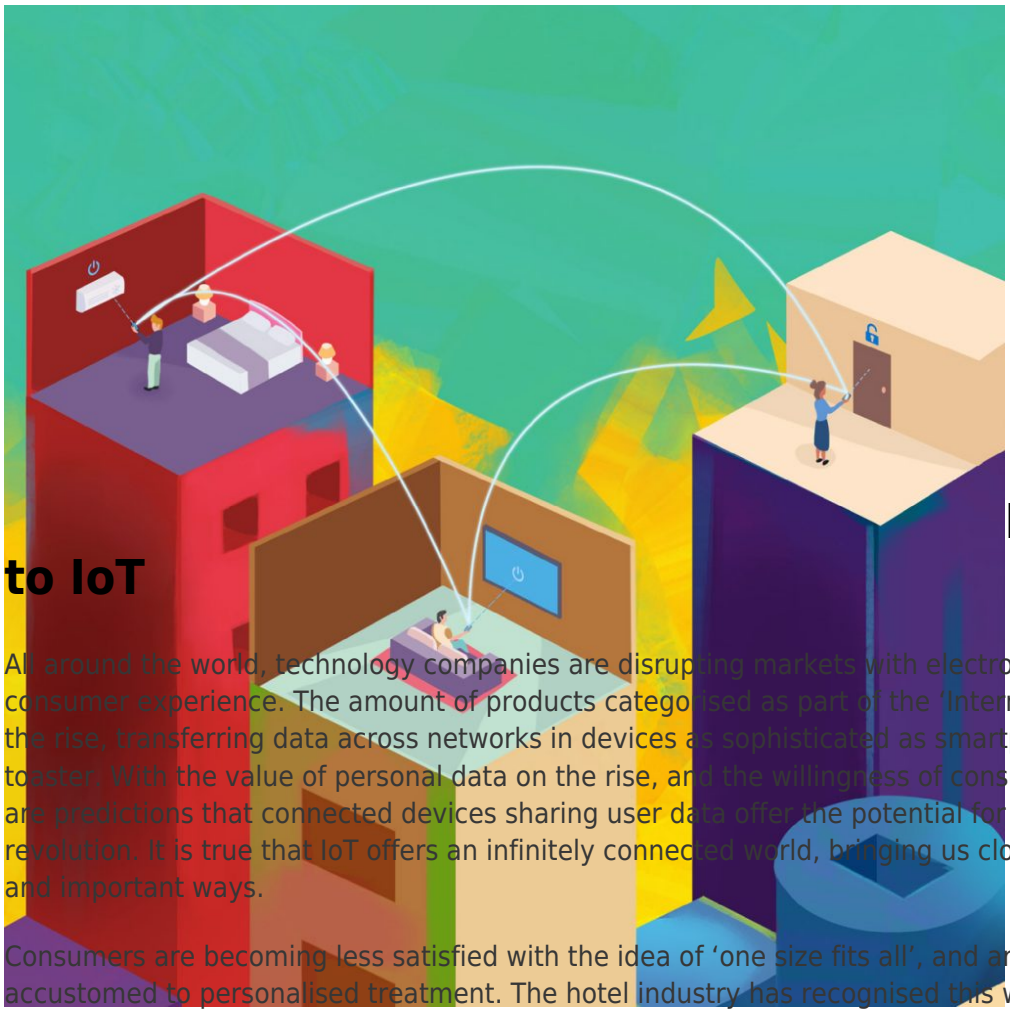
Staying smart: IoT in UAE hotels and the key legal issues

Martin Hayward - Head of Technology, Media & Telecommunications - Technology, Media & Telecommunications

m.hayward@tamimi.com - Dubai International Financial Centre

Charlotte Sutcliffe - Associate - Technology, Media & Telecommunications

c.sutcliffe@tamimi.com - Dubai International Financial Centre



Introduction to IoT

All around the world, technology companies are disrupting markets with electronics personalising consumer experience. The amount of products categorised as part of the 'Internet of Things' ('IoT') is on the rise, transferring data across networks in devices as sophisticated as smartphones, and as simple as a toaster. With the value of personal data on the rise, and the willingness of consumers to hand it over, there are predictions that connected devices sharing user data offer the potential for a fourth industrial revolution. It is true that IoT offers an infinitely connected world, bringing us closer together in very real and important ways.

Consumers are becoming less satisfied with the idea of 'one size fits all', and are growing a lot more accustomed to personalised treatment. The hotel industry has recognised this well; especially in the UAE, which is fast embracing the use of IoT in its hotels to offer a hyper personalised experience and act as a key differentiator in a highly competitive market.

IoT in hotels

Consumers now expect to find smart technology in their hotel rooms; technology that mirrors the smart technology they have at home, whether it is an intelligent thermostat, colour-changing lamp, or smart door lock. They are looking to control their hotel rooms at the press of a button or, increasingly, with a voice command. The hoteliers that get this right will secure key brand loyalty.

