5 Key Technologies That Are Driving IoT Development

Sophie Ross

21 November, 2018

The Internet of Things (IoT), under the influence of several exclusive technologies, is on the verge of booming into the next major technological wave.

It's potential to redefine our lives is simply unexplainable. For instance, heart patients continuously need to visit their cardiologist so they can record their heart rate and perform

It's potential to redefine our lives is simply unexplainable. For instance, heart patients continuously need to visit their cardiologist so they can record their heart rate and perform related tests. However, with IoT, these patients can quickly provide their physician with hourly updates even without needing to make a trip to the clinic. They can wear an IoT-connected heart monitor that allows their physician to assess the information periodically and suggest the right course of treatment.

For such to happen and for IoT to assume its position as a potent force, it needs support from various technological developments. What these technologies need to do primarily is not to necessarily support the IoT, but instead as they advance, they are subsequently going to massively boost IoT innovation as a whole.

Herein are five different technologies that are driving the development of IoT.

Cloud Computing

IoT is set to produce a significant data volume, and as such, you will need some considerable space to not only process but also store this data, and this is where Cloud computing comes into play.

Cloud computing is the only technology that boasts the potential to quickly and faultlessly process such a significant volume of data. For instance, where numerous smart devices transmit crucial health data to physicians from across the globe, enormous data volumes are produced. Unsurprisingly, only the cloud can process such masses of data effectively.

Several significant developments in innovation have rendered cloud computing

Marketing Automation

The main proponents of a majority of the activities which are contributing to the rise of IoT as a dominant force are of course multinational tech giants who want to gain commercially.

IoT has the potential to offer a substantial volume of information on customers, such as their hobbies, preferences or even what devices they use. International companies can find such data more than valuable as it can help them customise and sell their products and services to fit their market. IoT can also effectively help such firms to generate customer-focused items.

Currently, software developers are working to produce marketing automation software which can automate marketing procedures such as customer segmentation, integration

App Technology Boom

App technology is yet another critical component in the development of IoT solutions. The recent emergence of app innovation has drastically been scaling up the rate at which IoT is developing.

Generally, apps allow data exchange between various devices. In essence, they offer virtually everything that IoT offers. Apps have been vital for the development of IoT, and their relevance can best be captured through several examples including:

- Parking apps that can check all available parking spaces within a city.
- Noise monitoring apps that identify certain sound decibels in otherwise sensitive areas like hospitals and schools.
- Structural assessment apps, which can

IPv6

IoT will facilitate for the interconnection of millions of devices. Undoubtedly, all these devices will need IP addresses. IPv4, which is currently the most popularly used internet protocol, cannot cope with the subsequent demand surge for IP addresses. Furthermore, IPv4 has particular concerns that can hinder the progress of IoT, as can other security threats. IPv4 is not the most secure internet protocol, and considering the volume of confidential data that will be shared through IoT, it can be a risky option.

But with IPv6, which is IPv4's newer successor protocol, all these concerns are adequately addressed. Besides this, it also comes with multiple added benefits including the fact that to address a device, it offers four times more bits on the internet. With these extra bits, you can enjoy about 3.4×1038 address

Sensors

Several factors make IoT outstanding, and one of such is inter-device interaction notwithstanding their technological affiliations. Sensors which are fitted in these devices allow them to interact with multiple devices smoothly and effortlessly.

Sensors are among the core components of IoT. For instance, to unlock your main door, the key's sensor can open it, which instantly transmits a message for your lights to switch on and your thermostats to regulate the temperature in the house. All these activities happen simultaneously.

The science behind IoT sensor design is similar to how microprocessors work. They use the lithography procedure that ensures that various sensor copies are rolled out concurrently. However, IoT can only perform a

5 key drivers of IoT for Smart Buildings

Articles • April 27, 2020

Facility management is undergoing a complete transformation, as smart facilities and IoT technologies continue to evolve. Buildings are becoming streamlined operational ecosystems capable of collecting more actionable data, being more environmentally friendly, and significantly increasing resource efficiencies.

