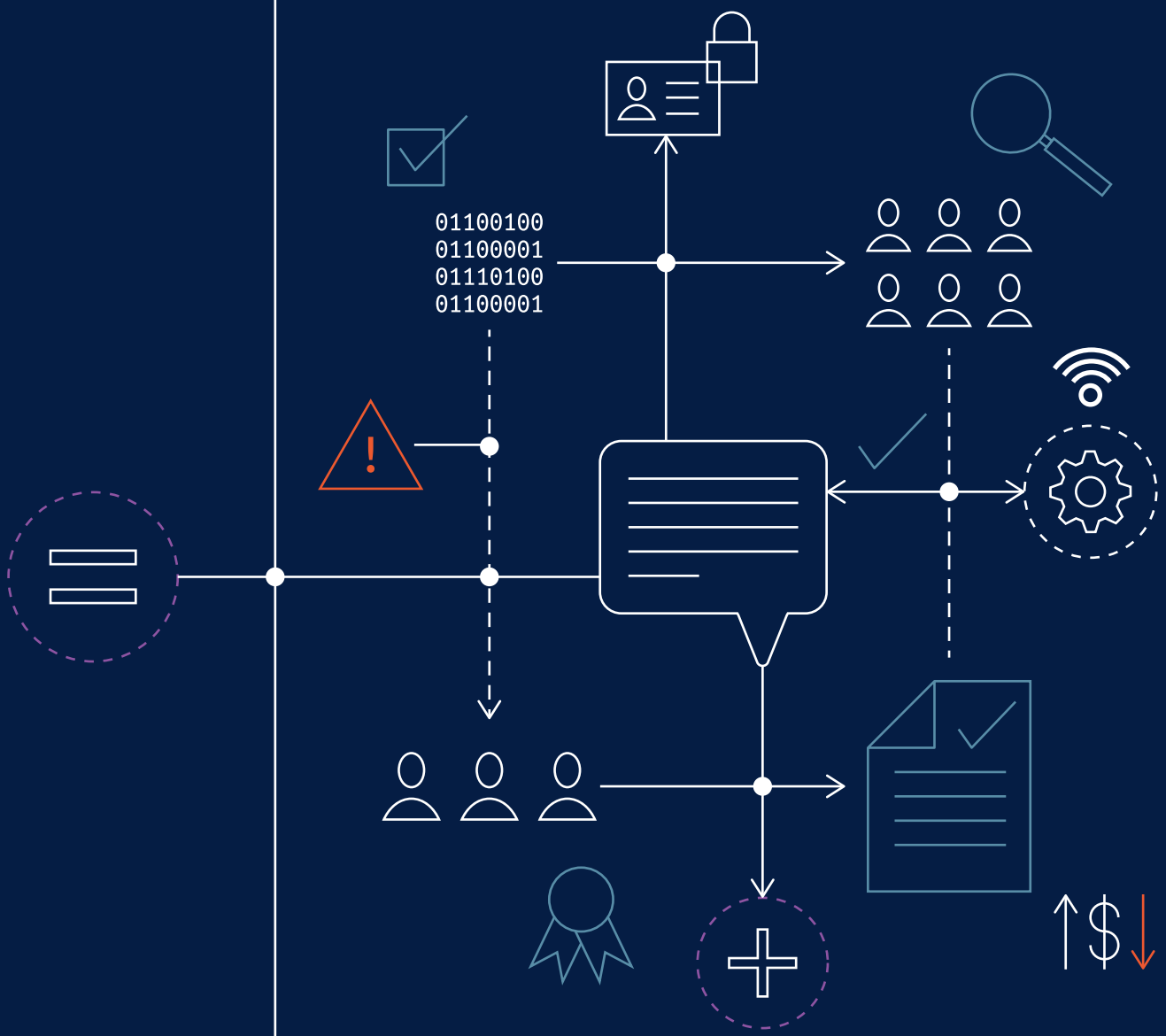
Gilbert Kamieniecky, Head of Private Equity Technology, Investcorp

The environmental impact of e-waste

Among the risks stemming from the proliferation of IoT devices is a significant increase in e-waste – not just sensors, actuators and other IoT devices and appliances, but also the plugs, electric cables and batteries that keep IoT applications running. "The waste being produced is enormous, and there is no global solution on recycling the huge amount of electronics, most of which have relatively short lives. The consumer IoT is perhaps the biggest source of waste, but the industrial IoT may also produce them," says Gilbert Kamieniecky, Head of Private Equity Technology at Investcorp.

To cope with the challenge, the PETRAS National Centre of Excellence for IoT Systems Cybersecurity has suggested a design approach for making IoT devices more sustainable, with design-for-life principles to enable users to effectively repair, upgrade, customize and recycle IoT devices.[92] The World Economic Forum has started an initiative for reducing e-waste, with the goal of enabling a circular economy for electronic devices in China through public-private cooperation.[93] The initiative supports the work of the E-Waste Coalition, a group of seven UN entities that have come together to increase cooperation and provide more efficient support to the UN's member states to address the e-waste challenge. The Forum hopes to end electronic waste, which is the fastest growing waste stream in the world, while also promoting the use of 25% recycled content in new IoT and electronics products manufactured in China.

Conclusion: Charting a path to a brighter connected future



Conclusion: Charting a path to a brighter connected future

The rise of the internet of things presents a tremendous opportunity to build a more sustainable and prosperous future for all. At the same time, it also poses new risks and governance challenges. The global COVID-19 pandemic has highlighted the role of IoT in providing the critical data needed to track and fight the disease, yet it also raises concerns about IoT's security, privacy, interoperability, economic sustainability and equity. Addressing the risks and governance gaps identified in this report is critical to enabling trust in IoT and promoting its long-term growth.

