Consumer Privacy in the Smart Era

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital and Data / Intellectual Property
n.oconnell@tamimi.com - Riyadh

Privacy as a fundamental right?

Before considering the implications on consumer privacy in the smart era, it is important to briefly touch on how privacy is protected in the law. Commentators on data protection in the UAE sometimes claim that the right to privacy is enshrined in the Constitution of the United Arab Emirates, and this forms a basis for analysing data protection issues. This would seem to be something of an overstatement when it comes to the Constitution's treatment of privacy, where at Article 31 it simply says: 'Freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with law'. The protection of personal data in the manner in which it is understood in the digital age is not contemplated in the Constitution of the UAE, and privacy is mentioned only in the context of privacy of post and communications.

Certainly around the Gulf, and across the broader region, the approach taken in the UAE is not out of the ordinary. While the claim to a fundamental right to privacy enshrined in the Constitution would be an overstatement, privacy is clearly a relevant concern in the context of doing business in the Middle East. All countries in the region have criminal prohibitions that, in some way, penalise unauthorised use and disclosure of personal information, as well as prohibitions or regulations specific to certain types of information or certain contexts – such as health records and information disclosed to medical professionals, or (for present purposes) consumer information in a telecoms context. Using a very broad-brush approach, it is fair to say that in jurisdictions without a modern data protection regime, the best way to manage the processing of personal data is to do so on the basis of the consent of the data subject.

Telecoms sector considerations – customer data

In a telecoms context, and focussing on the regulation of telecoms licensees (rather than issues such as hacking and cyber crime), the approach taken to the protection of consumer data varies across the region. Ultimately, from many of the following examples, the protection of personal data relating to telecoms subscribers as handled by telecoms licensees can be seen as significantly more prescribed than the protection of personal data more generally under the law.

By way of example, Article 12 of the UAE Telecommunications Regulatory Authority's Consumer Protection Regulations (Version 1.2 of 24 December 2015) places a number of clear obligations on telecoms licensees when it comes to the handling of subscribers' information. Licensees have to take all reasonable and appropriate measures to prevent the unauthorised disclosure or the un-authorised use of subscriber information. They must take all reasonable measures to protect the privacy of subscriber information that they maintain in their files, and use reliable security measures against risks such as loss or unauthorised access, destruction, leakage, inappropriate use, modification and unauthorised disclosure. They must limit access to subscriber information to their trained and authorised personnel, who are bound to protect the licensee's confidential information from unauthorised use and disclosure under the terms of a written agreement, and ensure that personnel engaged in the handling of subscriber information are fully aware of, and adequately trained in the licensee's security and privacy protection practices. Licensees must obtain a subscriber's prior consent before sharing any subscriber information with their affiliates and other third parties not directly involved in the provision of the telecommunications services ordered by the subscriber. Where it is necessary to provide subscriber information to affiliates or other third parties who are directly involved in the supply of the telecommunications services ordered by subscribers, the third-parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the subscriber information and to use it only as required for the purposes of providing the

telecommunication service. Licensees must ensure that the contract between them and any affiliate or other third party holds that third party responsible for the privacy and protection of the subscriber information. Licensees who have access to subscriber information as a result of interconnection are prohibited from using that information for any purposes other than interconnection, and use for marketing purposes is specifically prohibited.

The position in Qatar under Article 52 of the Qatar Telecommunications Law (and articles 91 and 92 of the associated by-law) is similarly detailed, and provides customers with a right to have their information corrected or removed, as well as obligations on service providers to use customer information only for the purposes for which it was collected (and not use it for any undisclosed or unauthorised purposes), and to ensure that customer information is accurate, complete and up-to-date for the purposes for which it is to be used.

In Oman, Resolution No.113 of 2009 issuing Regulations on Protection of the Confidentiality and Privacy of Beneficiary Data contains similar requirements, and includes a clear requirement to notify consumers in the event of data breaches that might affect them, as well as restrictions on sending consumer information abroad for the provision of subscribed telecommunications services without the approval of the Oman Telecommunications Regulatory Authority.

In Bahrain, the Privacy and Confidentiality section of the Bahrain TRA's Consumer Protection Guidelines imposes general obligations on licensees to take steps to protect the privacy of consumers regarding personal information and calling patterns, and notes that consumers should have an expectation of privacy, and protection from unauthorised use of their personal records and information, and protection from illegal, unsolicited, unwanted or offensive communications. The guidelines also state that licensees should only use information gathered from consumers for the purpose of providing the consumers with telecommunications services.

For Saudi Arabia, we were able to find only a very general reference in the KSA Telecoms Law, which at Article 3(8) simply places an obligation on telecommunications licensees to protect public interests and the interests of users and maintain confidentiality of communications and information security.

Kuwait, which is still in the process of establishing its telecoms regulator, is well-positioned to start with a blank page and draw from the experience of other countries.

