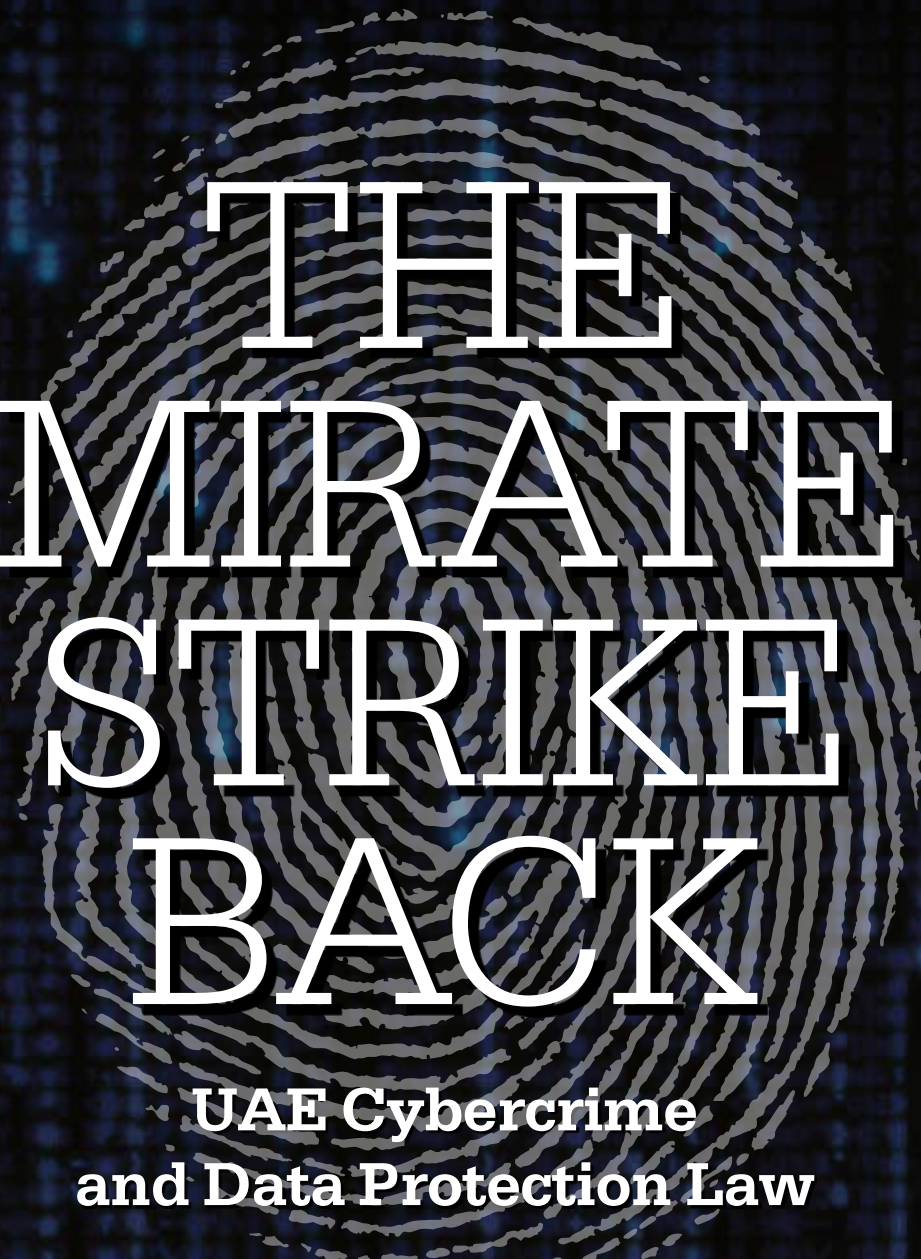


Emirates Law

Vol 1 Jan 2016 / Cyber Security

Business & Practice



THE EMIRATES STRIKE BACK

**UAE Cybercrime
and Data Protection Law**

**Paul Werné &
Paul Andrews
Investing
in Emerging
Markets**

**Dino Wilkinson
Regulation
of Data Use**

**Payam Beheshti &
Victoria Hambly
Social Media
Privacy
In the UAE**

Your local bridge to our global network

Baker & McKenzie Habib Al Mulla brings over 30 years' local know-how, extensive global resources, and one of the largest litigation teams in the UAE with full rights of audience before all UAE and DIFC courts.

Delivering unmatched on the ground support that reflects a deep understanding of local legal, regulatory and commercial practices, we are ready to serve as your strategic legal advisor in the UAE and around the world.

www.bakermckenzie.com/unitedarabemirates

Baker & McKenzie.Habib Al Mulla is a member firm of Baker & McKenzie International, a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

© 2015 Baker & McKenzie.Habib Al Mulla



Introducing a New Legal Magazine to the World



Justice Dr. Jamal Al Sumaiti
Director General, DJI

The culture in my beloved city Dubai is to be a pioneer and to lead the world in all aspects of life. It is the city of leadership where being number one is important, as runner-ups tend to be forgotten. In order to be a leader, you need to be courageous and ambitious so you can overcome whatever obstacles you encounter. As Alfred P. Sloan said, "There has to be this pioneer, the individual who has the courage, the ambition to overcome the obstacles that always develop when one tries to do something worthwhile, especially when it is new and different."

One of the most valuable competitive brand strategies any company can embark on is what I refer to as being a 'pioneer'. Being a pioneer means being first in the

region and the world to enter an emerging market or to create a new market altogether. This is the reason why we at Dubai Legal Institute have launched Emirates Law & Business Practice. Our aim is to be the most successful legal magazine in the world. To provide our readers with details of new concepts and issues that really attract practitioners from around the world and help make the life of investors easier.

We want to share knowledge, and add value to them and the legal community. We have decided our magazine will have its own personality so it can be seen as distinguished and provide readers with new and fruitful legal knowledge. As part of this we came up with the idea of having a theme in each issue. The theme in this issue is cybercrime and data protection in UAE. Our idea has been to compare the UAE position with various other regimes. As far as data protection regulation is concerned, this area is still not mature enough but there are some positive signs it is being strongly considered by the government. This can be seen by the new laws on open data in Dubai in 2015 and the current cyber crime law which was issued in 2012. Within the magazine, we plan to have an elite panel of practitioners from across the world, experts in each field we tackle who will write and share their thoughts.

Emirates Law & Business Practice will be a worldwide legal magazine created by Dubai Judicial Institute, which can be trusted and be of use to all practitioners. We hope it will be a rich and well informed magazine, providing our readers with a range of legal information about the law, global legal challenges and issues.