More efficiency with smart facilities

Haltian has operated with smart offices and smart washrooms for years now. These solutions are greatly enhancing the customer experience within the facilities while also increasing efficiency, hence lowering the operational costs. Smart offices are using space more effectively, while washrooms are becoming more digitized to include paper towel and trash bin fill levels, liquid soap refill optimizations and on-demand cleaning.

Smart buildings help you in

The achievements of smart offices and washrooms are also illustrations of the fact that whatever the data related problem you're experiencing in your facility, there is IoT sensor technology out there that can help.

You may wonder why this means:

This may mean tracking the amount of traffic in the building, the number of people in the meeting rooms, free workspaces, facility air quality, and temperature. This can be achieved by the installation of wireless IoT sensors. One thing is certain, smart facilities are the future.

Based on our years of experience with our facility customers, here are five key drivers setting the momentum of IoT and smart facilities:

- Scalability
- Easy installation and maintenance
- Reliability
- IoT security
- Integration

1. Scalability, the practical driver

The first key driver is perhaps not the most exciting, but probably the most practical: scalability. Creating a small proof of concept using widely available DIY (Do It Yourself) IoT kits is relatively easy, but **when you need to scale the implementation to thousands or hundreds of thousands of sensors, things get a little more complicated.**

A well designed IoT solution ensures that your solution is easy and fast to scale, secure, easy to use, and of course, cost-efficient.

The challenges with scalability are not only about adding more devices but also about maintaining them. Consider what it takes to keep the IoT devices on several locations operating effectively: monitoring their battery levels and replacing batteries, ensuring consistent and strong connectivity, dealing with each sensor's reporting intervals, as well as r

What is Massive IoT?

Massive IoT sets some requirements for the technologies used. For this article, we partnered with Wirepas to go through the meaning and implications of massive scale IoT.

LEARN MORE →

2. Easiness of installation and maintenance

Easy installation and scale are paramount for smart facilities. A wonderful instant benefit of IoT is that its hardware, including sensors and gateways, are easy to install and user-friendly for the technicians. For example, wireless sensor installation should be as easy as mounting the sensor to walls, ceilings, under tables, etc. in a matter of seconds and validatir

3. Reliability

Buildings are built to last, and that's how the design for sensors and gateways should be approached as well. Batteries in sensors last for several years, therefore requiring very little maintenance. Once installed, the sensor maintenance should be minimal.

As the installed sensor base scales, the less you need to worry about their connectivity, battery levels and signal strengths, the more time you have analyzing the data they give.

Reliable maintenance makes sure that the dataflow is constant, all the devices are in operation and where they should be, and that nothing comes in the way of getting the most out of IoT in your smart facilities solution.

4. IoT Security

The quality of security is one of the major key drivers of any type of development, and IoT data collection platforr

4. IoT Security

The quality of security is one of the major key drivers of any type of development, and IoT data collection platforms are designed with privacy and security in mind. End-to-end security is employed from the sensors to the cloud application in terms of software, and from the factory to the location with no unknown software layers. Comprehensive security allows for protected integration to your cloud platform and ensures the continuity of its transmission.

We at Haltian are overseeing security all the way from the manufacturing, where customer-specific encryption keys are installed in the software ensuring data integrity. We don’t use any unknown software layers and interfaces.

Our cloud partner for sensor operations is Amazon Web Services which means that our solution has gone through a thorough validation process and is tested regularly.

5. Easily integrated IoT ecosystem

IoT ecosystem and value chains are rather long and complex, hence implementing that IoT solutions require various layers to talk to each other. A system that can deliver a cost-effective data collection solution for smart facilities with full integration to any cloud-based application is a massive forward driver.

