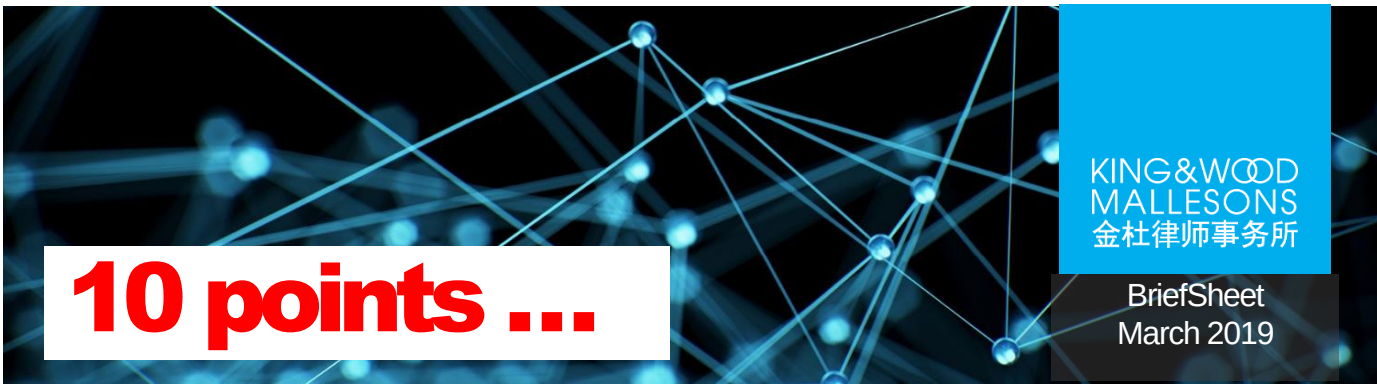

10 points …

KING&WOOD MALLESONS 金杜律师事务所

BriefSheet
March 2019

on digital identity

This KWM BriefSheet sets out 10 points on the what, how and why of digital identity

- **A digital identity can arise in many ways…** At its core, a digital identity is a set of attributes that can allow an individual or entity to be represented in digital form in an online environment. It could even represent a *thing.*
- **…and take many forms…** A digital identity can take a myriad of forms, ranging government protocols to private solutions and "self-sovereign" products. Even a gaming "avatar" and a social media profile are forms of digital identity. Digital identity may be accessed via a card / device, username / password or via your biometric data – or a combination.
- **…with a variety of attributes.** The data may be verified by a government body, financial institution or other third party. Conversely, it may simply be self-certified, or even false. It may comprise basic details such as name, date of birth and identification number, or extend to much deeper information, such as medical history, preferences, behaviour and social graph data.
- **Creating a digital identity can be simple or complex…** A digital identity can arise organically from information provided and activities online or it can be purposefully produced. Various technologies underpin these projects, including encryption, cloud, open API and/or blockchain.
- **…and it can be used in a variety of ways…** Digital identity can be used to facilitate identity authentication, digital signatures, rapid form-filling, regulatory compliance, data analytics and building cognitive systems. There are numerous current use cases, including Estonia's e-identity programme, India's "Aadhaar" scheme, and industry-specific applications such as Sweden's "BankID". The United Nations also deploys digital identity through the World Food Programme.
- **…including smart contracts and IoT.** Digital identities can help power smart contracts. When attached to *things*, they are also especially useful for building the internet of things (IoT), and assisting with its effectiveness and systemic integrity.
- **It must meet legal and regulatory requirements.** Data privacy, cybersecurity, outsourcing, anti-discrimination laws and other local market expectations must be addressed. If digital identity has a "regtech" compliance aim, it must also be fit for that purpose.

  For example, digital identity can only be used for AML/CTF purposes if it is accurate, reliable and up-to-date. It must also meet other tests. Whether or not data meets these tests depends largely on its source. For example, if open API connects a digital identity with government-held data, it is far more reliable than self-certified information.
- **Digital identity does not come without risk…** The most significant risk is data breach, particularly where sensitive information is used. In particular, biometric data can make digital identity more secure, but if "stolen", it cannot be "reset" as with a username and password. An individual's fingerprint will always be their fingerprint.
- **…which can be mitigated but not eliminated…** Risk is minimised through proper design, diligence and documentation. Three-factor authentication, the use of open APIs to minimise the creation of "honey pots" of data, regulatory controls and well-drafted contracts are some of the key risk management tools.

  Blockchain technology can also be useful, although one of its greatest advantages (immutability) can pose a barrier to privacy compliance if carelessly adopted. This means that legal and regulatory issues must be a part of its fundamental design.
- **…and responsibility must land somewhere.** The use of digital identity needs a robust statutory and/or contractual liability model to address complaints, civil claims and other consequences arising from the misuse, loss or unreliability of data.

  Importantly, it is not always possible to contract out of all liability. Regulators also often take a dim view on exclusions that unfairly affect customers. Reputation risk is particularly critical to manage, as digital identity is fundamentally predicated upon *trust*.

We are here to help you

URSZULA MCCORMACK
Partner, Hong Kong
T: +852 3443 1168
M: +852 6796 6130
urszula.mccormack@hk.kwm.com

SCOTT FARRELL
Partner, Sydney
T: +61 2 9296 2142
M: +61 409 042 883
scott.farrell@au.kwm.com

MINNY SIU
Partner, Hong Kong
T: +852 3443 1111
M: +852 6390 4561
minny.siu@hk.kwm.com

STEFANIA LUCCHETTI
Partner, Milan
T: +39 02 3031 751
M: +39 33 4618 3000
Stefania.Lucchetti@eu.kwm.com

SHAWN DAVIS
Partner, Dubai
T: +971 4313 1746
M: +971 5081 85510
shawn.davis@me.kwm.com

LEONIE TEAR
Senior Associate, Hong Kong
T: +852 3443 8375
M: +852 6075 0086
leonie.tear@hk.kwm.com