In response to the findings of this report, the World Economic Forum in partnership with the Global IoT Council has developed a Global Action Plan that aims to encourage collective action on the most pressing challenges the connected world currently faces. IoT is already an indispensable part of our daily lives and fundamental infrastructure. As it grows in extent and capabilities, we must act if we want to realize the full potential of IoT.

The Global Action Plan is structured around a set of high-level actions, which are tied to related initiatives and commitments. Our five high-level actions are as follows.

1 Action # 1

Increase public education and understanding of connected devices and help empower individuals and organizations to make informed decisions regarding the adoption and use of these devices.

2 Action # 2

Ease and incentivize the adoption of cybersecurity best practices to enable a common duty of care among connected device manufacturers, system integrators, service providers, purchasers and users.

3 Action # 3

Increase awareness of the positive and negative impacts of connected devices on the well-being of individuals, organizations and society to incentivize adoption that benefits the world.

4 Action # 4

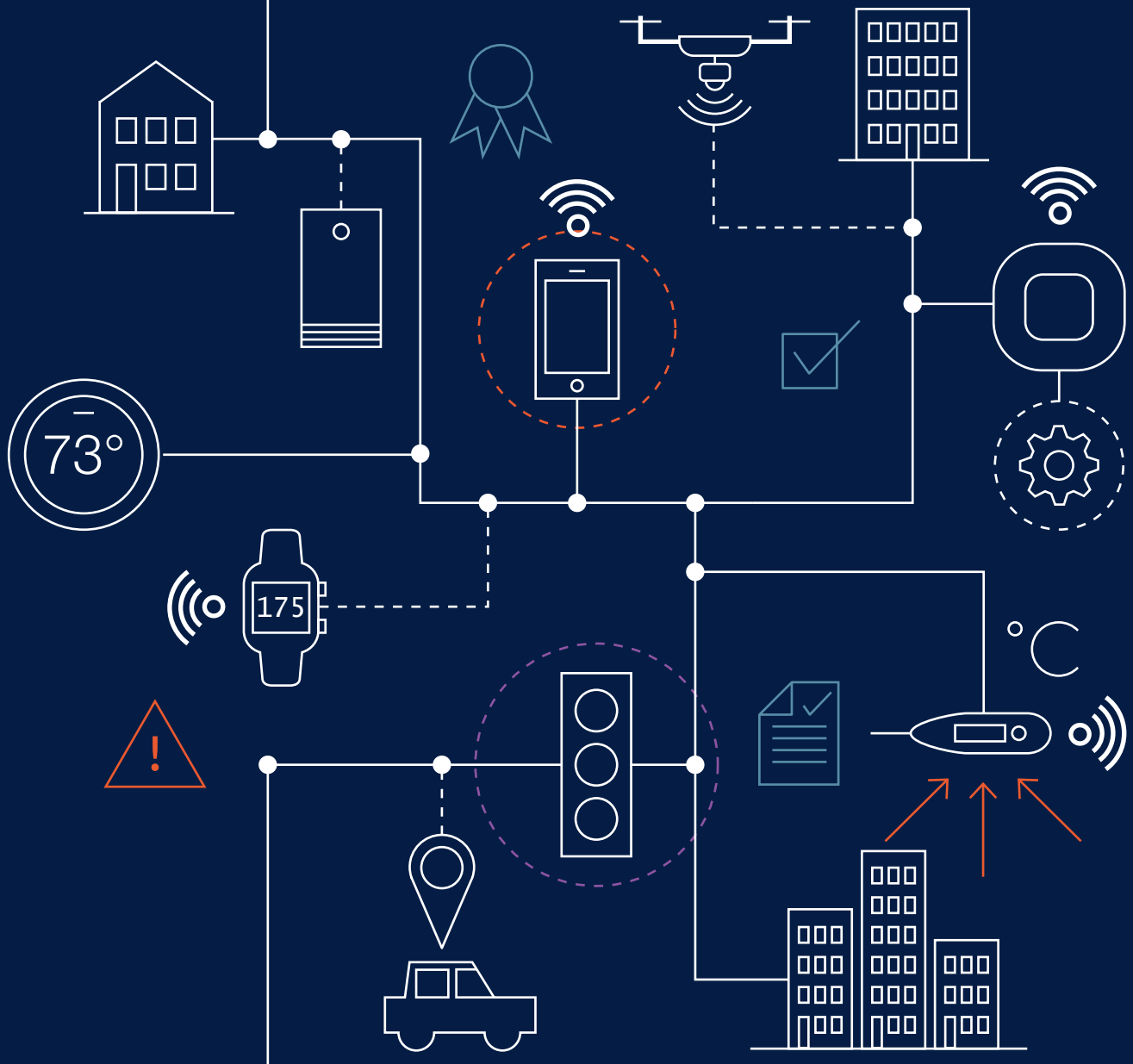
Accelerate the adoption of connected devices and systems among small and/or under-resourced communities and organizations through the introduction of new funding models, incentives and capacity-building mechanisms.

5 Action # 5

Strengthen collaboration and sharing of information and data across the IoT ecosystem to combat fragmentation of governance efforts, accelerate value creation and scale leading practices across geographies, sectors and industries.