I hope you enjoy our first issue, if you would like to read future issues either go to our website or contact our editorial team to find out if you qualify to be added to the print circulation.

Emirates Law Business and Practice

Emirates Law Business & Practice is a free quarterly printed publication reporting on recent legal developments around the world. Articles are practitioner oriented and non-academic. The magazine covers specialist subject areas offering independent analysis by experts in their field, such as the judiciary, academics, solicitors, barristers, in-house lawyers, government lawyers, corporate lawyers, and students. Our aim is to be an international law magazine, making a significant contribution to legal debate. Emirates Law, Business & Practice provides its readers with a wide selection of relevant law disciplines, addressing various aspects of law.

Dubai Judicial Institute

P.O. Box 28552
Dubai, U.A.E.
Tel +97142833000
Fax +97142827071
editorial@dji.gov.ae
www.dji.gov.ae

Editorial board

Editor in Chief

Justice Dr Jamal Al Sumaiti LL.M., Ph.D.

Editor Sogol Kaveity LL.M

skaveity@dji.gov.ae

Board Member

Mohamed Al Yafeai LL.B.

Advertising

Roudha Al Shamsi BSc.
ralshamsi@dji.gov.ae
Shamsa Al Marri MSc.
salmarri@dji.gov.ae

Advisory board

Baker & McKenzie Habib
Al Mulla: Dr. Habib Al Mulla, Clifford Chance;
Robin Abraham, Clyde & Co: Alec Emmerson,
DIFC Courts:
Justice Omar Al Muhairi,
Etisalat: Paul Werné, Hadeef & Partners: Sadiq Jafar, Jones Day: Sheila L. Shadmand, Norton Rose Fulbright: Patrick Bourke, Al Tamimi & Co: Essam Al Tamimi.

Publisher

LexisNexis Middle East
Head of Middle East
Publishing: Hussain Hadi
hussain.hadi@lexisnexis.co.uk
Editorial Consultant:
Claire Melvin claire.melvin@lexisnexis.co.uk;
Photographer, Mostafa Samir

Printed by Royal Printing Press, PO Box 2839, Sharjah

Circulation

Emirates Law, Business & Practice can be accessed online free of charge from dji.gov.ae. To find out if you qualify to be added to our controlled print circulation E-mail: editorial@dji.gov.ae

The publishers regret that they cannot accept liability for error or omissions contained in this publication, however caused. The opinions and views contained in this publication are not necessarily those of the publishers. Readers are advised to seek specialist advice before acting on information contained in this publication, which is provided for general use and may not be appropriate for the readers particular circumstances. The ownership of trademarks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system or transmitted in any form without the permission of the publishers in writing. An exemption is hereby granted for extracts used for the purpose of fair review.

© 2016 Dubai Judicial Institute

Justice Dr. Jamal Al Sumaiti



The Emirates Strike Back

Cybercrime & Data Protection

P5

Keeping IT Safe

Our expert panel considers the level of protection given to investors by the 2012 UAE Cyber Crime Law.



P8

Now IT's Personal

With UAE data protection legislation more dispersed than in some jurisdictions, our expert panel provides a guide to the key places to find it.



P10

A Sectoral View

The Credit, Telecoms and Health sectors all have specific data protection regulation issues to face, as our expert panel explains.

P15

Industry View

HE Majed Al Mesmar of the Telecommunications Regulatory Authority explains the regulator's view on spam and privacy protection.

P16

Cyber Security & Data Protection

Nick O'Connell of Al Tamimi & Co provides a run-down of necessary roles and responsibilities.



P19

Case Focus...

With the Shrems case leading to an EU rethink of the approach to US personal data transfers, Elizabeth Robertson and Rosalind Meehan of Jones Day look at the less publicised implications for UAE data transfer regulation.

P21

DDoS Attacks & Cyber Extortion: Growing Risks

Monty Raphael QC of Peters & Peters and Chair of the International Bar Association Cybercrime Subcommittee looks at the growing risks in this area for law firms.

P30

Key Precedent

Do you have a right to be forgotten?

The UAE may have a less centralised legal framework for regulating data and IT services than some jurisdictions but that doesn't mean it isn't tackling emerging risks and issues.

Our **expert panel** explains how the recent cybercrime legislation is tackling new areas including the growing risks from social media use and the changes in spam, and general and sectoral data protection regulations.

P23

To Post or Not to Post...

Payam Beheshti & Victoria Hambly of Clifford Chance look at the interplay between privacy and social media.



P25

Cybersecurity and Data Protection

Sana Saleem of Al Tamimi & Company explains how these issues are being tackled internationally and by other jurisdictions.



P28

Data Trends...

Dino Wilkinson of Norton Rose Fulbright LLP considers the regional trends in cyber security and data protection.



“Arbitration is an assurance for foreign firms to invest in the UAE.”

P32
Profile: Diana Hamade Al Ghurair
(Internatinoal Advocate
Legal Services)

P39 **Mastering the Legal Game**

Professor Sebastiaan Kodden of Nyenrode Business University in the Netherlands explains how theory can help legal practice.

P40 **UAE Business Hub** **with Justice Omar Al Muhairi**

Justice Omar Al Muhairi talks about a day in the life of a DIFC court judge.



P44 **Making Emerging Markets Less Risky Business**

Paul Werné and Paul Andrews of Etisalat Group review the dos and don'ts of investing in emerging markets.



P47 **Arbitration**

Case Focus: Enforcement of Foreign Arbitral Awards

Sami Tannous and Antonia Birt of Freshfields Bruckhaus Deringer LLP explain why the Dubai Court of Cassation's decision in the Al Reyami case has been so widely praised.

World Class Arbitration?

Arbitration activity may be increasing in Dubai, but Alain Farhad of Squire Patton Boggs, looks at whether it can now be classed as a modern international arbitration jurisdiction.

P51 **Helping Hands**

With Expo 2020 on the way, Mahmood Hussain of Mahmood Hussain Advocates & Legal Consultancy considers what changes the new Dubai Public-Private Partnership Law will make.



P53 **Lessons for Lawyers**

It's not just clients that need to think about cyber security – it can also cost law firms their business and reputation.



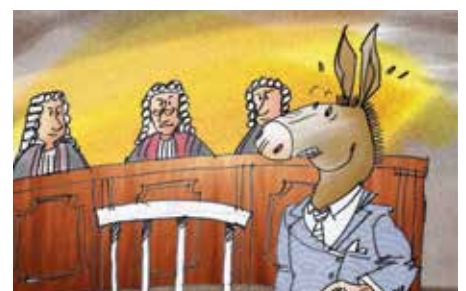
P55 **Law Graduate: Dina Al Dulaimi**

Dina Al Dulaimi talks about her experience of studying law in the Netherlands and her wish to work in Dubai.