International hotel chains are building their IoT technology footprint with key partnerships with IoT

providers. Examples of this are Marriott's partnerships with Legrand's IoT programme and Samsung's ARTIK cloud-based IoT platform.

Hotels are also using IoT services to offer personalised services such as restaurants, gyms and activities, using location-based information (which also brings with it certain legal challenges). This can be used to send real-time information about menu options, activities close by and transport updates.

Hotel guests can even rely on their smart phones to check in and unlock their hotel doors, perhaps setting up their hotel room preferences as they walk through the lobby on arrival, creating a truly seamless customer experience.

Real-time information also allows hotel staff to be alerted to any required repairs and preventive maintenance within the hotel. There is nothing a hotel guest dislikes more than a broken TV in their room on arrival!

In addition to the advantages of making hotel guests' stays more convenient, interactive and personalised, IoT in hotels has economic and environmental advantages. For example, smart rooms that are able to monitor and adjust air, heat or lights may save company owners money on energy bills. Hotels can leverage these cost savings whilst emphasising their green footprint to hotel guests who are increasingly choosing hotels based on environmental criteria.

Of course, like any industry disrupter, IoT has the potential to pose certain risks unless businesses fully understand the relevant legal landscape in which they are operating and take steps to ensure their compliance. Laws chase emerging technology trends, but sometimes struggle to predict the unchartered waters of this increasingly connected world. This is particularly relevant in the Middle East.

Cybersecurity considerations

As IoT devices are connected to the internet, they can be hacked. This is especially concerning given the number of IoT devices and the interconnection of each IoT device within each hotel room, and with the wider hotel network. If a hacker enters through a single point of entry, there is an ability for that hacker to compromise additional parts of the overall network. Given both the growth in the use of technology like virtual room keys activated via your mobile phone and the increasing collection of hotel guest personal data through IoT devices, this potentially puts hotel guests at increased risk.

The more use hotels make of IoT devices, the more information a hotel can collect on a hotel guest and the greater the opportunity for personalisation and increasing guest brand loyalty. Hoteliers need to take steps to ensure the risk of a security breach is low and hotel guest personal data collected via IoT devices is protected. Penalties for non-compliance with laws can be severe, as can the consequences of reputational damage for hotel brands. With a number of recent high profile global cyber incidents impacting hotels, hoteliers need to be very focused on installing robust and secure IoT systems

The laws to watch out for in the UAE

Hoteliers need to be aware of a number of key UAE legal and regulatory requirements as they move forward with greater guest data collection and usage:

- compliance with UAE IoT regulations; and
- compliance with UAE personal data protection laws.

UAE IoT regulations

The UAE Telecommunications Regulatory Authority ('TRA') recently issued an IoT regulatory policy which aims to regulate IoT with the intention of making the UAE a leading country in developing IoT services and driving innovation ('IoT Policy'). Please see our previous article titled 'What's Got Hot in the Internet of Things?'.

An IoT Service Provider is defined broadly under the IoT Policy as 'any person that provides an IoT Service to users (including individuals, businesses and the government), that will comprise the provision of IoT services'. IoT services is also broadly defined. IoT Service Providers have a number of key obligations, including registration with the TRA, under the IoT Policy, and hotels adopting new IoT solutions need to assess whether they could fall into the IoT Service Provider category.

Moreover, personal data collected via IoT devices needs to be kept secure and the IoT Policy sets out key requirements for ensuring data security, particularly in relation to the transfer of personal data outside the UAE. Hotel chains use global hotel management systems and transfer and store data regionally, or even, globally. UAE hoteliers need to consider whether their current data collection, transfer and storage practices meet the requirements of the IoT Policy.

Personal data protection laws

Hoteliers generally want large, centralised datasets to analyse and monetise. This allows them to track trends in the hotel industry, as well as guest behaviour and preferences. Please see the related article entitled 'Unlocking the value in data: successfully implementing compliant data monetisation strategies'. IoT devices, by their, nature generate large amounts of valuable personal data, particularly when aggregated and mined using emerging technologies, like AI.

As set out above hotel chains are global, running globalised IT infrastructure. They transfer and hold data at a regional, and often global, level. With no comprehensive 'European style' data protection legislation in the UAE specifically designed to regulate the collection, processing, transfer and/or use of personal data, except for certain specific UAE financial free zones (DIFC and ADGM), hoteliers need to be aware of a web of UAE laws that cover the use (and particularly the transfer) of personal data to ensure that they remain compliant. Where hotels are established in the DIFC and ADGM, hoteliers need to be aware of the current data protection laws that apply to them (and also the hotly anticipated new data protection laws that are expected very soon).

Conclusion

The implementation of IoT in hotels in the UAE is increasing and UAE hoteliers should be looking to take full advantage of the benefits IoT offers to their businesses. They need to balance this opportunity with heightened awareness of, and full compliance, with all relevant UAE laws.

For further information, please contact Martin Hayward (m.hayward@tamimi.com) or Charlotte Sutcliffe (c.sutcliffe@tamimi.com).