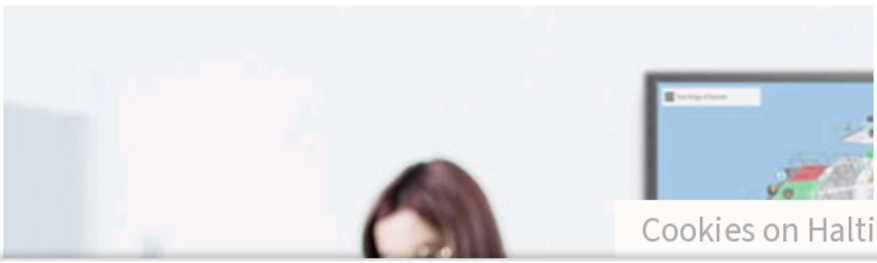
Haltian's Thingsee solution includes various sensors, gateways, cellular connectivity and software for device cloud. Our customers can have an IoT platform or cloud-based solution from another vendor, to which we integrate easily. The beauty of running a cloud-based solution is the ease of integration!

Connecting people, places and

Connecting people, places and processes

IoT and its capabilities will ensure a new and better understanding of buildings, facilities and people in the future. This will influence many areas and force new approaches to maintenance and design. IoT not only creates new business opportunities but results in more productive spaces and higher energy efficiency. It should not be overlooked that the efficient monitoring of different conditions will increase the life cycles of facilities for several years.

Changes are coming so ensure your buildings and facilities are ready for the opportunities provided by the Internet of Things!



IoT technologies as a driver for business model innovation and digital transformation in industrial companies

Published on Jan 23, 2022

Wim Vanhaverbeke
Professor digital strategy and innovation @...
Published Jan 23, 2022

You may know several companies that excel in developing technological innovations as a base to improve their products and secure their competitive advantage. As IoT technologies make data ubiquitous and data sharing super-easy, those companies usually face a major challenge as the main driver for competitive advantage is no longer advances in product technology but IoT enabled services which

1. **The benefits of a gradual digitalization process**

· The company developed its digitalization skills gradually as a supporting function for the prevailing business model – they developed free digital services to support premium priced products. In other words, digitalization was generating value from the start and business units were eager to integrate them as part of their sales strategy. Many firms, in contrast, start digitalization as a (corporate) transformation project that doesn't address the needs of its businesses and consequently doesn't receive internal support.

· The gradual development of IoT services backing the businesses led automatically to new insights about the potential of the technology and fueled the discussion about the need for new business and revenue models.

2. What type of revenue model to choose?

· The awareness that the company's business model had to change was growing as the IoT applications became more advanced. However, this awareness was unequally distributed in the company: the digital service development team was well aware of the potential while sales and marketing managers in the business were still clinging to the existing business model. This divergence in view is typical for companies that move fast to apply IoT technologies, and it is one of the major challenges during digital transformation processes.

· IoT enabled business models imply not only new revenue models, but also the transition from one to the other business and revenue model. As the company was progressing steadily with more audacious IoT enabled business models, it set up a

3. **Revenue models can't change without digital transformation**

· The switch to new IoT enabled business models can only be implemented successfully if companies are establishing a digital culture. The divide between the digital savvy people in the company's digital services team on the one hand and the businesses on the other hand can only be bridged through corporate wide initiatives that lead to the digital transformation of the organization and the culture. Sales is an excellent example: sales were still organized around selling products while digital services require a service oriented sales process in which technical knowledge is essential to offer value propositions to customers. Salespeople need to be technically skilled and they have to work together with technical people to understand, pitch and deliver new digital services to customers.

4. **From closed to open transformation**

· The company has been developing the digitalization process internally. Other companies that go through a digital transformation process tend to rely on partners to speed up and secure the transition. Reliance on external resources and competencies is necessary to succeed in a digital transformation journey: Collaboration with universities and research labs to find advanced solutions and skilled people; working with complementors and suppliers to offer joint solutions; participating in explorative R&D and innovation projects to explore the potential of digital applications integrating data across the supply chain; partnering with customers as lead users to get an in-depth understanding of their latent needs and aspirations.