These actions address systemic challenges, and therefore require the collective commitment of all stakeholders in the ecosystem. As such, we invite you to consider how your organization might contribute to the progress of one or more of these actions. Together, we can chart a path to a future connected world that is more sustainable, resilient and prosperous for all.

Appendices



Appendix A

Research methodology

We define a governance gap as the difference between the potential risk posed by a technology and society's ability to govern the development and use of that technology and to safeguard against its potential harm. Governance can include laws, industry standards or self-governance approaches.

The IoT governance gaps identified in this report are based on the expert perceptions of a wide range of IoT industry stakeholders. We have analysed them across two dimensions – impact areas and application domains:

Impact areas:

- **Safety and security:** The ability of IoT devices, applications and systems to maintain a safe and secure development, deployment and operational environment.
- **Privacy and trust:** The ability of IoT devices and systems to safeguard the privacy of users and engender trust that personal information will be collected, stored and used for agreed purposes in an ethical and responsible manner.
- **Interoperability and system architecture:** The ability of IoT devices and systems to interact effectively with each other to execute tasks in an efficient and cost-effective manner.
- **Societal benefits and equity:** The ability of IoT devices and systems to fairly benefit and protect societal stakeholders irrespective of geographic, socioeconomic or other factors.
- **Economic viability:** The ability of IoT devices and systems to be financially and operationally sustainable throughout their life cycles in the context of rapid technological and social changes.

Application domains:

- **Consumer domain:** Consumer-facing IoT applications such as smart home devices, internet-connected appliances, wearables and connected health-monitoring devices.
- **Enterprise domain:** Enterprise IoT applications such as smart factories, connected supply chains, intelligent building management systems and precision agriculture.
- **Public spaces domain:** IoT applications in public spaces such as smart city technologies for traffic and lighting management, public safety solutions, and emergency notification, waste management and fleet management systems.

The research involved a combination of quantitative and qualitative approaches, including surveys, interviews, workshops and desktop research.

Quantitative research: We distributed our State of the Global IoT Governance survey to IoT experts in the private and public sectors and to private citizens in civil society, asking them to assess both the risks associated with IoT and the current level of society's ability to safeguard against harm from these risks. (See Appendix B for demographic information on survey respondents.) We received 374 responses from around the globe, which we used to calculate the risk impact score, the current governance level score and the governance gap score for all five risk impact areas within all three domains.

We then stack-ranked the data collected into the heatmaps presented in Chapter 7, based on the overall level of risk and the current state of governance.

The initial results from the quantitative analysis were validated through a series of workshops carried out at Carnegie Mellon University in the US and University College, London.

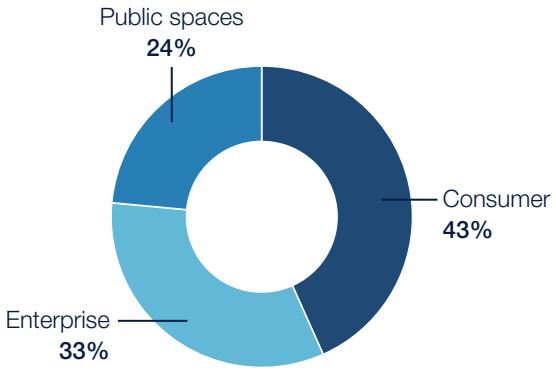
Qualitative research: In addition to the quantitative data from the survey, the survey respondents were asked to provide qualitative responses on examples of risk and governance measures as input to our qualitative research. We also conducted more than 50 interviews with global IoT experts to capture further insights on IoT risks and governance across the three domains. Finally, we conducted extensive desktop research on current governance measures across the globe

Taken together, the results of the quantitative analysis and the input from qualitative research enabled us to identify and prioritize the key IoT governance gaps described in this report.

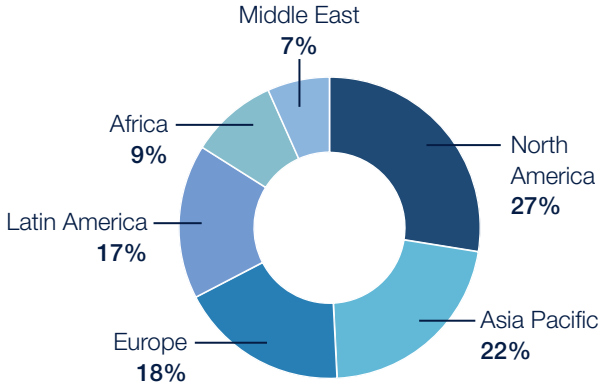
2020 Global State of IoT Survey demographics

