Letter from the Editor

By: [Scott St. John](#)

To say the proliferation of the Internet of Things (IoT) has been impressive, would be an enormous understatement. In fact, there are [more mobile-connected devices than humans](#) on the planet right now. Whether it's the smartphone in your pocket, your smartwatch or fitness device on your wrist, car, gaming console, connected doorbell, vacuum cleaner, or smart appliances. Or your work laptop, the connected device you use in the field, or the connected camera you use to livestream as you surf gnarly waves. The IoT touches nearly every aspect of our increasingly connected lives today, and this is just the beginning.

You can pick your favorite projection, of which there are many, but I think we can all agree the [IoT market is projected to be in the hundreds of billions of dollars](#) in just the next few years. I expect that to grow rapidly and by multiples, as more connected devices come online – such as AR/VR – with the advent and adoption of the metaverse. In the very near future there won't be an aspect of your life not impacted in some way by the IoT, down to the food you eat and water you drink.

But the rush to make the IoT a reality has had some monumental oversights. Gaps in security have led to breaches of national security and the shutdown of critical infrastructure. And that's only a sign of the risks that *were*; as risk of quantum-level IoT cybersecurity attacks are emerging *now*, even as you read this article.

The sheer scale of the IoT is staggering and beyond human performance capabilities. Even if people were a viable solution, the cost would make it prohibitive and human error would make it impractical. To efficiently and securely seize the IoT opportunity, many things are still needed including better standardization, sophisticated automation technologies, and state-of-the-art, proactive cybersecurity. Which is why this issue of *Pipeline* is so important.

In this issue of *Pipeline*, we explore the key aspects of the rapidly expanding IoT. In a special feature, we talk to Total Network Services and explore how [AI, blockchain, NFTs, RPA, and UCID are being used to secure mobile, connected devices](), improve CX, and transform the federal government. Telstra explains how satellite and communications service providers can collaborate to capitalize upon the opportunities resulting from [the New Space Race](). Blue-White Robotics shows us how the IoT is being used for smart agriculture, with [robot-as-a-service for self-driving tractors](); and Everline shares their unique perspective on how [IoT is being used to preserve one of our most precious natural resources](), water. Aptilo demonstrates how [private APNs can be reinvented to streamline the management of IoT]() connectivity and devices, and Everynet shows us how LoRaWAN is becoming [the backbone for massive IoT]() deployments. OneM2M discusses the development of open IoT standards to create [intelligent IoT systems]() and The Trusted Computing Group shows us how to create proactive [cyber resilience to secure the future of IoT](). FirstPoint Mobile Guard explores [the latest threats to enterprise cellular IoT](), and Webbing demonstrates how to [secure IoT connectivity]() and connected devices with the use of eSIMs. All this plus the latest [telecom and technology industry news]() and [more]().

We hope you enjoy this and every issue of *Pipeline*,

Scott St. John
Managing Editor
Pipeline
[Follow on Twitter]() | [Follow on LinkedIn]() | [Follow *Pipeline*]()