6 Important IoT Trends For 2023-2025

by Josh Howarth
September 8, 2023

You may also like:

- 8 Huge Cybersecurity Trends
- 20 Skyrocketing Data Storage Startups
- 23 Fascinating Remote Work Statistics

There are currently well over 13 billion Internet of Things (IoT) devices installed throughout the world.

That number is expected to rise to over 30 billion by 2025.

The economic impact of this technology is even more impressive. Deloitte predicted that by the end of 2023, global spending on IoT initiatives would exceed $1 trillion.

To learn about the most important trends impacting the IoT space in 2023, read on.

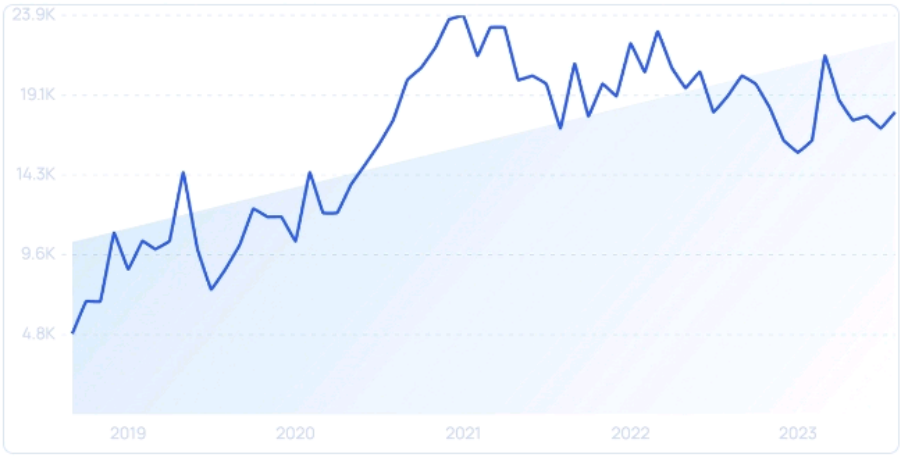
1. IoT Data Feeds AI Models

1. IoT Data Feeds AI Models

Artificial intelligence (AI) and the IoT are natural complements to one another.

And when combined, they allow for insights that were almost unimaginable before.

This combination is known as AIoT.



Searches for "AIoT" have increased by 275% in 5 years.

Back in 2019, Gartner found that only about 10% of IoT projects were utilizing AI to develop insights.

But as the IoT installed base grows, it's inevitable that AI will help parse the reams of data that are collected via IoT devices. And the data will be essential in "training" AI systems.

By 2025, it is expected that IoT devices will generate roughly 73.1 ZB of data.

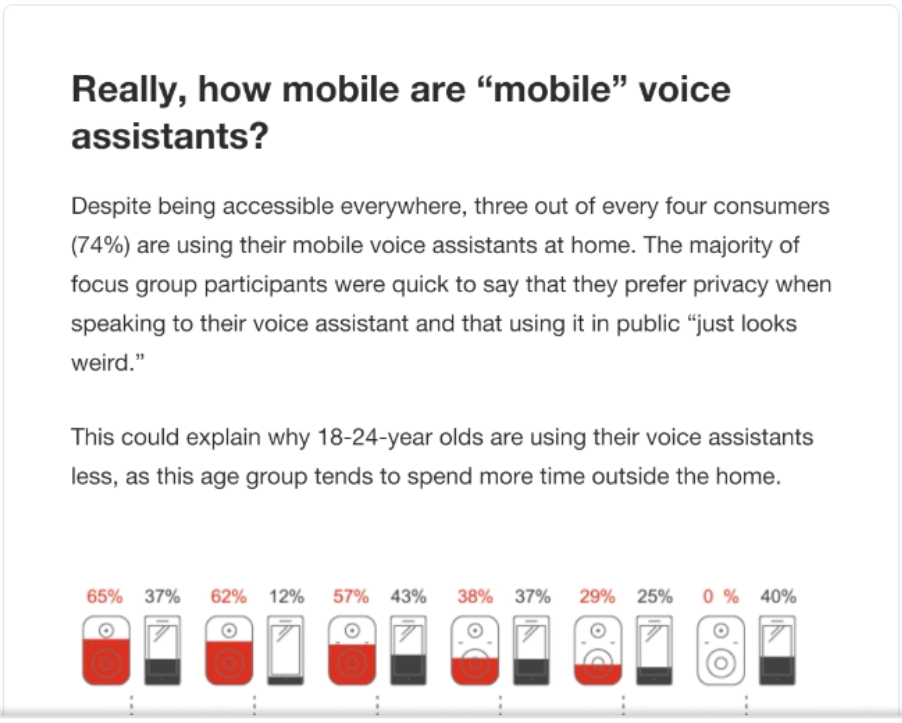
That's roughly 4x the 18.3 ZB generated in 2019.

