IoT Device Security:
Upcoming Rules and Regulations

WHITEPAPER

aeris

AT A GLANCE:

Customers whose IoT programs collect any personally identifiable data should keep a sharp eye on legal developments, state-wide, nationally, and globally, and keep security top of mind in designing and operating their products and services. Enterprises should look for technology partners who can help them meet all regulatory obligations.

IoT DEVICE SECURITY AND THE LAW OF THE LAND

The California legislature, alarmed by stories of distributed denial of service attacks (DDoS) using hijacked security cameras shipped with preset passwords, and concerned that other network-enabled consumer devices could be as easily hacked and data stolen, became the first jurisdiction in the country to pass a law intended to force improvements in device security. The new rules and regulations, which come into effect in January 2020, require that all "connected" devices sold in California, whether for consumer use or for commercial IoT applications, be able to ensure "reasonable security" and protect both the device and any data on it from "unauthorized access, destruction, modification, or disclosure." [1]

The law takes the interesting tack of assuming that end users may not voluntarily use the features on a device to improve security and, instead, places the responsibility of ensuring security, from the start, on device manufacturers. Manufacturers must equip all "connected devices" sold in California after January 1, 2020 with appropriate security features, such as shipping the device with a unique password, or requiring the user to generate a new means of authenticating the device before it can connect to a network outside of a local area network.

[1] California Senate Bill No. 327: Information privacy, connected devices

It's important to note that the law is neither prescriptive nor protective. The California legislature clearly understood that both threats and best security practices evolve. While the law suggests some minimum steps manufacturers should take, such as those mentioned above, they are free to use other security measures, so long as they are reasonable (meaning they aren't already known in the industry to have exploitable security vulnerabilities) and proportional to the sensitivity of any data that the device might collect.

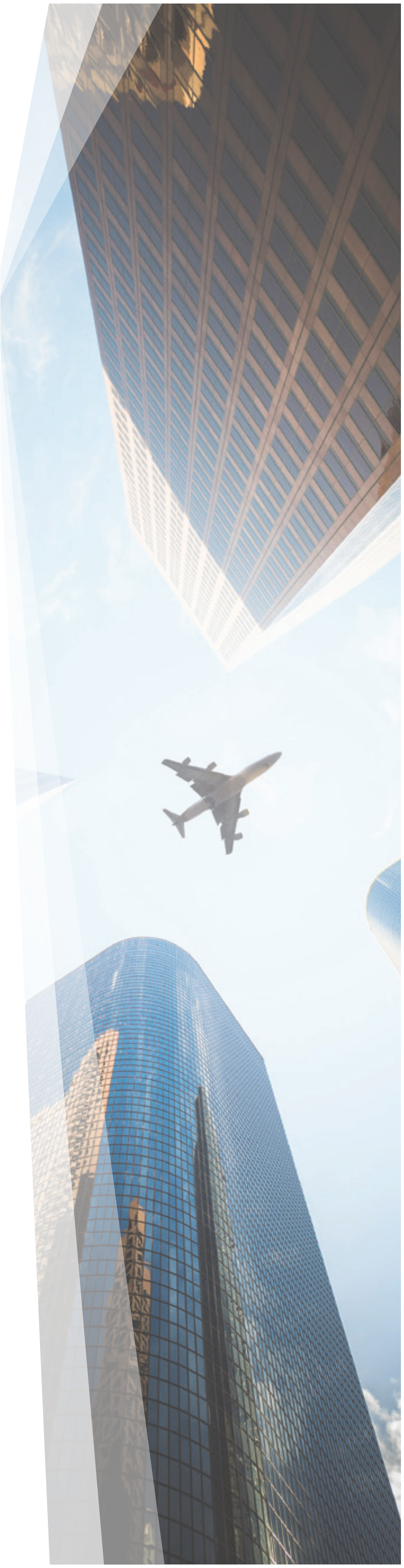
Similarly, the law does not define any fail-safe measures that will guarantee compliance or protect against future claims for compromising data security, such as compliance with a specific standard or protocol. It uses the vague term "reasonable security". Manufacturers, of course, will want to know how "reasonable security" is defined. Essentially, the standard is set by best practices in a given industry segment: if similarly-sized (and well-regarded) companies in that market are taking certain steps to secure their devices, that probably sets a minimum standard for what comprises "reasonable security" and what others in the market should be doing as well. Companies can do more, but they should not do less, and they must make some attempt to keep up-to-date on, and address, security developments, such as new threats and vulnerabilities, that also could affect their programs.