Total # of complete responses: 374

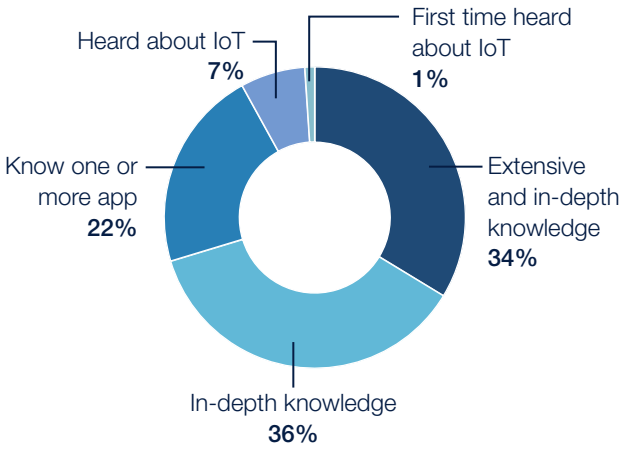
Area of expertise of respondents



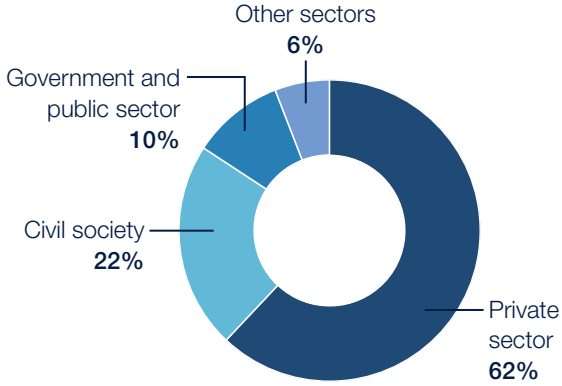
Region of respondents



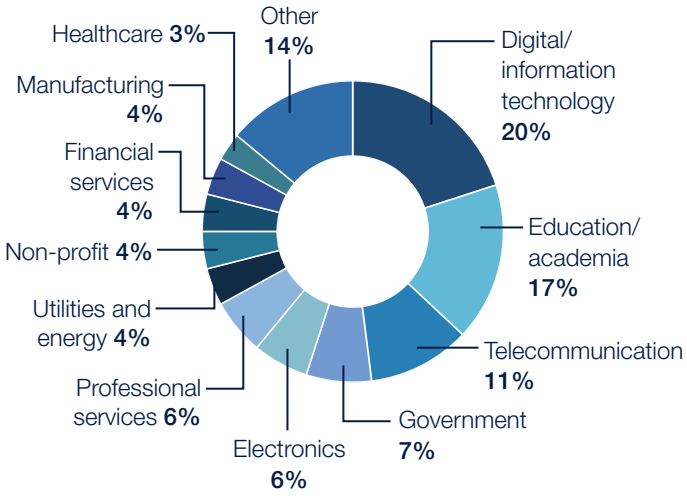
Level of knowledge about IoT



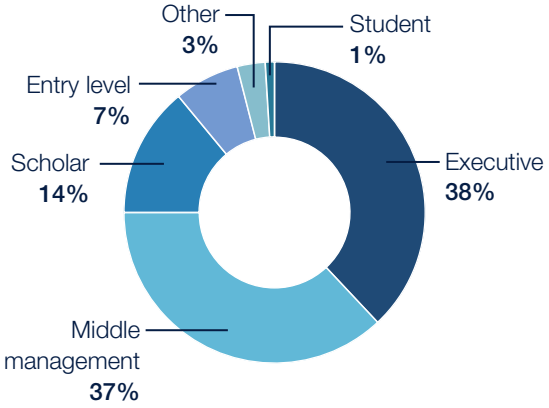
Sector categories of respondents



Employment sector of respondents



Employment level of respondents



Acknowledgements

The Global Internet of Things Council

This white paper benefitted from the input, guidance and review of the experts and stakeholders on the World Economic Forum's Global Internet of Things Council.

Council Co-Chairs

Cristiano Amon
President, Qualcomm Incorporated, USA

Adrian Lovett
President and Chief Executive Officer, World Wide Web Foundation, USA

Stella Ndabeni-Abrahams
Minister of Communications and Digital Technologies, Republic of South Africa

Report Review Committee

Cassandra Beck
Senior Public Relations Representative, Qualcomm Incorporated, USA

María Paz Canales
Executive Director, Derechos Digitales, Brazil

Madeline Carr
Professor of Global Politics and Cybersecurity, University College London, UK

Sam Hartmann
Special Assistant to the President and Chief Executive Officer, World Wide Web Foundation, USA

Eleri Jones
Head of PETRAS National Centre of Excellence for IoT Cybersecurity, University College London, UK

Karen Lightman
Executive Director, Metro21, Carnegie Mellon University, USA

Council Members

Anousheh Ansari
Chief Executive Officer, XPrize Foundation, USA

Alicia Asín
Chief Executive Officer, Libelium, Spain

Nihat Bayiz
Head of Global Research and Development, ARCELIK, Turkey

María Paz Canales
Executive Director, Derechos Digitales, Brazil

Madeline Carr
Professor of Global Politics and Cybersecurity, University College, London, UK

Fadi Chehadé
Co-Chief Executive Officer, Ethos Capital, US

Cristina Colom
Director, Digital Future Society, Mobile World Capital Barcelona, Spain

Sarah Cooper
General Manager, IoT Solutions, Amazon Web Services, USA

Carlos Alexandre Jorge da Costa
Deputy Minister for Productivity, Employment and Competitiveness, Ministry of Economy of Brazil, Brazil

Nobuhiro Endo
Chairman of the Board, NEC Corporation, Japan

Sridhar Gadhi
Founder and Chief Executive, Quantela, USA

Madeline Gannon
Founder and Principal Researcher, Atonaton, USA

Ken Hu
Deputy Chairman and Rotating Chairman, Huawei Technologies, People's Republic of China

Farnam Jahanian
President, Carnegie Mellon University, USA

Helena Leurent
Director-General, Consumers International, UK

Fanyu Lin
Chief Executive Officer, Fluxus, USA

Kristian Møller
Director General, Danish Agency for Data Supply and Efficiency, Danish Government, Denmark

Keisuke Naito
Vice-President, Chief Digital Officer, Dementia Total Inclusive Ecosystem, Eisai, Japan