With all this data, the use of AI and machine learning will be essential.

Because of this, Gartner predicted that over 80% of IoT initiatives would be paired with AI by the end of 2022.

For instance, Voice AI and Vision AI at scale seem to be impossible without the help of the IoT.

Approximately 74% of consumers between 18-24 report using a mobile phone voice assistant in their home.

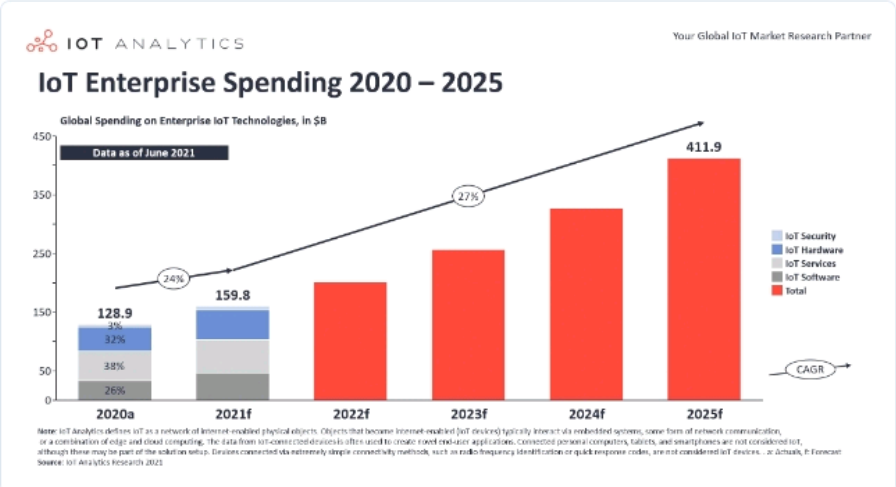


2. IoT Platforms Look To Improve Functionality

With the complicated nature of IoT data collection and analysis, it's inevitable that applications will come along to help inexperienced businesses cope.

For instance, spending on IoT software grew by over 24% in 2021.

While spending on the actual hardware only grew by around 5%.



While IoT hardware still comprises about 32% of overall spend, IoT software spend is rapidly catching up at 26%.