P59 **Did you Know?... where all the wigs and gowns come from?**

P60 **Remarkable!**

The donkey's day in court, and By Definition explains “De Jure”.



Leading IP practice in the MENA region

Clyde & Co has been involved in the protection of IP rights across the Middle East since the 1980's, with dedicated IP experts operating from our Dubai office for 12 years.

Our **33-strong IP team** includes experts recruited from some of the top IP practices around the world (including Australia, Hong Kong, Japan and the UK). The team has 8 native Arabic speakers.

We offer a full service IP practice and are able to assist clients with any aspect of the IP life cycle, **from strategy, through to registration, commercialisation and enforcement**. Our practice spans the full spectrum of IP rights and includes:

- patents
- trade marks
- copyright
- designs
- know-how
- trade secrets

We have a dedicated trade mark portfolio management team with experience across a wide range of industry sectors. We advise some of the largest and most established local, regional and global brand owners in relation to trade marks and domain names across the Middle East & North Africa.

For more information, please contact:



Rob Deans

Partner

E: rob.deans@clydeco.com

T: +971 4 384 4538



Rob Deans consistently provides clients with a high-quality service and strong commercial understanding of their business.

Chambers Global 2015



Joycia Young

Partner

E: joycia.young@clydeco.com

T: +971 4 384 4589



Joycia Young is behind many of the region's most lucrative IP transactions.

WTR 1000 2015



Jon Parker

Head of Trade Marks

E: jon.parker@clydeco.com

T: +971 4 384 4638



...he is extremely approachable and commercial in his advice – nothing is too much trouble for him.

WTR 1000 2014

www.clydeco.com

Key Law Federal Law No. 5/2012

On Combating Cybercrimes

Includes a range of new offences:

IT Security, State and Political Stability Offences

Hacking IT networks to steal data or change websites.

State Security, Dignity and Political Stability Offences

Unauthorised access to Governmental electronic systems, terrorism and organised crime through electronic systems.

Morality and Proper Conduct Offences

Using electronic systems to offend religious sanctities or encourage sins, provide pornography or gambling activities and slander.

Financial and Commercial (or Ecommerce) Offences

Forging and using forged electronic documents, obtaining goods fraudulently, producing and using debit or credit cards.

Keeping IT Safe

The UAE has upgraded its cybercrimes legislation to take account of technological and social change. Our expert panel considers the level of protection now given to investors.

“Federal Law No. 5/2012 created a range of new offences and imposed stricter penalties than under previous legislation (which was known as Federal Law No. 2/2006 or Concerning Information Technology Crimes) to combat information technology crimes in the UAE,” Victoria Woods of Hedef & Partners notes. “It has amended, refined, and expanded on many offences in the previous law.”

“For example, under Article 2 of the old law, the offence of wilfully accessing a website or information system illegally or by overstepping permitted access required an element of intent. Under the new legislation this is no longer needed for an offence to have been committed,” says Woods.

“The offence’s scope has also been broadened so that electronic sites, including social networking sites, blogs and personal pages (such as Facebook, Twitter and Instagram) are expressly now covered. In this developing field, perhaps some of these changes are intended, at least in part, to ensure the capture of new innovations in technology and commerce and new trends in social media.”

“The 2012 law on cybercrime also created additional categories of offences and added to social, cultural and moral crimes.”

“There are new express provisions on pornographic materials, gambling activities and materials which prejudice public morals, and we now

have expanded provisions regarding insulting others, harming the reputation of the State, exposing the State to security risk and promoting the weapons trade.”

DOES THIS LEGISLATION PROTECT INVESTORS?

“The UAE has been proactive in enacting specific legislation which deals with the very modern threat of cyber bullying and trolling while other jurisdictions generally tend to rely on broader legislation, like anti-harassment laws to address these issues,” says Payam Beheshti of Clifford Chance.

“Federal Law No. 5/2012 was introduced to bolster protection against cyber crimes. It covers a wide range of offences and provides greater certainty on the specificity of the crimes and their enforcement through significant fines and jail terms. For example, the mere act of recording conversations or saving photographs even when these are not published is prohibited.”

“Although we have yet to see if there is scope for the courts or legislature to impose some limiting factor on this given the difficulties in treating all these activities as criminal,” Victoria Hambly of Clifford Chance adds. “In view of increased online and other social media service usage, the 2012 Cyber Crime Law goes some ways to providing protection to the community and investors from becoming cybercrime victims.”

“However, due to the laws’ wide application and the fact that a person does not need to have any negative intention in their use of audio visual equipment or social media, individuals could find themselves inadvertently breaching this law,” Beheshti says.

“There are provisions in this law which criminalise a number of the most common privacy infringe-



Payam Beheshti
Senior Associate, Clifford Chance

“The UAE has been proactive in dealing with the very modern threat of cyber bullying.”



ments," says Mohamed Hamdy of Baker & McKenzie. "For example, Article 10 prohibits the disruption of electronic communication by spamming email. While Article 15 makes it an offence for people to intentionally and without permission capture and/or intercept communications online."

WHAT ABOUT PUNISHMENT?

"Another change investors may be pleased to see is the fact the 2012 law provides more specific and

notably more severe punishments, including imprisonment and fines.

There are sanctions of up to life imprisonment (for offences regarding overthrowing the State, changing the regime in the UAE or obstructing the provisions of the Constitution) and fines of up to AED 3 million (for offences relating to viruses)," says Woods.

"It's a much more rigorous framework with a tougher stance and harsher punishment. Although, while legislative provisions may act as a deterrent to perpetrators of these crimes, they alone cannot prevent the crime itself from taking place. Practical protections and technological safeguards like fire walls are still needed."

WHAT ADVICE WOULD YOU GIVE TO PROSPECTIVE INVESTORS?

"It is very important to be aware of what this law covers and make sure your internet usage is acceptable," Hambly notes.

"In particular, businesses that use social media sites (like Facebook and Twitter) should be aware of not only the content they publish themselves but also anything posted by customers on their site."

"There may be a risk businesses could be held accountable for their own and their customers' posts so it's wise for businesses to make sure user generated content is moderated before appearing on their company's social media pages," Beheshti adds.

"Both investors and the wider community should take the same level of caution in their actions online as they would in other areas of their life in the UAE."

HOW DO YOU REPORT OFFENCES?

"If a cybercrime has taken place in the UAE, there is a clear system of reporting this sort of incident," Woods explains.