Consumer data protection as a requirement for e-commerce take-up

With regard to e-commerce, a recent AT Kearney study ('Getting in on the GCC E-Commerce Game') identified consumer trust and awareness issues, along with embryonic government policies, amongst a number of key obstacles preventing the GCC e-commerce market from reaching its full potential. The report identified concerns about data security and fraud as compounding consumer trust issues. It suggested that consumers will only trust on-line channels if retailers focus on protecting customer privacy and data. The punchline is that when it comes to on-line commerce take-up, consumer concerns about privacy are a serious inhibitor.

Consumer data protection as a consideration for IOT and smart cities

As for the Internet of Things (IoT) and Smart Cities, there are massive opportunities for all those involved – but there are also broad consumer privacy considerations that need to be considered and addressed at the outset.

The mass adoption of connected digital technologies and applications by consumers, businesses, and governments is having an unprecedented transformational impact on the telecommunications industry. It is a fundamental driver to the strategic and operational decision making of telecommunications players around the world, including in the Middle East. Data can be harnessed to create innovative offerings and generate new revenue streams, it can allow businesses and governments to develop a deeper

understanding of users, improve user experience at every stage, get faster feedback, develop policy and customize services, and it allows organizations to take advantage of information in order to work intelligently and reduce costs. Connectivity and devices are increasingly ubiquitous, powerful and inexpensive. The Internet of Things will link all manner of items, from light bulbs to urban transport networks.

In this context, Dubai has issued Law No. 26 of 2015 regulating Data Dissemination and Exchange in the Emirate of Dubai. The "Dubai Data Law" has a number of objectives. It is aimed primarily at ensuring that data gathered by Dubai government entities is effectively shared amongst such entities and with the private sector, so as to maximise opportunities to capture the benefit of such data for the emirate's residents, visitors, and economy. The aims of the Dubai Data Law include managing data in conformity with international best practices, promoting transparency and establishing rules for data dissemination and exchange, increasing the efficiency of services provided by federal government entities and local government entities, and providing data necessary to non-governmental entities with a view to supporting the development of the Emirate of Dubai. Significantly, an expressed aim of the Dubai Data Law is to strike a balance between data dissemination and exchange and data confidentiality and privacy.

The IoT will have significant impacts on consumer privacy, and this is material to players in the telecoms space – whether they are device or app developers, or network operators providing the technical framework for processing big data and operating smart cities. Sensors embedded in millions upon millions of devices in as many locations, all processing an enormous amount of data – including personal data – at different locations, will make it hard for people to know exactly who is using their personal information, and the purposes for which it is being used. Being able to cross-match data across different data pools/sources raises question as to whether anonymity is a relative term, and the ability to find secondary uses of data – which could be seen as a key benefit of big data – further raises questions about gathering data for one purpose, and then using it for other purposes. This potential lack of clarity raises issues from a consent perspective, as if users do not know what information is being collected (or whether it is being collected at all), and the purposes for which it will be used, it will be difficult for individuals to provide meaningful consent. Additionally, where devices gathering data may be more difficult to secure (e.g. due to limitations on encryption and wireless communication, and the fact that many devices may be outside a traditional IT infrastructure and thus not have security built-in), there is a greater risk of data loss, unauthorised access and infection by malware.

Telecoms operators have unrivalled expertise in providing high-quality, well-managed, and reliable networks. They have significant expertise in hosting, on-line security and identity authentication. A major part of the opportunity that lies in store for telecoms operators will be to monetize the large volumes of data that pass through these networks. In this context, a key duty of telecoms operators, particularly in the Middle East, will be to set the standards for safeguarding the personal information and commercial information shared by consumers, companies, and machines over these ubiquitous networks.

The types of products and technologies in which telecoms operators are likely to become involved in this context give rise to important privacy issues that cannot be addressed solely by reference to the regulatory landscape applicable to telecommunications operators. By way of example, the delivery of e-health and telemedicine solutions and associated data analytics, will also touch on concerns relating to medical confidentiality, patient health information and the location and retention period for storage of medical records. The adoption of an advertising-funded business model may use behavioural and demographic tracking to increase relevance. The provision of smart grid/metering solutions may raise privacy concerns that tie-in with pricing-related consumer rights considerations.

With the wide variety of services in which telecommunications service providers may become involved in the digitized age, the relevance of 'traditional' telecommunications-sector consumer protection regulations, particularly with regard to privacy, may need to be revisited. Those looking to participate in the IoT and big data space need to consider the consumer privacy implications of what they are doing at the earliest opportunity so as to incorporate sufficient privacy and security mechanisms at the outset –

rather than having to ‘retro-fit’ them into devices, systems and processes as an afterthought.

Al Tamimi & Company’s Technology, Media & Telecommunications team regularly advises on issues at the core of innovation, including issues to do with the development and regulation of new technologies and issues to do with consumer privacy. For further information please contact Nick O’Connell (n.oconnell@tamimi.com).