Julie Owono
Executive Director, Internet Sans Frontières (Internet Without Borders), France

Victor Pineda
President, World Enabled, USA

David G. Rosenberg
Co-Founder and Chief Executive Officer, AeroFarms, USA

Charlotte Roule
Chief Executive Officer, China, ENGIE Group, France

Richard Soley
Chairman and Chief Executive Officer, Object Management Group, US

Åsa Tamsons
Senior Vice-President; Head, Business Area Technologies and New Businesses, Telefonaktiebolaget LM Ericsson, Sweden

Michele Turner
Senior Director, Google Smart Home Ecosystem, Google, USA

Jan van Zoest
Chief Architect, Royal Philips, Netherlands

Lauren Woodman
Chief Executive Officer, NetHope, US

Kuek Yu Chuang
Former Vice-President, Asia-Pacific, Netflix, Singapore

Additional acknowledgements

The World Economic Forum, PwC and the Global IoT Council would like to acknowledge the many experts and representatives from companies large and small, industry associations, academia, government and civil society who participated in the report interviews, surveys and workshops.

We offer our special thanks to the Global IoT Council's Research Fellow Tushaar Bhatt and members of the World Economic Forum's Platform for Shaping the Future of the Internet of Things and Urban Transformation for their dedication and support to help bring this initiative to life.

Finally, the authors would like to thank Edward Baker for his patience and dedication to pulling this report together through multiple reviews over many months.

Contributors — Lead Authors

World Economic Forum

Jeff Merritt
Head, Internet of Things and Urban Transformation
World Economic Forum

Geoffrey Wylde
Lead, Internet of Things and Urban Transformation
World Economic Forum

Kimmy Bettinger
Specialist, Data Policy
World Economic Forum

PwC

Rob Mesirow
Principal, Connected Solutions
PwC

Devin Yaung
Director, Connected Solutions
PwC

Wei Wang
Manager, Connected Solutions
PwC

Endnotes

1. IDC, The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast, June 2019, https://www.idc.com/getdoc.jsp?containerId=prUS45213219 (link as of 7/9/20).
2. GSMA, IoT's Contribution to Economic Growth, August 2019, https://www.gsma.com/iot/iot-knowledgebase/iots-contribution-to-economic-growth/ (link as of 7/9/20).
3. World Economic Forum, The Effect of the Internet of Things on Sustainability, January 2018, https://www.weforum.org/agenda/2018/01/effect-technology-sustainability-sdgs-internet-things-iot/ (link as of 7/9/20).
4. PwC, Leveraging the Upcoming Disruptions from AI and IoT, 2017, https://www.pwc.com/gx/en/industries/communications/assets/pwc-ai-and-iot.pdf (link as of 7/9/20).
5. Thomas Alsop, Technology Spending into Smart City Initiatives Worldwide from 2018 to 2023, Statista, February 2020, https://www.statista.com/statistics/884092/worldwide-spending-smart-city-initiatives/ (link as of 7/9/20).
6. Frank Gillett, Predictions 2020: IoT Expansion Brings Even More Change, Forrester, November 2019, https://go.forrester.com/blogs/predictions-2020-iot/ (link as of 7/9/20).
7. Carrie MacGillivray et al., Worldwide Internet of Things Forecast Update, 2019–2023, IDC, January 2020, https://www.idc.com/getdoc.jsp?containerId=US45862020&pageType=PRINTFRIENDLY (link as of 7/9/20).
8. James Blackman, IoT Slumps 18% with COVID-19 Impact – but Rallies Around "New Normal" in Mid-Term, Enterprise IoT Insights, May 2020, https://enterpriseiotinsights.com/20200529/channels/news/iot-slumps-with-covid-impact-rallies-around-new-normal (link as of 7/9/20).
9. Jonah M. Kessel, How Infrared Images Could Be Part of Your Daily Life, New York Times, July 2020, https://www.nytimes.com/2020/07/02/technology/coronavirus-infrared-cameras-temperature-sensors.html (link as of 7/9/20).
10. David Vergun et al., Department Uses Thermal Imaging to Detect COVID-19, US Department of Defense, May 2020, https://www.defense.gov/Explore/News/Article/Article/2178320/department-uses-thermal-imaging-to-detect-covid-19/ (link as of 7/9/20).
11. Kif Leswing, As Workplaces Slowly Reopen, Tech Companies Smell a New Multibillion-Dollar Opportunity: Helping Businesses Trace Coronavirus, CNBC, May 2020, https://www.cnbc.com/2020/05/10/coronavirus-tracing-for-workplaces-could-become-new-tech-opportunity.html (link as of 7/9/20).
12. Strategy Analytics, Strategy Analytics: Post-COVID Smart Home Device Markets Set to Rebound in 2021, July 2020, https://www.businesswire.com/news/home/20200714005194/en/Strategy-Analytics-Post-COVID-Smart-Home-Device-Markets (link as of 7/9/20).
13. GSMA Intelligence, Intelligence Brief: Covid-19 and What it Means for IoT, https://www.mobileworldlive.com/blog/intelligence-brief-covid-19-and-what-it-means-for-iot/ (link as of 7/9/20).
14. ABI Research, COVID-19 Pandemic Impact: Germ Concern over Shared Surfaces Will Help Push Near 30% Growth in Smart Home Voice Control, Apr 2020, https://www.abiresearch.com/press/covid-19-pandemic-impact-germ-concern-over-shared-surfaces-will-help-push-near-30-growth-smart-home-voice-control/ (link as of 7/9/20).
15. Strategy Analytics, Strategy Analytics: Post-COVID Smart Home Device Markets Set to Rebound in 2021, July 2020, https://www.businesswire.com/news/home/20200714005194/en/Strategy-Analytics-Post-COVID-Smart-Home-Device-Markets (link as of 7/9/20).
16. GSMA Intelligence, Intelligence Brief: Covid-19 and What It Means for IoT, May 2020, https://www.mobileworldlive.com/blog/intelligence-brief-covid-19-and-what-it-means-for-iot/ (link as of 7/9/20).
17. Meticulous Research, Industrial IoT (IIoT) Market Worth $263.4 Billion by 2027 – Exclusive Report Covering Pre and Post COVID-19 Market Analysis and Forecasts by Meticulous Research, June 2019, https://www.globenewswire.com/news-release/2020/06/19/2050758/0/en/Industrial-IoT-IIoT-Market-Worth-263-4-billion-by-2027-Exclusive-Report-Covering-Pre-and-Post-COVID-19-Market-Analysis-and-Forecasts-by-Meticulous-Research.html (link as of 7/9/20).
18. US Centers for Disease Control and Prevention, Using Telehealth to Expand Access to Essential Health Services during the COVID-19 Pandemic, June 2020, https://www.cdc.gov/coronavirus/2019-ncov/hcp/telehealth.html (link as of 7/9/20).