"For example, in Dubai, there is a Cyber Crimes Department within the Police force."

"The Dubai Police urges cyber-crime victims (including those who have been victims through social networking sites like Facebook or Twitter) to approach the authorities to report instances of such crimes in order to help tackle the reported increase in the number of cyber crime cases in the UAE."

"However, as we all know, the internet is a global forum, so while the

UAE legislative framework may offer victims in the UAE, a clear route for reporting this sort of crime, with severe sanctions for identified offenders, the provisions of the UAE law on Cyber Crimes may not be capable of aiding in the prosecution of perpetrators overseas," Woods notes.



Victoria Woods
Senior Associate, Hadeef & Partners

"It is a much more rigorous framework with a tougher stance and harsher punishment. Sanctions include life imprisonment."

Penalties Federal Law No. 5/2012

On Combating Cybercrimes

Includes a range of new penalties such as:

Passwords and access without permission

Under Article 14 which covers use of confidential numbers, codes or passwords used to access any electronic site the penalties for use without permission are either imprisonment and/or a fine not less than AED 200,000 but not more than AED 500,000.

Unlawful credit card and bank access

Article 12 which covers unlawfully access to credit card numbers, electronic card numbers, bank account statements and electronic payment method details, is relevant to those who either intend to use such information or do use it to obtain funds belonging to third parties. They face prison sentences of at least six months and/or a fine not less than AED 200,000 but not more than AED 1,000,000.

Right in a moveable asset

Among the various offences created under the Cybercrimes Law, there is an offence against obtaining a right in a moveable asset, benefit or document through fraudulent methods with reference to signature, use of a false name or impersonation of a false capacity. The punishment for this is imprisonment for at least one year and a fine of no less than AED 250,000 and no more than AED 1 million.

IS THERE A CROSS OVER BETWEEN CYBER-CRIME LEGISLATION AND DATA PROTECTION?

"The UAE Cyber Crimes Law did create some new data protection measures when it came into force in 2012."

"For example, this law states a person who gains unauthorised access to a website or IT system and amends, deletes or discloses any data or information is subject to additional penalties if the information is personal," Dino Wilkinson of Norton Rose Fulbright states.

"The Cyber Crimes Law does not actually define what 'personal' is in this context, but it is likely to cover areas involving a person's private or family life (which are protected under the Penal Code) and potentially the other personally identifying sorts of information which are often protected by international data privacy laws."



Victoria Hamby
Associate, Clifford Chance

password or any other means of accessing an IT system without legal right, or using a computer network or IT system to invade another person's privacy (unless it is permitted by law) by eavesdropping, interception, recording or other specified means, is also treated this way."

CREDIT, BANK, PAYMENT CARD PROVISIONS

"Article 12 which covers unlawfully access credit card numbers, electronic card numbers, bank account statements and electronic payment method details, is relevant to those who either intend to use such information or do use it to obtain funds belonging to third parties. They face prison sentences of at least six months and/or a fine not less than AED 200,000 but not more than AED 1,000,000," Hamdy notes. "Under Article 14 which covers use of confidential numbers, codes or password used to access any electronic site the penalties for use without permission are either im-

prisonment and/or a fine not less than AED 200,000 but not more than AED 500,000," Hamdy says.

"These are fairly substantial deterrents in the context of online activities which could pose a risk to personal data. However, unfortunately, the Cyber Crimes Law alone does not create the framework for specific rights and civil remedies which would generally be available to data subjects under other international data protection regimes," Wilkinson explains.

DO YOU THINK THAT IT SAFE TO USE ELECTRONIC SIGNATURES IN THE UAE?

"Federal Law No 1/2006 (or the E-Commerce Law) provides where a rule of law requires a signature to be subscribed to a document, an electronic signature that is reliable within the meaning of the specific criteria set out within the E-Commerce Law generally satisfies that requirement," Yasmene Aweti of Hadeef & Partners explains.

"In terms of the use of electronic signatures within the UAE, Federal Law No. 1/2006 does provide a comprehensive set of criteria which can be used to determine if an electronic signature is reliable within the meaning of the law, and if it is a protected signature. This is a complex subject and so it is worth taking legal advice depending on the circumstances of the particular case. While, the law cannot guarantee the safe use of electronic signatures in the UAE, it offers some protection."



Yasmene Aweti
Partner, Hadeef & Partners

RECOGNISED SERVICE PROVIDERS

"There is one more point of note on this question. Secure electronic signatures must be issued by recognised service providers in order to qualify as secure and reliable electronic signatures under the law," Hamdy adds.

WHAT ARE THE KEY DATA PROTECTION OFFENCES?

"There are also other specific offences in the Cyber Crimes law involving data protection," Wilkinson notes.

"These include obtaining, possessing, modifying, destroying or disclosing electronic data about medical examinations, medical diagnosis, medical treatment or care or medical records without authorisation."

"Having unauthorised access to credit or electronic card numbers or data or to bank accounts, numbers or data or any other electronic payment method or unauthorised interception and/or disclosure of communications through an IT network are also offences under this piece of legislation," Wilkinson adds.

"In addition, obtaining any secret number, code,

Now IT's personal

As UAE data protection legislation is more dispersed than in some jurisdictions, our **expert panel** provides a guide to the key places to find it.



“Data protection is a topical area in the UAE at the moment. A new Dubai law on the subject was announced towards the end of last year,” explains Mohamed Hamdy of Baker & McKenzie.

WHAT'S THE SCOPE OF THE NEW DUBAI DATA LAW?

“This new law aims primarily to take data gathered by Dubai Government entities and store it in a 'Data Bank' which will be accessible to and shared between Government entities, with the private sector and the wider economy to enhance the Government's E-government vision,” Hamdy explains.

“However, its application is limited to Dubai and

it doesn't have Federal application. Its primary aim is data collection and providing a credible data source to Government institutions and the public.”

COULD IT HELP DUBAI BE A SMART CITY?

“In recent months, there have been press reports about the Government's initiative to transform Dubai into the first Arab 'Smart City'.”

“Through the use of new technologies to link together different aspects of society, such a move could fundamentally change the way our work and private lives inter-relate. It is possible the new Data Law is being introduced to support that vision,” explains Victoria Woods of Hadeef & Partners.

Key UAE data protection laws

Federal Laws

Certain provisions on privacy of the individual are found in the UAE Penal Code (Federal Law No. 3/1987) which provide the legal basis for data protection in the Emirates. However, these provisions don't specially envisage the types of technological advancements typical in data protection. A number of other Federal Laws such as the Medical Liability Law (Federal Law No. 10/2008) and the Credit Information Law (Federal Law No. 6/2010) also restrict personal information use in specific circumstances.