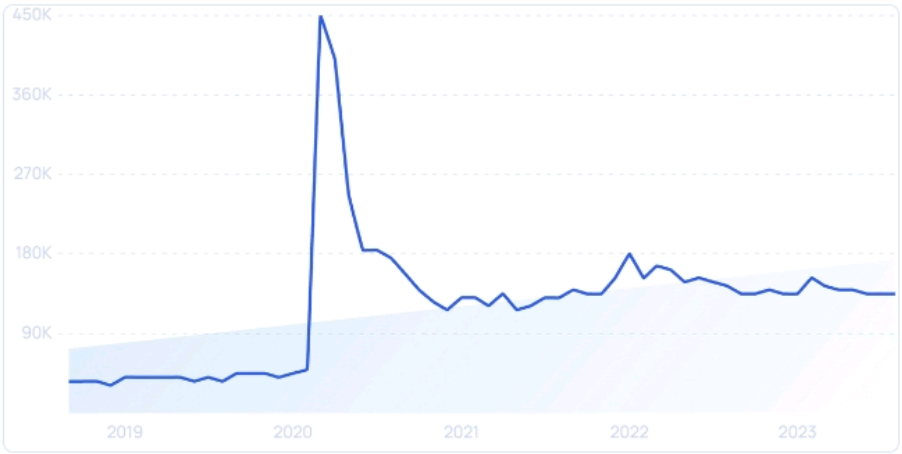
It's obvious that the most important changes are taking place in the software ecosystem that supports IoT.

3. IoT Connects Healthcare To Patient Needs

COVID-19 lockdowns changed the way healthcare was delivered in the US.

Before 2020, there were around 36 million estimated virtual health visits a year.

This number quickly jumped after the beginning of COVID, with some experts estimating around 1 billion telehealth visits in 2020.

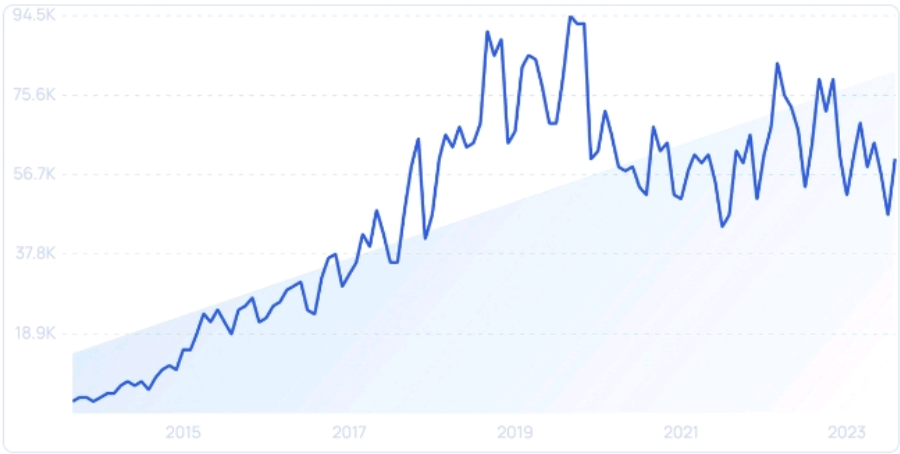


Searches for "Telehealth" have spiked. But are still well above pre-pandemic levels.

McKinsey has found that telehealth visits to doctors' offices and outpatient facilities have stabilized at roughly 38x higher than it was pre-pandemic.

4. Industry 4.0 Increasingly Relies On IoT

Industry 4.0 (or the Fourth Industrial Revolution) is a term that refers to vast improvements in manufacturing and industry brought about by widespread automation and increased efficiency.



Searches for "Industry 4.0" have increased by around 2,000% over the last decade.

A major component of this concept is IoT. Without IoT, the large-scale data collection and monitoring required to improve industrial capacity would be impossible.

And of the four major components of Industry 4.0 (IoT, AI, cloud infrastructure, and big data/analytics), Statista reports that industrial organizations find that IoT is the most important (72% of them said so in a study).

5. Cybersecurity And Data Privacy Are Very Serious Concerns

Because IoT could be so integral to the infrastructure of a country or the health of its citizens, it is also subject to serious cybersecurity threats.

Palo Alto Networks found that a concerning 57% of IoT devices are susceptible to attacks by malicious actors.

Even more worrying, the same report found that a whopping 83% of medical imaging devices are running on unsupported operating systems. This leaves their entire network vulnerable to attack.

This is even more serious when you consider that over half of all hacking threats to healthcare providers involve imaging devices.

This is where a company like SentinelOne comes in.

