# Data Protection and Privacy Issues in the Middle East

by Nick O'Connell - n.oconnell@tamimi.com - Riyadh

January – February 2012

The following is a summary of key aspects of notes from Nick O'Connell's presentation at the Telecommunications Law & Regulation in the Middle East conference, held in Dubai on 12 & 13 December 2011.

**Introduction**

The topics that I have been asked to cover are privacy, data protection, spam, consumer protection and cloud computing. The common thread between these topics is the need to balance the benefits of living in the information age with the expectation of privacy. On the one hand, the information age brings with it many benefits (including greater efficiency and convenience with regard to gathering, storing and using data). On the other hand, expectations with regard to protection from arbitrary interference with privacy are generally considered a well-established social and legal norm – including in this region.

**Privacy**

Generally speaking, the position in most of the GCC countries is that the privacy of an individual is protected under general provisions of laws not specifically focused on the issue of privacy. By way of example, the UAE Penal Code makes it an offence to publish, through any means, news, pictures or comments pertaining to the secrets of people's private or familial lives. It also makes it an offence for anyone who is, by reason of profession, craft, circumstance or art, entrusted with a secret, to disclose the secret, or use it for his or her own benefit, or that of another, unless such disclosure or use is permitted by law or by the consent of the person to whom the secret pertains.

The key point that I wish to illustrate by these examples is that the these privacy related provisions have not been drafted with the information age in mind. To provide some context, we have recently relied on provisions such as this to advise on a corporate client's proposed transfer of employee data to an off-shore data storage facility and another client's proposed use of customer data for purposes other than those for which it was originally gathered. Would a company's use of personal information (such as employee information or customer information) for fairly mundane business purposes (such as off-shore data storage or targeted marketing campaigns) fall within prohibited uses of 'secret' information under these penal provisions?

Other laws restrict the use of personal data in certain circumstances. By way of example, the UAE Medical Liability Law (Federal Law No. 10 of 2008) prohibits a doctor from disclosing the secrets of the patient that the doctor becomes aware of in the course of practice, either if the patient trusted him with the secret or if the doctor became aware of the secret in the course of practice.

We recently conducted a review of the situation in other GCC countries and essentially confirmed that privacy is protected in these other countries in much the same way as in the UAE. Laws designed primarily to protect privacy do not typically exist as laws in their own right. Provisions relating to protection of privacy may be found in the context of other laws, including respective penal codes and laws relating to specific matters such as regulation of conduct of medical practitioners, credit disclosure and unfair business practices.

**Data protection**

Both the Dubai International Financial Centre and the Qatar Financial Centre have their own data protection specific laws or regulations. These legal provisions are generally consistent with data protection laws from other developed jurisdictions (specifically, the EU Data Protection Directive 95/46/EC and the UK Data Protection Act 1998). They apply to specific types of personal information that can relate to identifiable individuals, and set out obligations requiring that personal data be processed fairly, lawfully, securely and for a specified and legitimate purpose. They also contain restrictions on data transfer from within the respective Financial Centres to places outside those Financial Centres. The most significant point to note about the respective data protection provisions of these Financial Centres is that they are applicable only to activities within those Financial Centres – or transfers from those Financial Centres to places outside the Financial Centres.

In contrast, Oman and Qatar both have laws relating to e-Commerce which contain provisions relevant to data protection. Oman's Electronic Transactions Law (Royal Decree 69/2008) and Qatar's Electronic Commerce and Transactions Law (Law No. 16 of 2010) are both based largely on the UN Model Laws relating to e-commerce and electronic signatures – but the laws as enacted in both countries go beyond these to include specific provisions relating to data protection. Specific data protection regimes appear to be common in respect of telecommunications service providers. By way of example, Qatar's Telecommunications Law (No. 34 of 2006) requires telecommunications service providers to operate their telecommunications networks and related systems with due regard for the privacy rights of their customers, and requires telecommunications service providers to be responsible to protect any customer data in their custody and to refrain from collecting, using, retaining or publishing any customer information unless with the customer's consent or as permitted by law. Additionally, service providers must ensure that all the information submitted is accurate, complete and valid for use (and correct or remove data upon the customer's request).

Similar provisions (although with varying degree of detail) apply to telecommunications service providers licensed by the telecommunications regulatory authorities in other GCC countries. The UAE's Telecommunications Regulatory Authority has issued the Privacy of Consumer Information Policy. Oman's Telecommunications Regulatory Authority has issued Resolution No. 113/2009 issuing Regulations on Protection of the Confidentiality and Privacy of Beneficiary Data. Thus, telecommunications service providers should be aware that special data protection regimes may apply to their activities, even if there may be no data protection laws of general application.

**Consumer protection and spam**

The next topic ties in with the issue of privacy and data protection in the sense that personal contact details, such as mobile numbers and email addresses, may be disclosed by customers in the context of procuring goods and services, and then used subsequently for electronic marketing purposes. Many people find this type of marketing to be invasive of their privacy, and prefer to receive it only if they have 'opted-in'.

In some countries in the region there are general prohibitions on this type of activity. By way of example, the consumer protection provisions of Qatar's Electronic Commerce Law restricts the ability of e-commerce service providers (not necessarily telecommunications providers) to be involved in providing unsolicited marketing communications, and requires consumers to be able to opt-out from the receipt of such communications.

In July 2010, the UAE Telecommunications Regulatory issued a specific policy on unsolicited marketing communications. Under this policy, licensed telecommunications providers in the UAE are required to minimize spam and take all reasonable steps to ensure that spam is not being sent

over their networks. If a licensee (ie. a telecommunications provider) fails to take all practical steps to prevent spam 'with a UAE link' (which includes spam originating both inside and outside the UAE) from being sent over the licensee's network, then the regulator can take action against the licensee. The policy also prohibits licensees from being involved in 'address harvesting', and it requires them to implement 'opt-in' consent processes for all electronic marketing provided to customers. Additionally, by way of an annex to the policy, the UAE TRA has provided similar restrictions specifically in respect of SMS spam sent via mobile phones.

**Cloud computing**

The term "cloud computing" describes a broad range of remote access computing services, generally involving situations in which users have access to applications and data storage services on demand and delivered over an external network. This basically involves the use of software and/or data storage space provided by someone else – allowing for savings on things such as licensing software or buying data storage hardware.

Some of the key privacy and data protection considerations in a cloud computing environment are:

- Data security – The cloud user will have its own data security and access management policies. The cloud provider's policies should, at a minimum, be compliant with the cloud user's policies.
- Data location – It is necessary to consider the impact of the various laws governing privacy and data protection on the collection and transfer of data to the cloud provider, and the movement of that data across different jurisdictions as part of the provision of the cloud service.
- Data retention obligations – Different jurisdictions have different commercial record retention obligations. If data storage obligations are outsourced to a cloud provider in a different country, it will be necessary to ensure that, at a minimum, the cloud provider complies with document retention policies applicable to the user of cloud services.

Corporate users of cloud services may place responsibility for direct control of critical data and applications in the hands of third parties. If there is an outage or a security breach, the user could be exposed to claims from its own customers (and potential reputation damage) even though the fault was on the part of the cloud provider. Similarly, failure on the part of the cloud provider (eg. with regard to compliance in respect of data privacy) could lead to regulatory non-compliance on the part of the cloud user. Cloud users should conduct thorough due diligence of the provider they are considering and in particular focus on the privacy and security levels of the services to be offered.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on data protection matters in the Middle East. For further information, please contact David Yates (d.yates@tamimi.com) or Nick O'Connell (n.oconnell@tamimi.com).