Dubai Laws

Another key law is Dubai's new Data Law (which has recently been published in the Official Gazette) and aims at ensuring Dubai Government entities effectively share open data but it does not relate to identifiable persons so hasn't provisions on identifiable natural persons or personal data provisions. As at the time the interviews were carried out this law had not been officially published so it was unclear if it would fully protect personal data in some way as is the case with EU laws such as the EU Data Protection Regulation.

Freezone Laws

The Dubai International Financial Centre (DIFC), Dubai Healthcare City (DHCC) and Abu Dhabi Global Market (ADGM) have their own comprehensive legislative regimes including specific data protection provisions, which apply to companies established in those zones. The DIFC Data Protection Law is modelled on the EC Directive 95/46 and aims to ensure the fair, lawful and secure treatment of an individual's personal data, while striking a balance between a data subject's right to control, access and use their personal data against the collection and use of such personal data for legitimate purposes.

IS PERSONAL DATA PROTECTION FULLY COVERED BY THE NEW LAW?

"This is a new law (which was not publicly available when these interviews took place). From press reports it seems that rather than providing a data protection regime for personal information the new Dubai Data Law is geared towards creating a framework which facilitates the exchange of 'open data', that is, non-confidential data, between Government and other entities," Yasmene Aweti of Hadeef & Partners notes. "It has been reported it will contain data protection provisions, but the extent to which this is the case is not yet known."

HOW DOES EXISTING LAW WORK?

"In Dubai, it is important to draw the distinction between the UAE 'onshore' regime and the framework for governing data in the DIFC freezone. The DIFC operates its own discrete data protection regime that is distinct from that of onshore UAE," Hamdy adds.

"There is no single piece of legislation in onshore UAE, similar to that in the EU but individuals have various statutory protections afforded to them on data protection contained within domestic federal legislation. Although, these may not be as readily identifiable as they would be under a 'data protection law', the UAE does have legislation for the strict protection of personal information and in fact, the principle of a right to privacy of such information is enshrined in the UAE Constitution itself."

WHAT CHANGES DO YOU EXPECT FROM THE NEW LAW?

"Hopefully, the new Data Law will provide some useful guidance on helping identify what is, and what is not, 'personal' data. As it is intended to enable non-personal data to be shared, it will need to explain exactly what makes data suitable for sharing," Hamdy notes.

WHAT WILL THE CHALLENGES BE?

"The most obvious is that while data which doesn't relate to identifiable natural persons is now the subject of a law, there is still a question around personal data relating to identifiable natural persons. We need to know if we can also expect legislation setting out the requirements entities processing personal information on identifiable people must comply with."

"The key obstacle around data collection and processing will be the criteria for data to be classified as personal or non-personal which may then constitute a clear breach of the invasion of privacy regulations," Hamdy notes.

DO YOU THINK THESE ISSUES COULD BE OVERCOME?

"In many jurisdictions which already have implemented open data policies, a challenge that has been faced seems to be balancing open data with an individual's right to privacy. This could be overcome by adopting a robust infrastructure with clear guidelines to help reduce the potential risks of users breaching data protection, which could be mitigated by requiring the redaction of any personal data that may be contained in the open data," Aweti adds.

WHAT ABOUT QUALITY AND SAFEGUARDS?

"In terms of how the exchange, use and re-use of open data will take place, it will be interesting to see what data protection provisions may be contained within the Dubai Data Law, as well as whether any safeguards will be adopted to uphold an individual's right to privacy. Other practical obstacles may include quality control of the open data and ensuring it is reliable," Aweti notes.

"Whether users can easily use the data (e.g. if it is technical or complex is also key, as is whether the main sources participating in data sharing have the resources to effectively do so."

HOW DO YOU RATE UAE DATA PROTECTION?

"The existing UAE Federal law provisions on personal data protection, particularly those in the Penal Code, provide strong protections for individuals and perhaps more causes of action than in some other jurisdictions with distinct data protection laws," says Victoria Woods of Hadeef & Partners.

HOW WILL THIS NEW LAW HELP?

"The new Law will need to provide a framework for non-personal data to be shared, this means that the law must explain exactly what makes data suitable for sharing. In doing so, it will be necessary to provide a framework for categorising whether data is personal or sensitive."

"Indirectly, this may provide some useful guidance when analysing data protection related issues in the Emirates," says Hamdy.



Mohamed Hamdy
Senior Associate, Baker & McKenzie

Definitions

Personal Data

'Personal data' is any information relating to an identified or identifiable natural person usually. As in the EU Data Protection Directive, EU Directive 95/46/EC an identifiable person is one who can be identified, directly or indirectly, particularly by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Examples can include an individual's name, home address, age, race, blood type, income, marital status, education, and employment status.

Open Data

'Open data' is basically understood as data that can be freely used, redistributed by anyone, uninhibited by technical interoperability issues or the absence of a common approach to data categorisation. Its aim is to create greater knowledge from larger data sources and volumes and see new patterns in data, which can lead to innovation in products and services, or enhanced efficiency.

Right to be Forgotten

Right to be forgotten is the right to delete data if retaining it lacks a legitimate reason. There is no such right in the UAE.

Authorities

Freezones

The DIFC Commissioner of Data Protection is responsible for administering the DIFC Data Protection Law and Regulations in that freezone.

Federal

There is no onshore data protection authority.

Dubai

A Dubai Open Data Committee was reportedly appointed to strike a balance between the availability and sharing of open data and the upholding information security.

A sectoral view

The Credit, Telecoms and Health sectors all have specific data protection regulation issues to face, as our **expert panel** explains.



Offences

Federal

There are no general data privacy provisions under the Civil Code which permit private individuals to seek compensation directly for breaches of their privacy rights but there are useful provisions in various other Federal Laws.

The UAE Constitution

provides for freedom of communication 'by post, telegraph or other means' and guarantees the right to secrecy of these communications.

Federal Law No. 5/1985 (or Civil Code) makes a person liable for acts causing harm generally, which could include harm caused by unauthorised use or publication of another person's personal or private information.

Federal Law No. 3/1987 (or Penal Code) sets out offences involving the publication of matters relating to a person's private or family life, the unauthorised disclosure of secrets entrusted to a person by reason of their profession, craft, circumstance or art and the interception and/or disclosure of correspondence or a telephone conversation without the relevant individual's consent. Punishment for these offences can include fines and/or imprisonment.

