www.pipelinepub.com
Volume 19, Issue 4

Looking Ahead to IoT Trends for 2023

By: Ken Figueredo

Within the Internet of things (IoT) market in its broadest sense, the pendulum of attention veered toward the consumer sector over the course of 2022. The impetus of behind-the-scenes initiatives make this an obvious area to focus on in predicting 2023 market dynamics.

In addition to momentum effects, however, other developments will shape future market dynamics. These include market shocks, such as the global pandemic, that trigger and accelerate new developments. Fresh ideas from new entrants disrupt conventional thinking, leading to changes in user expectations, which represents another avenue to predict future trends.

In parsing the 2023 prospects for the IoT sector, it also makes sense to look beyond near-term triggers. The gradual impact of structural changes will resonate through the industry over a period of several years. That makes it imperative for industry participants to think in terms of a roadmap for IoT and to plan beyond 2023.

The swing to consumer IoT

On the commercial front, large vendors such as Apple, Amazon, Google, and IKEA are backing the Matter connectivity protocol, an initiative of the Connectivity Standard's Alliance. Their collective aim is to revive interest in the connected home market. They recognize that growing numbers of consumers want to monitor their homes and possessions via apps and connected home-gateways.

Consumers' initial focus on convenience and security will evolve and expand over time. Over the coming winter and spring months, price inflation and energy usage efficiency considerations will result in homeowners seeking better insights into their utility costs and consumption patterns.

Large vendors recognize that a highly fragmented market for smart devices depends on interoperability. In turn, this requires industry coordination and standardization. Expect to see smaller firms and niche hardware suppliers jumping on the Matter bandwagon to increase the range and choice of smart home devices available to builders, property managers, and homeowners. There will also be market-entry and competition for smart home services as providers explore ways to become the trusted provider for portfolios of smart home services.

Regulatory angle on consumer IoT

The private sector is not alone in taking action to develop the consumer IoT sector. Associations representing consumers and regulators are voicing the need to prepare for increasing numbers of consumer devices in the home. Notably, they are drawing attention to privacy, safety, and security concerns. This is because it is not unusual for consumer IoT devices to use weak passwords or to lack mechanisms to patch software flaws. Currently, too many connected devices contain security vulnerabilities that would open the door to hacking and malicious attacks. At present, consumers and hardware providers tolerate a market of inexpensive devices that perform a basic function. They also do not care overly much about security. This is problematic for the future as IoT increasingly seeps into the infrastructure that enables everyday living.

In 2023, two regulatory initiatives will drive industry change. One of these involves the US, where the government is taking action over cybersecurity concerns by introducing a labeling program for consumer IoT devices. The scheme bears similarities to the "Energy Star" rating system and aims to educate consumers about the risks associated with routers, smart speakers, connected door locks, and security cameras. Researchers at Carnegie Mellon University have already canvassed industry views on a smart devices security and privacy label to help consumers make informed purchasing choices and to encourage manufacturers to disclose their privacy and security practices.

The second initiative relates to the European Union (EU), where there are plans to enact the Cyber Resilience Act. The Act will require smart devices manufacturers to follow strict cybersecurity rules. Manufacturers would need to review their products' risk profiles and fix any discovered vulnerabilities. They would need to notify the authorities within 24 hours if a problem or threat were uncovered. Failure to abide by the provisions could trigger fines as high as €15 million or 2.5 percent of global turnover and, potentially, a ban on sales.

The combination of commercial interests and regulations carrying material financial penalties will shape the consumer IoT market from 2023 onwards. The effects are likely to spill over from the smart home sector and into the wellness arena, for example, once consumers pay attention to the data and recommendations their wearables generate. As with payments and General Data Protection Regulation (GDPR) privacy regulations, expect new regulatory measures in one geography to also have cross-border effects.

A wake-up call for enterprise IoT

While consumer IoT might be the immediate focus for industry watchers, organizations planning to adopt and evolve their IoT systems should remain attentive to industrial sector developments. Perhaps the biggest surprise of 2022 was Google's quiet pull back from offering its IoT platform services. In basic terms, IoT platforms contain a toolkit of software functions that help providers to deploy and maintain their IoT systems. Device management is one such function that is required in every IoT system. Other highly reusable functions include location tracking, security, and configurable policies to manage access control for privacy and selective data-sharing purposes. Because developers use them repeatedly to build, deploy, and support IoT systems, they are often labeled common service functions (CSFs).

In the aftermath of Google's announcement, smaller providers raced to help organizations migrate their IoT solutions to other platforms. These efforts will succeed to the degree that users understand what risks they are taking. For example, what happens if their new provider is acquired? Might their provider go out of business? What guarantee is there that their provider will not pivot to a different value proposition? These are real considerations when viewed in the light of Google's financial might

not being enough to carve out a viable stake or commit to a long-term presence in the growing IoT sector.

During 2023, expect adopters and strategic users of IoT to be much more hard-nosed about the survivability of their providers. This includes risk-management considerations about providers' technology roadmaps and migration capabilities, both for individual deployments and their associated data.

IoT evolution and innovation expectations

The early challenges in the IoT market tackled issues of wide-area and mobile connectivity. Through industry ecosystem efforts, a string of developments simplified adoption. By focusing on scale economies, they also improved affordability. As the IoT sector has matured, organizations are beginning to identify new requirements that build on top of a foundation of ubiquitous connectivity.

One of these new requirements takes a systems view to IoT. It projects a future where individual IoT solutions are elements in larger and cooperative IoT systems. Take the examples of a smart city or an intelligent transport system—in both situations, there is value in cross-connecting applications. An example involves sharing IoT data and coordinating activities between three IoT systems: for private vehicles, for public transport networks, and for municipal fleets. IoT-data sharing could improve traffic management and improve emergency responsiveness. Then, there are environmental-quality application opportunities that leverage dynamic street lighting systems and pollution monitoring sub-systems. The systems view is essential for cross-silo and federated systems.

This leads to a second set of requirements for new, common service functions. These encompass common data models to enable semantic data sharing between different users and organizations. Another emerging requirement is for reusable AI tools based on standardized techniques for building AI into IoT systems.

These are two examples of how IoT requirements are evolving. They are also structural drivers that will shape how IoT-platform and service providers organize their solution roadmaps. Over 2023, expect to see a shift beyond connectivity into the realms of services that improve the ease of data sharing, both technically and commercially.

Alignment with external influences

The IoT industry does not exist in isolation, so it should come as no surprise to see its future being shaped by external factors. Sustainability is one factor whose role will continue to grow in 2023. For evidence of this, look no further than the stream of studies and research reports emanating from IoT industry analysts whose views mirror industry preoccupations. Beyond addressing the role of IoT in enabling sustainability, expect to see technology providers designing capabilities to make IoT itself sustainable. This will involve many small improvements to improve the carbon footprint of power-and processor-constrained devices.

Augmented reality and metaverse concepts are another external development that will affect the IoT sector in 2023. There is a close connection because the delivery of metaverse experiences relies on IoT sensors and the application of IoT data to create digital twins of the objects being studied. In the educational sector; this might mean that biology students would allow students to "walk" around a digitally rendered and interactive version of a plant. Eventually, novel interfaces and IoT sensors will support touch and smell sensations. There are parallels in the industrial context where technicians can practice repairs in a virtual setting or remotely intervene on machinery. While these possibilities will take years to materialize, expect to see investments and experiments during 2023.