While the new California law does not specifically spell out what manufacturers should do if they find a security vulnerability, meaning there is no requirement to push out updates or to directly notify consumers of security patches, we believe that agencies tasked with enforcing this law could use the vague "reasonable security" standard to punish failure to promptly address cyber vulnerabilities as they arise, especially if a company's peers in that market are taking steps to fix those problems.

Product Security is Bigger than Device Security

Companies offering connected devices or services that use connected devices need to understand that the California bill only talks about what is needed to give a device reasonable security. Security of an overall product or service is outside the scope of this law, and companies should expect agencies, such as the Federal Trade Commission and state attorneys general, to continue enforcing other laws — for example, concerning data privacy.

Companies that use connected devices as part of an overall solution still need to secure all of the different parts of their service, from apps to cloud. Companies should look at the various security frameworks that are commonly used, such as NIST standards, or ISO 27001, and use those as guidelines to develop solutions that adequately protect systems, devices, and data from attack.



AERIS: THE RIGHT IoT SECURITY PARTNER

Aeris, as a technology leader, provides advanced solutions for securing IoT devices and the data they generate. And since security should never be an afterthought, keeping devices and their data safe starts during device design and at device provisioning and deployment. Aeris Fusion IoT Network provides solutions to device security, addressing the issue with 360-degree security best practices for IoT device communications. They include the following:

Prevent

◇ Device identity management (SIM as secure element and scalable distribution via Aeris Zero Touch Provisioning)

◇ Secure Network Edge: Use of site VPN from access edge

◇ Private dedicated IP address and APN for enterprise traffic isolation

Detect (early identification)

◇ Monitor device usage for benchmarking normal access (machine learning and AI)

◇ Reporting, auditing, and alerting of unauthorized access based on abnormal use

Protect

◇ ConnectionLock™: Restricting access to/from authorized sites

◇ Platform-level disabling of consumer traffic and device-to-device communications

◇ SMS via secure APIs only, use of non-dialable numbers for voice

◇ DoS prevention via throttling techniques (limited SMS, data caps, etc.)

◇ Software-defined transit network (SDTN) provides role-based access control and whitelisting for remote access

Respond & Resolve

◇ Contain breach by quarantining affected devices (block, suspend, cancel devices)

◇ Fix the offending devices via over-the-air (OTA) campaign management

As regulations and rules ramp up, the Aeris Fusion IoT Network can provide the appropriate solutions to device security. The following section takes a deeper dive into some of its device security capabilities.

SIM as Secure Element: Security by Design, at Design Stage

Security is best achieved when considered at the start of a new device design project, not "bolted on" afterwards. Manufacturers increasingly will be pushed, both by market demand and by regulations, such as the new California law, to equip devices from the design phase through manufacturing and distribution, with features reasonably designed to prevent unauthorized access after field deployment.

Many IoT devices are designed so as not to require further configuration after shipment from the factory. They need to be "plug-and-play" and ready to go. So, unlike consumer devices, where the consumer manually connects them and can, for example, change the default password, these IoT devices need to be secured at an earlier point in the supply chain. Designing IoT devices to use the Aeris SIM as a secure element to control provisioning and activation can be a simple way to meet these objectives. The Aeris SIM comes with a built-in secure identity and tools that enable customers to automate the identity and access management (IAM) process between the device and the network, as well as between the device and the cloud.

Defining the Allowed Network: Transit over Access-Controlled VPN

The Aeris Fusion IoT Network continuously evolves with new capabilities to support secure IoT deployments at scale, such as routing device communications over a private VPN, automating assignment of credentials, and whitelists at provisioning so that access to IoT devices over the transit network strictly is limited to the appropriate users or devices. Customers can be confident that if they manage user credentials appropriately, others will not be able to communicate with their devices.

Restricting Endpoint Access: Aeris ConnectionLock

Unless network restrictions are in place, devices can send data to or receive data from any other address on the Internet, even unauthorized ones. This increases the risk that devices will be hijacked and come under the control of rogue actors, and that application data gathered by the device could be compromised, leading to data privacy violations. Such violations would not only be expensive to remediate, they could be catastrophic for sensitive applications, such as remote patient monitoring or security systems.

In order to restrict communications with devices, Aeris provides the ConnectionLock capability, which restricts data delivery to authorized or designated IP addresses or endpoints. ConnectionLock can be activated on all devices by the Aeris support teams during the onboarding process, completely eliminating the need for customers to take additional action.

Security from the Start: Zero Touch Provisioning

Deploying IoT programs at scale calls for simplifying device onboarding processes and reducing manual steps. A common goal is to set up each deployed device to immediately be able to communicate over networks to the right destination in the cloud. But doing that securely requires examining all the steps in the process and setting the right parameters for those devices. Aeris provides customers looking to onboard hundreds, or even millions, of IoT devices with access to its Zero Touch Provisioning (ZTP) solution. ZTP is highly cost-effective, enabling customers to securely provision and connect their devices to the cloud with minimum (near zero) effort.