Federal Law No. 5/2012 (or the Cyber Crimes Law) contains certain offences including particular types of personal data in electronic or online contexts.

Both the Penal Code and the Cyber Crimes Law set out criminal offences but do not directly confer rights upon individuals on the misuse of their data.

However, Federal Law No. 35/1992 (or the Criminal Procedures Law) permits people who sustain a direct personal injury from a crime to pursue their civil rights before the criminal courts during the criminal proceedings. This may give scope to seek compensation for damage suffered as a result of misuse of personal data.

Organisations collecting personal data must consider data subjects' needs. They may need to verify this data with specific organisations, like Dubai Customs in cases where export and import figures are indicated and in certain sectors, there are specific laws and regulations addressing privacy rights in particular areas.

BANKING & FINANCE

The key legislation in this area is Federal Law No. 6/2010 (or the Credit Information Law).

HOW DOES THE AL ETIHAD CREDIT BUREAU HANDLE DATA PROTECTION?

"Federal Law No. 6/2010 (or the Credit Information Law) established the Al Etihad Credit Bureau," Dino Wilkinson of Norton Rose Fulbright explains.

"Under this law one single source issues credit information reports to lenders by disclosing the individual's financial details, in particular prospective borrowers' credit worthiness. As a result, Al Etihad Credit Bureau has the exclusive right to request, collect, keep and analyse financial data."

"The bureau's aim is to safeguard the UAE economy," Mohamed Hamdy of Baker & McKenzie adds. "It was established to develop the financial structure and add transparency and clarity to the borrowing process and individual debt levels. It is hoped it will help banks better assess risks they take in lending to individuals or facilitating the KYC (Know Your Client) when determining individual creditworthiness."

"The Credit Information Law also regulates collection of financial data on a person, their financial commitments, current and prior payments, financial rights and details of their creditworthiness."

"These elements called 'Credit Information' are the basis on which credit records and credit information reports are prepared," adds Wilkinson.

"According to Article 5 of Federal

Law No. 6/2010, 'the gathering and circulation of information and data directly or indirectly related to the details or facts of a private life of a natural person, or the opinions, beliefs or health thereof shall be prohibited,' Wilkinson notes.

"A person's consent must also be obtained before issuing credit information reports and there are various restrictions on the use of information gathered for this law's purposes."

"These and other obligations in Federal Law No. 6/2010 provide a level of protection for personal data but only in the narrow context of credit information."

"This is also reinforced by sanctions including imprisonment and/or fines for those who disclose or acquire credit information, reports or records other than in line with the law or who breach confidentiality or intentionally distort data or submit incorrect credit information to the Bureau," Hamdy explains.

"Consent is signed pre-approval by not only the individual but also the company (in the case of lending institutions or any other entity authorised to obtain credit reports from the Al Etihad Credit Bureau) on individuals or companies and must be in writing."

HEALTH CARE

In this sector there are a range of rules at Federal, Emirate and Free-zone level.

WHAT BODIES GOVERN DATA PROTECTION?

"The Dubai Health Authority is responsible for the healthcare sector in Dubai. Its Hospital Regulation 2012

determines medical negligence and generally guides medical practitioners. However, the Health Record provision of these rules, in particular, cover the management of healthcare information and patients' medical records. Another key law in this area is Federal Law No. 10/2008 (or the Medical Liability Law) which ensures patient information is treated confidentially and protected from any kind of disclosure, loss or destruction," Wilkinson explains.

"The Medical Liability Law is useful in providing protection against disclosure of patient's medical data," Hamdy says.

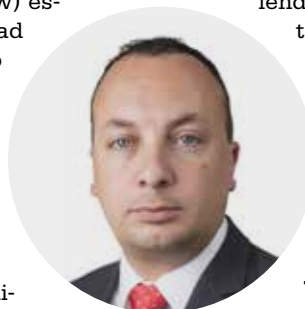
KEY EXEMPTIONS?

"Article 5(5) has restrictions on disclosure of patients' secrets which a doctor becomes aware of while practising or because of their profession. This is the case either if the patient trusts them with the secret or the doctor becomes aware of one."

WHAT IS A DOCTOR'S DUTY?

"The doctor's duty to protect patient information is an ancient one, derived the Ancient Greek Hippocratic Oath. In many countries doctors must take the Hippocratic Oath as part of their medical training," adds Rosalind Meehan of Jones Day.

"While the Hippocratic Oath has a core commitment to patient privacy, it also recognises there are



Dino Wilkinson
Partner, Norton Rose Fulbright

circumstances where information a doctor learns during treatment should be disclosed, and laws regulating medical records specify these circumstances.”

WHAT ARE THE MEDICAL LIABILITY LAW DISCLOSURES?

“Under the Medical Liability law, patient data can be disclosed if:

- a patient requests it,
- it is in the interest of a husband or wife and is notified personally to either of them, or
- it is to prevent or report a crime, and disclosure is made to an official authority.”

“It is also allowed when a doctor is assigned by a judicial authority or official investigation authority in the state as an expert or if they are summoned as a witness in an investigation or criminal case.”

“Doctors assigned by life insurance companies or employers to make examinations, can also disclose if their disclosure does not exceed the purpose of the assignment. Recognising many patient records will be kept electronically, the Dubai

Health Authority has recently established an Electronic Medical Record Executive Board and Steering Committee to oversee the implementation of electronic records across the Emirate.”

DUBAI HOSPITALS

“In Dubai, patient records are covered by the Medical Liability Law as well as the Hospital Regulations,” Meehan adds.

“The Hospital Regulations also focus on the need to maintain the accuracy of health records.”

“They state, ‘This health record is a legal document which should accurately outline the total needs, care and management of patients. It facilitates communication, decision making and evaluation of care and protects patients, physicians and hospitals.’ Medical records are expected to be complete and accurate. Section 52.4 of these Regulations provides a detailed list of the information every health record should include.”

“The Regulations also contain detailed requirements that all hospitals must maintain a records management policy and system to ensure the secure, safe and systematic storage of data and records and the destruction of records when they are no longer required. Finally, to avoid confusion, section 55 sets out the medical record retention requirements.”



Rosalind Meehan
Trainee Solicitor, Jones Day

Specific Sectoral Laws

There are no general data privacy provisions under the Civil Code which permit private individuals to seek compensation directly for breaches of their privacy rights but there are useful provisions in various other Federal Laws.

Telecommunications

The Telecommunications Regulatory Authority’s Consumer Protection Regulations issued under Federal Decree-Law No. 3/2003 (or the Telecommunications Law) requires telecoms operators to protect the privacy of subscriber information.