Endnotes

19. World Economic Forum, Realizing the Internet of Things: A Framework for Collective Action, January 2019, http://www3.weforum.org/docs/WEF_Realizing_the_Internet_of_Things.pdf (link as of 7/9/20).

20. Altman Vilandrie & Company, Survey: Nearly Half of US Firms Using Internet of Things Hit by Security Breaches, June 2017, https://www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security (link as of 7/9/20).

21. Josh Fruhlinger, The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet, CSO, March 2018, https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (link as of 7/9/20).

22. Privacy Rights Clearinghouse, Data Breach Notification in the United States and Territories, December 2018, https://privacyrights.org/resources/data-breach-notification-united-states-and-territories (link as of 7/9/20).

23. UK Department of Digital, Culture Media & Sport, Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf (link as of 7/9/20).

24. Consumers International, Consumers International Launches Trust by Design Guidelines for Consumer IoT, February 2019, https://www.consumersinternational.org/news-resources/news/releases/consumers-international-launches-trust-by-design-guidelines-for-consumer-iot/ (link as of 7/9/20).

25. Michael Fagan et al., Foundational Cybersecurity Activities for IoT Device Manufacturers, Computer Security Resource Center, May 2020, https://csrc.nist.gov/publications/detail/nistir/8259/final (link as of 7/9/20).

26. ETSI, CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI EN 303 645 V2.1.1 (2020-06), https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (link as of 12/9/20).

27. UK Department for Digital, Culture, Media & Sport, Code of Practice for Consumer IoT Security, Oct 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf (link as of 7/9/20).

28. Council to Secure the Digital Economy, The C2 Consensus on IoT Device Security Baseline Capabilities, https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf (link as of 7/9/20).

29. Cloud Security Alliance, CSA IoT Security Controls Framework, March 2019, https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework (link as of 7/9/20).

30. ioXt Alliance, ioXt Certification Program, https://www.ioxtalliance.org/get-ioxt-certified (link as of 7/9/20).

31. Ponemon Institute, Second Annual Study on the Internet of Things (IoT): A New Era of Third-Party Risk, March 2018, https://sharedassessments.org/wp-content/uploads/2018/04/2018-IoTThirdPartyRiskReport-Final-04APR18.pdf (link as of 7/9/20).

32. Katie Pyzyk, IBM, Threatcare Uncover Vulnerabilities of Smart City Tech, Smart Cities Dive, August 2018, https://www.smartcitiesdive.com/news/ibm-threatcare-uncover-vulnerabilities-of-smart-city-tech/529783/ (link as of 7/9/20).

33. Consumers International, The Trust Opportunity: Exploring Consumers' Attitudes to the Internet of Things, May 2019, https://www.consumersinternational.org/media/261950/thetrustopportunity-jointresearch.pdf (link as of 7/9/20).

34. NCTA, IoT Has Quietly and Quickly Changed Our Lives, February 2019, https://www.ncta.com/whats-new/iot-has-quietly-and-quickly-changed-our-lives (link as of 7/9/20).

35. Internet Society, Policy Brief: IoT for Policymakers, September 2019, https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/ (link as of 7/9/20).

36. Yoram Wurmser, Wearables 2019 Advanced Wearables Pick Up Pace as Fitness Trackers Slow, eMarketer, January 2019, https://www.emarketer.com/content/wearables-2019 (link as of 7/9/20).

37. Mordor Intelligence, Smart Wearable Market – Growth, Trends, and Forecast (2020–2025), 2019, https://www.mordorintelligence.com/industry-reports/smart-wearables-market (link as of 7/9/20).

38. Guido Noto La Diega and Ian Walden, Contracting for the Internet of Things: Looking into the Nest, European Journal of Law and Technology, Vol. 7, No. 2, 2016, https://ejlt.org/index.php/ejlt/article/view/450 (link as of 7/9/20).

39. David Choffnes et al., Information Exposure from Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach, September 2019, https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf (link as of 7/9/20).

40. Alice Gast, World Economic Forum, Why We Need to Talk About Big Data, January 2020, https://www.weforum.org/agenda/2020/01/privacy-in-a-world-of-ai-and-big-data (link as of 7/9/20).

