Privacy and principle: Data protection in light of Saudi's Vision 2030

Against a background of great change in the Kindgom of Saudi Arabia, Courtney Bowman provides an overview of Saudi privacy law generally, as well as trends to watch going forward.

Data privacy laws are becoming an increasingly important consideration in companies' compliance strategies in almost every jurisdiction around the world. These laws regulate how, when, where, and for what purpose a company may collect, transfer, and process data about individuals, such as customers and employees, thereby forcing companies to rethink their data flows and data-storage practices.

While certain high-profile legislation, such as the EU's impending General Data Protection Regulation, Russia's data localisation law, and China's Cybersecurity Law, currently serve as the primary compliance targets (and, in some cases, the greatest sources of consternation) for privacy departments worldwide, other jurisdictions' laws tend to fly under the radar. However, it is important for any multinational company to understand the privacy laws in each jurisdiction in which it operates in order to ensure compliance and avoid any of the (sometimes onerous) penalties for violating those laws.

One of the countries that presents a privacy law paradox for many companies is Saudi Arabia. Although many US- and EU-based companies conduct business in the Kingdom, there is little easily accessible information about Saudi privacy laws and how they may impact foreign businesses in the country. Further complicating any analysis of existing laws is the fact that the government has pledged to make the country a more business-friendly jurisdiction, potentially heralding new initiatives and more streamlined laws to encourage investment – meaning that there is potential for the privacy law landscape to shift in the near future.

Legal atmosphere

As a preliminary matter, it is essential to understand the context in which Saudi privacy law exists. Like many countries, Saudi Arabia derives its privacy law from two primary sources: its constitution (the Basic Law of Governance) and privacy-specific legislation. In terms of its legislation, Saudi Arabia – unlike the EU – does not have a single omnibus privacy law that governs a wide range of issues, from data collection and storage to data breach notification, and there is no single governmental body charged with privacy enforcement. Instead, the Kingdom has implemented a number of sector-specific laws that impose privacy-related requirements on certain industries. For example, banking and health data may only be transferred abroad with the permission of certain Saudi government agencies, while the Telecommunications Act prohibits internet service providers from intentionally disclosing the contents of messages sent over their networks.

What distinguishes the Kingdom from many other countries from a privacy perspective, however, is the fact that it also derives some of its privacy principles from a third source: Sharia, which is sourced from *The Quran* and the practices of the prophet Muhammad. Although it often is referred to as 'Islamic law', that description does not capture the more comprehensive nature of Sharia, which provides a guide for living one's life in compliance with Islamic principles. Countries throughout the Islamic world have incorporated different interpretations of Sharia into their legal systems to varying extents. In Saudi Arabia, where Islam permeates nearly every aspect of society, judges apply Sharia in adjudicating claims – particularly in areas where no legislation exists. This means that even if a company is not subject to one of Saudi Arabia's sector-specific privacy laws, it may still face liability for wrongful disclosure of an individual's private information – which is considered a tort under Sharia principles. Unfortunately for those looking to educate themselves on how the law is applied in practice, many Saudi court decisions are unpublished and, in any event, are not always considered precedential.

What distinguishes the Kingdom from many other countries from a privacy perspective is the fact that it also derives some of its privacy principles from a third source: Sharia.

This panoply of laws and legal sources makes Saudi Arabia a particularly

challenging jurisdiction in which to operate from a privacy perspective. Given the dearth of published regulatory guidance and precedential court decisions, it is difficult to determine which laws are relevant to a company's privacy practices and how they might be enforced – making knowledgeable counsel essential to any business that wishes to operate in the Kingdom.

Trends to watch

As in other Gulf countries, the Saudi government seems to have realised that its continued dependence on oil revenues is not a viable path forward and has undertaken initiatives meant to diversify the economy. In that spirit, the government has published its ambitious 'Vision 2030' plan, portions of which suggest an effort to improve the ease of doing business in the country in order to encourage investment and grow the economy. One of the areas that appears to have been targeted for growth is the digital sector, and particularly the cloud computing space; however, Saudi authorities have indicated an awareness that the current legal landscape, as described above, makes it difficult for companies to determine which regulations apply to their operations in the country.