6. IoT Transforms The Global Supply Chain

Global supply chains have become increasingly complex and interdependent.

This has allowed for amazing improvements in transportation and delivery. But it has brought headaches as well.

For instance, in the past manufacturers and logistics companies may have been aware that certain product components had left a port or were en route to a certain country.

But they had no way to track every piece of this complex supply chain.

With IoT, this is no longer a problem.

Every shipment can be tracked and monitored. And mistakes can be caught as soon as they happen.

It's no wonder then that 70% of retailers are attempting to make their supply chains IoT-complaint.

International courier company, DHL, is already taking matters into its own hands.

Conclusion

That's all for the top IoT trends of 2023.

Overall, IoT is rapidly changing many parts of the manufacturing supply chain as well as industries you may not expect (like the medical field.)

However, to expand at the pace many expect, the IoT industry will have to overcome serious cybersecurity and data privacy concerns.

IoT governance, privacy go hand in hand

Specific forms of governance include informational, financial, medical, legal, risk management and regulatory. IoT governance, specifically, **focuses on IoT devices and applications**. IoT data governance emphasizes data and data assets as crucial elements in IoT devices. 10-Jan-2023

https://www.techtarget.com › tip

[Explore the relationship between IoT governance and privacy - TechTarget]

About featured snippets Feedback

People also ask

What are the overview of governance regarding IoT?

What is the overview of IoT devices?

standards and regulations, as well as technologies like AI and fog computing, will shape the IoT governance landscape.

IoT governance, privacy go hand in hand

In general, *governance* refers to the rules, controls, regulations and policies that direct the operation of an organization. Specific forms of governance include informational, financial, medical, legal, risk management and regulatory. IoT governance, specifically, focuses on IoT devices and applications. IoT data governance emphasizes data and data assets as crucial elements in IoT devices.

It is imperative that organizations apply governance to IoT devices, applications and data, but just as importantly, governance is needed to regulate IoT user privacy. For example, governance is essential for IoT medical devices to sustain human life, while privacy is needed to protect a patient's data, categorized as protected health information. Enterprise leaders and admins must understand the significance of IoT data privacy to protect their strategic operations.

Continuity, consistency and cooperation underpin IoT governance. Without these factors, poor data governance can hamper regulatory compliance, as well as adherence

Standards and laws related to IoT governance

Various standards bodies promulgate, develop and coordinate technical standards to ensure the safety of IoT device users.

Standards bodies discovered a need for IoT governance based on the lack of data privacy in IoT applications. Additionally, governance regulations are embedded in longstanding security and privacy rules. For instance, NIST developed the Federal Information Processing Standards related to computer security and the processing of censored data. Further, NIST Internal Report 8295 is focused on setting standards for mobile radio operators over broadband for the purpose of data sharing with 911 dispatchers and first responders.

Other standards groups and/or regulations that apply to IoT devices include Internet Engineering Task Force, Regional Internet Registry, information security operations center, IEEE, HIPAA and GDPR.

Enterprises with IoT deployments must be familiar with these standards and regulations. More importantly, they must understand the role data governance plays in compliance with them. In particular, organizations should

What's next for IoT governance

Looking ahead, there's likely to be a growing emphasis on how the government can protect IoT data.

Expect new regulations related to IoT privacy for devices, data, consumers and the industry as a whole. Some U.S. states have already developed IoT security legislation. Expect more states to follow suit, especially as consumers demand privacy laws. In addition, there will be growing demand for IoT devices and storage systems with embedded privacy and security technologies. The secure storage of personal data will be of key importance.

Further, AI and machine learning will play an increasing role in IoT. Telemetry will become essential, as organizations automate the recording and transmission of data from remote sources.

Lastly, with the proliferation of IoT devices and human connectedness to multiple remote services, fog computing will only increase and accompany cloud computing. Simultaneously, edge computing will become more essential to process time-sensitive data in businesses and government organizations.