General

Federal Law No. 8/1980 (or Labour Law) requires certain types of employee data to be protected.

Banking and Finance

Federal Law No. 6/2010 (or the Credit Information Law) covers credit information.

Medical

Federal Law No. 10/2008 (or the Medical Liability Law) covers patient records.

DISCLOSURE FOR RESEARCH

“Dubai Healthcare City also has its own set of regulations on health data, the latest set of which is in the Health Data Protection Regulation (Dubai Regulation No. 7/2013). These are different from the Medical Liability Law and the Hospital Regulations as they allow disclosure on an ongoing basis for research and statistical business.”

They expand on the circumstances in which medical records can be disclosed beyond the exceptions in the Medical Liability Law if that disclosure is made on an anonymous basis,” says Elizabeth Robertson of Jones Day.

“This includes disclosure of information which would benefit the wider public. This could include:

- for statistical and research purposes;
- to prevent or lessen a serious and imminent threat to the public, the life or health of the individual patient or another individual;
- to enable professionally recognised accreditation of a healthcare facility for a professionally recognised external quality assurance programme; and
- for risk management assessment.”

LESSONS FROM THE UK

“In 2012, the UK NHS unveiled proposals for data gathered by them anonymously in order to provide better healthcare and aid medical research which could have some for Dubai. That programme, called ‘care.data’s’ aim was to build a database of anonymous data gathered from general practice surgeries across the UK to generate better under-

“The UK experience of ‘care.data’ on use of medical data as part of an open data programme may be instructive to Dubai’s health care regulators as they seek to grow its reputation as a world-class treatment centre.”

standing of diseases and develop drugs and treatment."

"They also hoped to understand patterns and trends in public health and disease to ensure better quality care; to plan services and NHS budgets; compare health across different areas in the UK and monitor drug and treatment safety. The plan was to gather patient data from GPs, make the data anonymous and store it in a database. Although data was to be anonymous, it was felt the programme would not be publicly acceptable if patients were not given an opportunity to consent to the use of their medical data."

"The 'care.data' team proposed consent be on an opt-out basis, meaning patient data could be used unless the patient actively refused permission."

"However privacy campaigners, supported by many doctors, argued patient data should only be included in the 'care.data' programme on an opt-in basis. The 'care.data' team noted people seldom opt-in to the use of their personal data, and an opt-in rule would mean a much smaller database."

"Such has been the controversy over the consent process and whether it should be opt-out or opt-in the 'care.data' pilot programmes were halted for the fourth time in September 2015. They will remain on hold until further guidelines for the protection of patient data are released, which is expected early in 2016. This experience may well be instructive to Dubai healthcare regulators as they seek to grow Dubai's reputation as a world-class centre for healthcare treatment and research."



Elizabeth Robertson
Partner, Jones Day



Joycia Young
Partner, Clyde & Co

TELECOMMUNICATIONS

In the telecommunications sector, the key concern is around the control of spam which is not limited solely to email.

WHAT DATA PROTECTION REGULATIONS HAVE BEEN ISSUED IN THE

TELECOMS SECTOR?

"One key piece of the regulatory framework in this sector is the Telecommunications Regulatory Authority's (TRA) Consumer Protection Regulations which were issued on 30 January 2014 replacing a number of earlier policies including the Privacy of Consumer Information Policy. These Regulations apply to all licensees providing public telecommunications services in the UAE. These licensees must also ensure their agents and representatives'

comply with them," says Wilkinson.

"Article 12 of the Regulations contains general obligations on the privacy of subscriber information. Licensees must take all reasonable, appropriate measures to prevent unauthorised disclosure or use of subscriber information. If a licensee has access to subscriber information as a result of interconnection with another licensee, the first licensee is strictly prohibited from using that information for any purposes other than interconnection. In particular, the Regulations state such information may not be used for marketing purposes."

ARE THERE ANY MARKETING OBLIGATIONS?

"In addition, Article 16 covers marketing obligations and practices. There are obligations around the content of marketing messages including their truthfulness, substantiation of claims and legality."

"However, while there is a requirement that marketing communications and practices shall not be 'unduly intrusive' under Article 16.25, there is no specific prohibition on sending unsolicited marketing messages."

ARE THERE SPAM RESTRICTIONS?

"The TRA has a separate regulatory policy on unsolicited electronic communications or spam which was issued on 30 December 2009," Wilkinson says.

"This applies to all electronic communications originating in the UAE or from an individual or company physically located in the UAE, accessed from a device in the UAE or if the recipient is physically present here. Licensees had to comply with the Policy by 30 June 2010. It places them under a general obligation to put 'all practical measures' in place to minimise the transmission of unsolicited electronic messages or spam. This Policy contains detailed principles for consent, although Government entities are excluded from its application."

WHAT WAS THE AIM?

"It is designed to minimise transmission of spam to and from the UAE. Under the Policy, telecommunications service providers in the UAE, i.e. Etisalat and Du, must minimise spam and take all reasonable steps to ensure it is not being transmitted over

"When using unsolicited marketing communications obtain consent from as many customers as possible before sending any marketing messages."



their networks,” Joycia Young of Clyde & Co notes.

WHAT IS A UAE LINK IN THIS CONTEXT?

“If a licensee (i.e. 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 their network, the regulator can take action against the licensee,” Hamdy adds.

WHAT ABOUT DATA STORAGE?

“There are protections around storing certain consumer information. Telecommunication service providers are specifically prohibited from ‘address harvesting’ which means collecting, capturing and compiling electronic addresses by using software, tools, technologies or other methods. In terms of consumer protection and spam, the TRA Protection Regulations include rights for the non exploitation of consumers as well as provisions concerning consumer complaints and disputes handling,” Yasmene Aweti of Hadeef & Partners notes.

“The Policy also prohibits telecommunication service providers from being involved in the process of obtaining email address or mobile number lists for spam purposes,” says Young.

“However, this does not apply to electronic communications sent by Government entities.”

HOW IS SPAM DEFINED?

“Under the Unsolicited Communications Policy, spam is defined as ‘marketing electronic communications sent to a recipient without their consent’, while marketing electronic communications are ‘advertisements, promotions, offers for goods/services or any other purpose designated by the TRA’,” explains Aweti notes.

WHAT ARE THE SPECIFICS?

“Under the policy, there are specific rules on consent and how consent is retained, including rules for:

- ‘opt-in’ and ‘opt-out’ procedures,
- ‘subscribe’ and ‘unsubscribe’ options.”

“The types of communication covered by the Policy are broad.”

