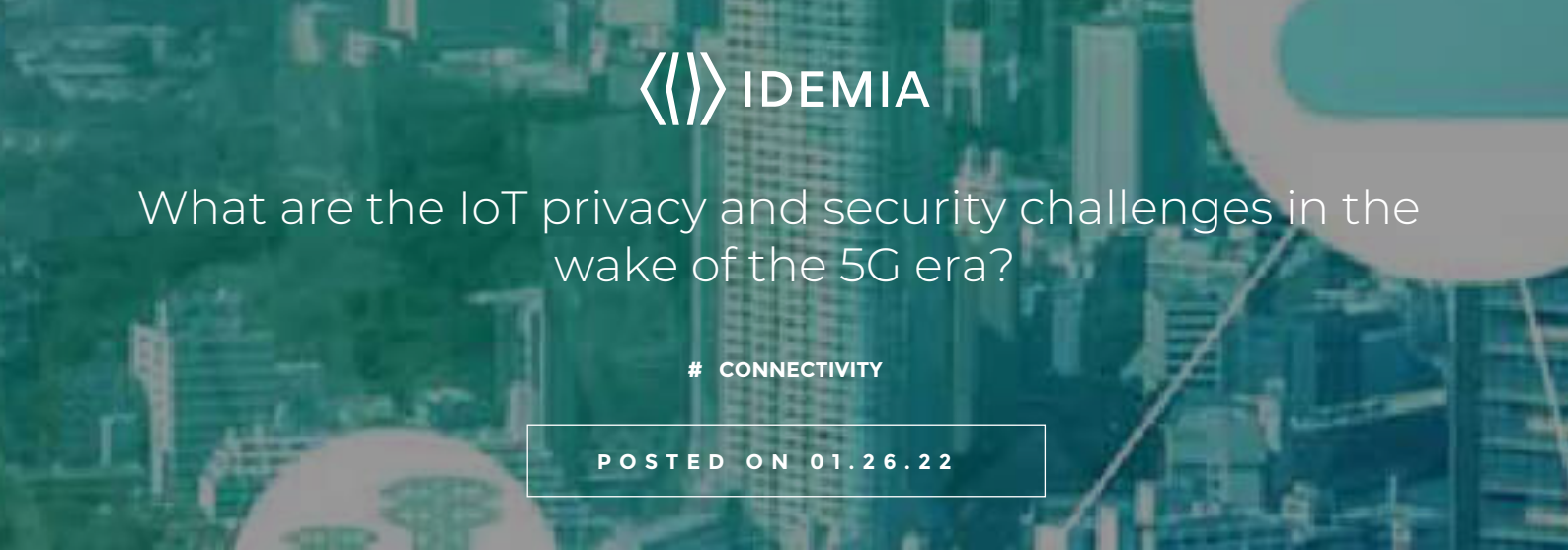

What are the IoT privacy and security challenges in the wake of the 5G era?

CONNECTIVITY

POSTED ON 01.26.22

The high speed, low latency and extreme stability of 5G connectivity are redefining what is possible in the connected world while also generating an unprecedented IoT boom. As billions of IoT devices begin to capture, store and transmit sensitive information, user expectations for increased efficiency and effectiveness not only apply to connectivity, but to data protection as well. New IoT privacy and security concerns arise for consumer and industrial devices alike.

The IoT privacy and security challenge in a fragmented ecosystem

Mobile devices were originally introduced to the market by a handful of OEMs (namely handset makers); however, the sheer **quantity of IoT devices flooding the market** today ushers in thousands of new OEM players. The manufacturers in this very fragmented market often have limited expertise around security and privacy issues and are less engaged in mobile standardization than their handset maker counterparts. **Beyond mobile handsets, user privacy concerns also extend to consumer IoT devices** that collect extremely sensitive information, such as wearables (smart watches, health monitoring devices, fitness trackers), connected cars, and smart home gadgets.

The variety and number of devices in the IoT ecosystem creates a huge challenge in terms of implementing IoT privacy and security measures. One key step in protecting end-user privacy is **encrypting the IMSI**, a unique identifier for each subscription. However, the lack of device interoperability makes device-based IMSI encryption very difficult, if not impossible. In the IoT ecosystem, the SIM (or its embedded cousin, the eSIM)—a standardized and secure vault—turns out to be the only realistic option for IMSI encryption. When executed properly, this new privacy and security feature—introduced along with 5G standardization—**protects connected device users from being tracked, as well as against other forms of privacy invasion**.

Protecting industrial IoT devices

In the industrial space, IoT devices are quickly becoming **key components in critical infrastructures** and transmit sensitive data—creating a more complex set of security challenges. Soon, the industry will **need to secure applications running on billions of IoT devices**—from smart meters to robots to various types of critical communication equipment. Here, the complexity lies in the fact that these devices are not secure by design.

Even more than in the consumer segment, the industrial IoT ecosystem is extremely fragmented. To overcome that challenge, the GSMA recommends a **market-endorsed solution called IoT SAFE** (IoT SIM Applet For Secure End-2-End Communication). Rather than using proprietary device hardware, the purpose of IoT SAFE is to rely on the standardized SIM to enable interoperability and protect all data communications from being intercepted or altered. More precisely, the principle of IoT SAFE is to rely on the SIM (or eSIM) to secure the app layer, and thus protect IoT device applications as well as the associated data transmitted to the cloud. As 5G transforms connectivity and paves the way for new IoT

opportunities, the SIM, more than ever, will play an essential role in addressing growing IoT privacy and security challenges.