Endnotes

41. Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye, Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models, Nature Communications, 10, Article 3069, July 2019, https://urldefense.proofpoint.com/v2/url?u=https-3A__www.nature.com_articles_s41467-2D019-2D10933-2D3&d=DwMGaQ&c=VWART3hH1Kkv_uOe9JqhCg&r=sMDV_PgeOAdmDWFOQCGuulQz4qnuEJbej1gSClSdM5U&m=pe1EE5y-AEiR60tKQN2V1VN2dwgKHhMZht1ryS8u2NQ&s=jXqmNP6SPRxG7P9edWrVnwHtrnM-5EYaN83d9HDemsk&e= (link as of 7/9/20).

42. Bryan Tau, Americans Favor Aggressive Coronavirus Measures, Poll Finds, The Wall Street Journal, 31 March 2020, https://www.wsj.com/articles/americans-favor-aggressive-coronavirus-measures-poll-finds-11585687911 (link as of 7/9/20).

43. World Health Organization, Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing, Interim Guidance, 28 May 2020, https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf (link as of 7/9/20).

44. Douglas Belkin and Kirsten Grind, MIT Researchers Launch Location-Tracking Effort for the New Coronavirus, The Wall Street Journal, 27 March 2020, https://www.wsj.com/articles/mit-researchers-launch-location-tracking-effort-for-the-new-coronavirus-11585315674 (link as of 7/9/20).

45. UK Department for Digital, Culture, Media & Sport, Code of Practice for Consumer IoT Security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf (link as of 7/9/20).

46. Countries covered include Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (limited to the Privacy Shield framework). European Commission, How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection, 2016, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (link as of 7/9/20).

47. Ann Cavoukian, Privacy by Design: The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices, November 2006, https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf; https://collections.ola.org/mon/24005/301946.pdf (links as of 7/9/20).

48. Aravind Ravi, Turning Privacy Laws into User Stories: CCPA for UX Designers, UX Collective, December 2019, https://uxdesign.cc/ccpa-for-ux-designers-8ccb5072e70e (link as of 7/9/20).

49. IoT Council, The Internet of Things, https://www.theinternetofthings.eu/sites/default/files/Rob%20van%20Kranenburg/Internet%20of%20Things%20Institute%20for%20Internet%20&%20Society%20Discussion%20Paper.pdf (link as of 7/9/20).

50. National Institutes of Standards and Technology, NISTR8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, June 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf (link as of 7/9/20).

51. Jennifer Patterson Tuohy, Google Kills Works with Nest as it Prepares for a Google Assistant Future, The Ambient, May 2019, https://www.the-ambient.com/news/works-with-nest-shut-down-google-assistant-1583 (link as of 7/9/20).

52. Nicholas Martin et al., How Data Protection Regulation Affects Startup Innovation. Information Systems Frontiers 21, 1307–1324, 2019, https://doi.org/10.1007/s10796-019-09974-2 (link as of 7/9/20).

53. Ann Cavoukian, Privacy by Design, The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices, November 2006, https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf; https://collections.ola.org/mon/24005/301946.pdf (links as of 7/9/20).

54. Coconut, An IDE Plugin for Developing Privacy-Friendly Apps, https://coconut-ide.github.io/ (link as of 7/9/20).

55. Sidewalk Labs, Designing for Digital Transparency in the Public Realm, https://www.sidewalklabs.com/dtpr/ (link as of 7/9/20).

56. Yunpeng Song et al., I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios, Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, April 2020, 1–13, https://dl.acm.org/doi/abs/10.1145/3313831.3376585 (link as of 7/9/20).

57. Peter Bihr, A Trustmart for IoT, September 2017, http://peterbihr.com/2017/09/a-trustmark-for-iot/ (link as of 12/9/20).

58. Yun Shen and Pierre-Antoine Vervier, Why We Need a Security and Privacy "Nutrition Label" for IoT Devices, Norton LifeLock, February 2019, https://www.nortonlifelock.com/blogs/research-group/why-we-need-security-and-privacy-nutrition-label-iot-devices (link as of 7/9/20).

59. Daniel Tkacik, Buyer Unaware: Security and Privacy Rarely Considered Before Buying IoT Devices, Carnegie Mellon University Security and Privacy Institute CyLab, May 2019, https://www.cylab.cmu.edu/news/2019/05/30-buyer-unaware-iot-devices.html (link as of 7/9/20).

Endnotes

60. Victoria O'Laughlin, Internet of Things and Privacy in Public, University of Washington Henry M Jackson School of International Studies, 12 April 2019, https://jsis.washington.edu/news/internet-of-things-and-privacy-in-public/ (link as of 7/9/20).

61. Consumers International, The Trust Opportunity: Exploring Consumer's Attitudes to the Internet of Things, May 2019, https://www.consumersinternational.org/media/261950/thetrustopportunity-jointresearch.pdf (link as of 7/9/20).

62. ITU, Measuring Digital Development Facts and Figures 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf (link as of 7/9/20).

63. The World Bank, Connecting for Inclusion: Broadband Access for All, https://www.worldbank.org/en/topic/digitaldevelopment/brief/connecting-for-inclusion-broadband-access-for-all (link as of 7/9/20).

64. Omnia Health, DoH-Abu Dhabi Launches Remote Healthcare Platform to Contain COVID-19, April 2020, https://insights.omnia-health.com/coronavirus-updates/doh-abu-dhabi-launches-remote-healthcare-platform-contain-covid-19 (link as of 7/9/20).

