Middle East Lighting Association

# Middle East Lighting Association Position on Cybersecurity & Data Privacy in Connected Lighting

## Introduction

Market research firm Gartner has estimated that the number of Internet of Things (IoT) devices in use globally will grow from 8.4 billion in 2017 to 20.4 billion this year. This near exponential increase in the number of Internet of Things (IoT) devices in the last few years, has significantly influenced even the lighting industry. Most legacy or unconnected lighting devices (throughout this paper devices can mean products, systems or services and used interchangeably) have taken the path to digitization and are now connected to the Internet, thus increasing the attack/threat surface. Such a surge in connected lighting devices will have ramifications both in terms of cybersecurity and data privacy.

While cyber security threats can impact the lighting industry by directly influencing command and control of the lighting devices, most likely they are used as a pivoting point to gain access to other connected systems (e.g. HVAC, BMS). Data privacy issues might arise from the fact that most connected lighting devices tend to have other purposes than just lighting and might collect, store, or process personal data such as geolocation, users' personal credentials including username and password.

Depending on the threat vector, lapses in cyber security and data privacy can have varying result such as an annoyance; minor disruption; compromise of personal data; safety concerns (e.g. Lighting in Airports, Hospitals, Stadiums).

In this digital age, for most organizations cybersecurity threats and data breaches can be detrimental by impacting its revenue, reputation and incurring the wrath of the regulatory agencies via fines and penalties. Thus, cybersecurity and data privacy should be addressed throughout the IoT device lifecycle (development, maintenance, support, and de-commission).

The objective of this position paper is to bring the issue of cybersecurity and data privacy in connected lighting to the attention of regulatory authorities in the Middle East region and suggest a practical path forward. This in the hope that future regulatory activity can include safeguards to protect 'data subjects' and inform and bind those who hold their data to the highest standards.

## Background to Connected Lighting Systems

While there is no formal definition of connected lighting systems (as it can mean different things to different people depending on the context), we define them to be either wired or wireless lighting systems that are either directly or indirectly connected to the internet. This makes a clear distinction between Networked lighting systems which can be defined as those having one or more lighting products communicate with another networked product but are not connected to the outside world (internet). Though networked lighting systems have existed for many years, these older wired systems are generally not connected to the Internet and in a way are air gaped, hence secure and out of scope for this position paper. In case of an on-premise standalone solution, they can be secured to a large extent by using existing IT infrastructure and by incorporating defense-in-depth mechanisms.

From a consumer viewpoint, small connected lighting systems are often found in residences and could be connected to the Internet via Wi-fi or a smart home hub. Thus, there is a huge range of connected lighting systems ranging from very small, say just one bulb (e.g. Wi-Fi connected), to large installations with thousands of luminaires.

These days lighting is frequently connected to one or more systems such as building management systems which in turn is most likely to be connected to the Internet. Many malls, supermarkets increasingly have building management services that facilitate centralized command and control. Energy monitoring and tenant billing services are integrated, thereby increasing complexity of such systems, and raising concerns on cybersecurity and data privacy.

Smart cities have enabled and accelerated connectivity of outdoor lighting. Across the globe, many city councils and municipalities are leveraging the benefits of IoT applications to make their cities more liveable, resilient, sustainable, and prosperous. For example, using connected lighting control system, the municipalities can remotely monitor and manage their street lighting. They can even predict when one of the bulbs might go bad and switch it before the event happens, there by increasing efficiency of its maintenance crew and ensuring safety of its residents along with illumination.

Additional features such as using pole-mounted sensors to monitor and manage noise levels on the streets, alerting the police if the noise level is beyond a certain threshold (e.g. accident/gunshot detection), is already available in certain cities across the world. Li-fi (short for Light Fidelity) works on the principle of modulating light waves to transmit data. Along with great quality light, users can also experience reliable, secure, and high-speed wireless connection. These examples show that apart from the basic lighting function, connected lighting installations also have other added benefits and both cybersecurity and data privacy is essential for such applications.

## Regulatory Action so far

Multiple government(s) and their agencies across the world have recognized the importance of cybersecurity and privacy for connected devices. In fact, some countries have already started to regulate them. A summary is provided below.

- EU passed the Cybersecurity Act[1], NIS[2] and GDPR[3] (referred as gold standard among data privacy regulation) which impacts organizations based in Europe and beyond.
- EU also published EN 303 645, the first standard targeting consumer IoT devices. EU is exploring opportunities to activate delegated acts of Radio Equipment Directive (RED). ISA/IEC 62443 and EN 303 645 are strong potential candidates.

[1] https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en The radio equipment directive 2014/53/EU (RED) establishes a regulatory framework for placing radio equipment on the market. It ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects. These include technical features for the protection of privacy, personal data and against fraud.