With Aeris ZTP, identity and access management best practices are deployed during the entire device deployment lifecycle. Devices using the ZTP SIM card have the ability to instantly access connectivity from manufacturing onward, simplifying initial provisioning, and protecting ongoing daily operations with robust security.

Remote Updates: Connectivity-Aware OTA APIs

Media reports about attacks using hijacked devices have brought the issue of firmware updates into the awareness of the public, including regulators. In the Mirai botnet attack, bad actors accessed unprotected devices and instructed them to receive unauthorized firmware downloads that converted consumer products into “bots”. The press noted that, for most of these devices, the manufacturer had no way to contact users or to send security patches and that, even if they had, most consumers likely would ignore the warnings to update.

Clearly, planning for authorized remote updates is a critical requirement for future IoT deployments, not only to add new features that enable additional revenue, but also to fix security problems. However, pushing out remote over-the-air (OTA) updates historically has been time-consuming and hard to do at scale. Devices that are offline, for example, might not receive an update, or the network might become congested trying to reach devices that temporarily are in an area with low connectivity or busy executing other instructions. And downstream customers or users might want assurance that their devices can’t accept OTA payloads from bad actors.

Aeris has developed new services, including a set of APIs, that allow customers, with the click of a control-center button, to start an OTA campaign that leverages the deep awareness that the Aeris network has of the connectivity status of devices, and completes the OTA delivery when devices are online and ready to receive the communication. Customers can spend less time manually managing their OTA campaigns and have a higher level of confidence that critical updates have gone through. These features, combined with other Aeris security features, such as ConnectionLock, help provide assurance that the right update payloads, and only the right ones, will get through.

Looking Forward

Manufacturers have justifiable concerns that a patchwork of device security requirements across the country will complicate their businesses, requiring different SKUs for different markets. What appears to be happening, however, is a game of “follow the leader”, with many states adopting regulations similar to the new California law. In effect, the California law is defining a new minimum set of requirements.

At the U.S. national level, a bill has been introduced (the “SMART IoT Act”) that similarly addresses device security, but from a different angle. This bill would call for a study of IoT security, as well as the development of recommendations from appropriate agencies, including NIST, of a minimum set of security requirements that should be met for products to be eligible for federal procurement, rather than for sale into general commercial and consumer markets.

So while it is likely that there will not be national legislation any time soon that will define a unified national standard for device security across markets, or that will centralize enforcement into a single Federal agency, we expect to see more work in the development of best practices that could be used to put more meaning into the term “reasonable security”. Aeris will continue to communicate with its customers as more clarity is gained.

We also expect to see more legislative activity in regulating the privacy of personally identifiable information (PII). California, for example, has passed one of the first consumer data privacy laws in the country, and fears of another patchwork of conflicting state requirements are motivating the U.S. Congress to consider legislation at the national level that would preempt state laws and establish a uniform system for regulating data privacy, including IoT applications. What would that law say? Would it, like the California Consumer Privacy Act, just require companies to allow consumers to ask to see what data about them is held, or to demand that their data not be sold? Or would it be far more comprehensive, like the European General Data Protection Regulation (GDPR), which specifically states that privacy is not possible without security? Companies with the most transparent data collection practices, and the strongest promises to users about the privacy of their data, still will fall short of GDPR requirements if they don’t have appropriate technical and organizational measures in place to assure security, including security of devices.

Customers whose programs collect any PII should keep a sharp eye on these developments, and keep security top of mind in designing and operating their products and services. They also should look for partners who can help them meet their regulatory obligations. Aeris will keep abreast of legislative developments and will continue to engineer solutions that help our global IoT customers deploy compliant applications and services and successfully achieve unit growth.

ABOUT AERIS:

Aeris is a pioneer and a leader in the market of the Internet of Things with a proven history of helping companies unlock value through connected technologies. We strive to fundamentally improve business performance by dramatically reducing costs, accelerating time-to-market, and enabling new revenue streams. Built from the ground up for IoT and road tested at scale, the Aeris Fusion IoT Network™ and the Aeris Mobility Platform span the IoT technology stack—from global connectivity to application services.

Visit www.aeris.com or follow us on Twitter @AerisM2M to learn how we can inspire you to create new business models and to participate in the revolution of the Internet of Things.

United States Contact:
info@aeris.net
or +1 408 557 1993

Europe Contact:
EU_info@aeris.net
or +44 118 315 0614

India Contact:
india_info@aeris.net
or +91 01206156100

aeris