In an effort to clarify relevant requirements and encourage growth in the cloud computing sector, the Kingdom's Communications and Information Technology Commission published a set of cloud computing regulations that are scheduled to go into effect in March 2018 (see box). The regulations require some cloud services providers – such as those which have 'critical' infrastructure in Saudi Arabia – to register with the Communications and Information Technology Commission in order to operate in the country. They also introduce a number of privacy law concepts that have surfaced with increasing frequency around the world but were, until now, largely absent in Saudi law, such as a data breach notification requirement and a mandate that cloud computing providers adopt certain cybersecurity measures. The cloud computing regulations signify a possible shift toward a more business-friendly atmosphere in which privacy laws and regulations are further developed and streamlined for foreign companies seeking to do business in the country.

Conclusion

The first step for any company concerned about its privacy practices in a particular country is to develop an awareness not only of that jurisdiction's legal landscape, but of potential impending changes that could represent a shift in the current system. Privacy law is an important consideration for any company seeking to do business in a foreign jurisdiction, and Saudi Arabia's privacy law regime presents unique challenges, given its multitude of sector-specific laws and the potential applicability of Sharia in some situations. However, recent developments, such as the adoption of cloud computing regulations and, more broadly, the government's focus on diversifying the economy and attracting investment, indicate that the legal and commercial landscape may be changing – and that privacy law may change along with it.

It also is important to note that this development is one facet of what has the potential to be a larger societal change within Saudi Arabia. The country, infamous for forbidding women to drive, finally has promised to allow women behind the wheel beginning this summer. A long-standing ban on cinemas appears to have been lifted, and tourist visas – notoriously difficult, if not impossible, to obtain – may become a reality as soon as next month, representing an effort to boost tourism.

Of course, it is difficult to predict whether these changes will leave an enduring mark on Saudi society (or, for those promises yet to be realised, whether they will be implemented at all). Likewise, it still is too early to tell whether the country will make the legal changes necessary to fulfill its apparent desire to develop a reputation as a business hub.

Nevertheless, the prevailing attitude seems to be one that is more open to change than in years past, which could mean that many legal areas – including privacy law – likewise may be more susceptible to change in the coming years. ■

Cloud computing in the Kingdom: key facts

- 'Customer Content' (that is, information that is stored or processed in the cloud and is provided or generated by a user of a cloud service) is divided into one of four classifications, which in turn determine the level of information security that must be afforded to that data. These classifications range from Level 1 data ('Non-sensitive Customer Content of individuals or private sector companies') to Level 4 data ('Highly sensitive or secret Customer Content belonging to relevant governmental agencies or institutions').
- While the regulations do not provide a definition for the term 'sensitive', they do provide some examples of how certain types of data may be classified. For example, data associated with 'natural persons with a Residence in the Kingdom' is considered Level 1, while data relating to 'any government or State services or agencies' is classified as Level 3.
- Level 3 data may not be transferred outside Saudi Arabia in any format or for any length of time unless expressly allowed by other laws. The regulations therefore appear to place a premium on the protection of governmental data.
- The regulations include a data breach notification provision. In the event of 'any security breach or information leakage' (i.e. a data breach), a cloud service provider must alert its customers of the incident 'without undue delay' if the incident is likely to affect those customers' content or data stored on the cloud, or any cloud service those customers may receive from the provider. The cloud service provider must alert the Saudi Communications and Information Technology Commission 'without undue delay' if the incident is likely to affect any Level 3 content, or a 'significant number' of cloud customers.

See The Cloud Computing Regulatory Framework:
www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf

Courtney M. Bowman is a litigation associate in the Los Angeles office of Proskauer Rose. She specialises in international data protection law.

CBowman@proskauer.com