[2] Directive on Security of Network and Information Systems

[3] The EU General Data Protection Regulation (GDPR)

- Finland IoT security labelling scheme, Singapore smart product labelling scheme and UK BSI IoT Kitemark scheme have also been aligned to EN 303 645. Though these schemes are voluntary in nature, it is matter of time before they become mandatory.
- The UK is very likely to introduce regulation this year for all smart consumer products to meet “basic requirements” derived from EN 303 645 (i.e. no universal default passwords; publish vulnerability disclosure policy; publish minimum support period for security updates)
- In the US, starting Jan 2020 the states of California and Oregon has passed a regulation that requires connected devices use “reasonable security features”. Many other states are expected to follow suit. There is growing support to draft both privacy and cybersecurity laws at the national level.
- Qatar and Dubai have already passed cybersecurity regulations for critical infrastructure.
- With connected lighting growing its imprint globally, it is a matter of time before other governments such as Canada, Australia, New Zealand, China, India & Mexico pass similar regulations.

Unlike in the past, regulators need to constantly keep track of the latest technology developments and work with all relevant stakeholders (end users, manufacturers, distributors, installers, academia) to create holistic frameworks. Thus, it is also the responsibility of the lighting industry to initiate and maintain the dialogue with such policymakers to ensure that the regulations are pragmatic (i.e., capture industry trends as well as enforceable by regulators and implementable by manufacturers). To this end the Middle East Lighting Association (MELA) is keen to make inroads into this new policy area by engaging with regulatory authorities in its focus countries.

Possible approach

For cybersecurity to be effective, it must be addressed from end-to-end (design, development, installation, use, disposal) including operational aspects of maintenance and support.

This means be it product, system, or an organization - cybersecurity and data privacy is not only the responsibility of manufacturers but also other stakeholders, such as integrators, distributors, third party suppliers, support personnel and end users. This should also involve supply chain, holding the suppliers accountable to the same standards the manufactures themselves adhere to by incorporating and enforcing key clauses via contracts or master service agreements.

- For a manufacturer, it could mean incorporating cybersecurity and data privacy throughout the product development life cycle using principles of security/privacy by design and default. If manufacturers also offer maintenance and support, they must always ensure the personnel providing such services also be trained in security. They should also vet their suppliers (up-stream or down-stream) to ensure vulnerabilities (if any) are mitigated effectively. Effective incident and vulnerability management is another key aspect and so is informing the users of the timeframe (2/3/5 years) for which security updates are available.
- For an integrator, it could mean securely configuring and installing the connected systems at the customer location. They could also bridge the gap between manufacturer and end user in terms of creating awareness of the systems functionalities and hence form a critical piece of the puzzle.

- For an end user, it could mean to constantly update themselves in terms of knowledge and keep track of new developments and any vulnerabilities that might impact their product as put out by the manufacturer. This will enable them to securely operate the product, and to follow best practice as provided in the user manual. E.g. Installing or enabling security update(s) provided by the manufacturer(s).

Regulators should ensure they talk often to the ecosystem (manufacturers, consumers, academia...) and draft enforceable regulations adhering to international best practices as much as possible. E.g. Standards such as ISA/IEC 62443, EN 303 645 and regulations such as GDPR, Radio Equipment Directive provide a good starting point. However, regulators should also take note of the fact that with a lot of existing legacy systems there is no need to incorporate or implement security in the product itself, due to the inherent nature of protocols used or limitations with the systems (e.g. memory, processing speed, data transfer). In case where systems are indirectly connected to the internet, manufacturers, integrators and end users should use compensating IT controls to mitigate the threats.

Final thoughts

Connected Lighting Systems can come in various forms. This means there is no one size fits all solution. Always a thorough risk-based analysis should be performed by manufacturers to determine the specific cyber security measures needed for their systems.

This should include, but not be limited to, authentication, authorization, logging, ensuring system integrity, restricting data flow, and keeping in mind the basic tenets of security – confidentiality, integrity, and availability at the core of risk analysis. Other stakeholders should support in making the system more secure. People, process, and technology should be given equal attention.

For many lighting manufacturers and even regulators, this is relatively a new topic as previously for many decades there was no need for cybersecurity or even data privacy in a lighting setup. Now that the rate of connected lighting is increasing rapidly, it should be noted that it is cheaper in terms of cost and faster in terms of time, to integrate security and privacy measures from the beginning rather than bolt on at a later point in time.

Currently and more going forward, connected lighting systems will continue to interact with other even larger systems (e.g. Building Management System) that might be manufactured in a different geography and by a different manufacturer. This is just the nature of globalization and digitization. It is important, more than ever for manufacturers and regulators to take a holistic risk-based approach based on international standards and regulations such as ISA/IEC 62443, EN 303 645 and GDPR.

We look forward to engaging with the regulatory authorities of the MELA focus countries to ensure that future regulatory activity acknowledges the need to include safeguards to protect ‘data subjects’ and inform and bind those who hold their data to the highest standards.