65. Gulf News, New Service Launched to Monitor, Treat Diabetics Remotely, January 2019, https://gulfnews.com/uae/new-service-launched-to-monitor-treat-diabetics-remotely-1.61707221 (link as of 7/9/20).

66. European Research on the Internet of Things, IoT Governance, Privacy and Security Issues, January 2015, http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf (link as of 7/9/20).

67. World Economic Forum, Accelerating the Impact of Industrial IoT in Small and MediumSized Enterprises: A Protocol for Action, 2020, https://www.weforum.org/projects/accelerating-the-impact-of-iot-technologies (link as of 7/9/20).

68. Danish Agency for Data Supply and Efficiency, Large Increase in the Value of the Free Geographical Basic Data, 21 March 2017, https://sdfe.dk/data-skaber-vaerdi/nyheder/nyhedsarkiv/2017/mar/stor-stigning-i-vaerdien-af-de-frie-geografiske-grunddata/ (link as of 7/9/20).

69. Contiki-NG operating system, https://www.contiki-ng.org/ (link as of 7/9/20).

70. RIOT operating system, https://riot-os.org (link as of 7/9/20).

71. TinyOS operating system, http://www.tinyos.net/ (link as of 7/9/20).

72. OpenWSN, https://openwsn.atlassian.net/wiki/spaces/OW/overview (link as of 7/9/20).

73. Industrial Internet Consortium, Influencing Standards, 17 July 2016, https://www.iiconsortium.org/accelerating-innovation.htm (link as of 7/9/20).

74. OneM2M, http://www.onem2m.org/ (link as of 7/9/20).

75. Alljoyn, https://openconnectivity.org/technology/reference-implementation/alljoyn/ (link as of 12/9/20).

76. IoTivity, https://iotivity.org/ (link as of 7/9/20).

77. OMA Specworks, Lightweight M2M (LWM2M), https://omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/ (link as of 7/9/20).

78. Chinese Electronics Standardization Institute, Industrial IoT Interoperability White Paper http://www.cesi.cn/images/editor/20180917/20180917165307623.pdf (link as of 7/9/20).

79. Sophia Antipolis, ETSI CIM Group Releases Full-Feature Specification for Context Information Exchange in Smart Cities, ETSI, January 2019, https://www.etsi.org/newsroom/press-releases/1519-2019-01-etsi-cim-group-releases-full-feature-specification-for-context-information-exchange-in-smart-cities (link as of 7/9/20).

80. European Union Agency for Cyber Security, Baseline Security Recommendations for IoT, November 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (link as of 7/9/20).

81. Brazil PL. 7.656/17.

82. Lee Raine and Janna Anderson, The Internet of Things Connectivity Binge: What are the Implications? Pew Research Center, 6 June 2017, https://www.pewresearch.org/internet/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/ (link as of 7/9/20).

83. Victoria Escudero, The IoT in Latin America: Prospects and Challenges, CoMarch, August 2018, https://www.comarch.com/telecommunications/blog/the-iot-in-latin-america-prospects-and-challenges/ (link as of 7/9/20).

84. Internet World Stats, Internet Users Statistics for Africa, March 2020, https://www.internetworldstats.com/stats1.htm (link as of 7/9/20).

Endnotes

85. PwC, 2019 IoT Survey: Speed Operations, Strengthen Relationships and Drive What's Next, 2019, https://www.pwc.com/us/iotpov (link as of 7/9/20).

86. Harrison Jacobs, Chinese People Don't Care About Privacy on the Internet – Here's Why, According to a Top Professor in China, Business Insider, Jun 2018, https://www.businessinsider.com/why-china-chinese-people-dont-care-about-privacy-2018-6 (link as of 7/9/20).

87. Pablo Urbiola et al., Data Flows Across Borders: Overcoming Data Localization Restrictions, Institute of International Finance, March 2019, https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf (link as of 7/9/20).

88. Shinzo Abe, Prime Minister of Japan, Office of the Prime Minister of Japan, Davos Speech, 23 January 2019, https://www.weforum.org/agenda/2019/01/abe-speech-transcript/ (link as of 7/9/20).

89. Nik DeCosta-Klipa, Cambridge Becomes the Largest Massachusetts City to Ban Facial Recognition, Boston.com, 14 January 2020, https://www.boston.com/news/local-News/2020/01/14/cambridge-facial-recognition (link as of 7/9/20).

90. PwC, PwC Publishes Results of Global Survey on Technology, Jobs And Skills, September 2019, https://www.pwc.com/gx/en/news-room/press-releases/2019/global-skills-survey-2019.html (link as of 7/9/20).

91. Pablo Illanes, et al., Retraining and Reskilling Workers in the Age of Automation, McKinsey, January 2018, https://www.mckinsey.com/featured-insights/future-of-work/retraining-and-reskilling-workers-in-the-age-of-automation (link as of 7/9/20).

92. Michael Stead et al., The Little Book of Sustainability for the Internet of Things, PETRAS, 2019, https://s3-eu-west-1.amazonaws.com/uclpetras/wp-content/uploads/2019/10/28145726/Little_Book_of_Sustainability.pdf (link as of 7/9/20).

93. World Economic Forum, A New Circular Vision for Electronics: Time for a Global Reboot, 2 April 2020, http://www3.weforum.org/docs/WEF_A_New_Circular_Vision_for_Electronics.pdf (link as of 7/9/20).

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