“A Mobile Spam Annex to the Unsolicited Communications Policy describes ‘opt-in’ and ‘opt-out’ requests, necessary consents and other requirements involving mobile telecommunications (like SMS & MMS).”

“Again, the intention is to stop unsolicited marketing via MMS/SMS messages”, Aweti notes.

WHAT ELSE IS COVERED?

“It is important to remember these rules do not just apply to emails but any electronic communication conveyed through the telecommunications net-

work to an electronic address. This could include:

- emails;
- URL;
- ISP; and
- telephone numbers.”

HOW SPECIFICALLY DOES CONSENT WORK?

“Prior consent by marketing message recipients is not expressly required before sending them a marketing communication. However, the TRA may investigate complaints from consumers who receive unsolicited marketing communications,” Young explains.

ARE THERE ANY SPECIFIC PENALTIES ?

“While the policy includes no specific penalty, the telecommunications service providers have wide discretion to suspend access to network services if they consider it appropriate.”

“Under Federal Decree-Law No.3/2003, the TRA can also issue fines of between AED 50,000 and AED 200,000. People can also be faced with custodial sentences of up to one year for failing to take all practical steps to prevent spam from being sent over their network.”

WHAT WOULD YOU ADVISE BUSINESSES TO DO?

“It is good practice when using unsolicited marketing communications to obtain consent from as many customers as possible before sending any marketing messages, giving customers the chance to ‘opt-in’,” Young notes.

“If unsolicited marketing messages are sent it is worth ensuring initial messages include a request for consent, as well as any promotional or marketing information or offers.”

POINTS TO NOTE ON CONSENT AND BEST PRACTICE

“You should also ensure anyone who refuses consent is not contacted again. That can mean maintaining consent records so you can track and prove who has consented.”

“Finally do not send messages to individuals between 9pm and 7am.”

“It is also important to provide details of how an individual can change their mobile or application settings to block notifications, and how to unsubscribe from marketing campaigns.”

JUST TELECOMMUNICATION SERVICE PROVIDERS?

“Although the Unsolicited Communications Policy is geared towards telecommunication service providers, the overriding principle appears to be aimed at preventing spam altogether, and telecommunication service providers are charged with seeking to prevent the use of their network for these activities,” Aweti adds.

“You should ensure those who refuse consent are not contacted again which can mean keeping consent records.”

“The aim is to stop unsolicited marketing messages via MMS or SMS messages.”

Industry View

The Telecommunications Regulatory Authority

HE Majed Al Mesmar of the Telecommunications Regulatory Authority explains the regulator's view on spam and privacy protection.



“ The Telecommunications Regulatory Authority (TRA) has issued the Consumer Protection Regulations (CPR) which are designed to protect telecommunications service users in the UAE's interests.

DOES THE PRIVACY OF CONSUMER INFORMATION POLICY HELP RESTRICT SPAM?

The policy was designed with the aim of protecting telecommunication services consumers, and this is clearly highlighted in the below rules:

- Subscriber contracts must have clear terms and conditions particularly on prices and billing.
- There is protection against unannounced price increases by licensees.
- There is protection against misleading advertisements.
- There are provisions on service activation and deactivation to ensure subscribers are not provided with unwanted services.

WHAT ABOUT PRIVACY OF SUBSCRIBER INFORMATION?

To address the point most relevant to this question, this policy does require privacy of Subscriber Information. Subscriber Information is defined as any personal data about a specific Subscriber and includes, but is not limited to:

- that person's name;
- call records;
- message records; and
- telephone number.

UAE licensees must take all reasonable and appropriate measures to prevent the unauthorised disclosure, or unauthorised use to Subscriber Information.

ARE THERE ANY OTHER REQUIREMENTS FOR LICENSEES?

There are additional requirements, licensees need to be aware of including:

- they must limit access to Subscriber Information to their trained and authorised personnel;
- they must obtain a Subscriber's prior consent be-

fore sharing any Subscriber Information with third parties; and

- if subscribers ask the licensee to disclose their own Subscriber Information to them, they must disclose it free of charge and without delay.

This basically means Subscribers have the right to obtain their own Subscriber Information on request.

WHAT ABOUT CONSENT?

The ability, or otherwise, of licensees to disclose Subscriber Information turns on consent. Disclosing Subscriber Information without prior consent is a breach of the Regulatory Framework.

HOW ARE CONSUMERS PROTECTED AGAINST SPAM?

In line with the TRA strategy to offer a spam free mobile experience to all UAE subscribers, the Authority has announced more proactive measures to control and minimise unwanted promotional text messages (Spam SMS) received by mobile phone subscribers in the UAE. After recent data showed most unwanted promotional messages come from international companies located in GCC countries, and in coordination with Etisalat and Du, the TRA introduced a monitoring device which can identify and block advertising messages from outside the UAE. In the case of advertising messages originating from the UAE, the TRA enforces a strict auditing process so repeat offenders could risk their service being temporarily terminated after an initial warning. They could also be subjected to a fine and permanent cease of service if they reoffend.

This new measure complements a full set of initiatives already in place. At the end of 2009, the TRA established a regulatory policy that applied to both licensees (Etisalat and Du) which aimed to dramatically reduce marketing messages sent to customers without their consent. There was a clear focus on mobile SMS. This policy is still binding on both service providers who have been given instructions to take appropriate measures to fight spam and to give consumers the choice of receiving such messages or not.

“Repeat offenders could risk their service being temporarily terminated after an initial warning.”

Cyber Security & Data Protection

Roles & Responsibilities

With so many laws making up the UAE regulatory framework in this area, Nick O'Connell of Al Tamimi & Co provides a run-down of necessary roles and responsibilities.

The UAE Federal government, local governments and Government entities, have all recently released laws and policies aimed at ensuring appropriate security measures are implemented. It is also not uncommon for organisations in many sectors, including Government entities, to require specific, objective information security standards to be applied within their organisations. In addition, technology customers also often require technology vendors to comply with specific information technology standards when providing technology products and services.

GOVERNMENT SECTOR

In the Government sector, some organisations have their own information security policies which require compliance with standards, like ISO standards. However, Government sector entities must also be aware of, and comply with, the specific information security laws and regulations which apply to them. For example, Cabinet Decision No. 21/2013 Concerning the Regulation of Information Security in Federal Authorities (or the Federal Information Security Resolution) provides a framework for ensuring security of information in federal agencies. It basically covers email, internet and system security and storage and backup.

Email Security provisions cover issues like passwords (including mobile device security), spam, and statements of offensive, discriminatory or slanderous nature. The provisions in this category can be summarised as follows.

- **Personal email** use, including Yahoo!, Gmail, Hotmail is prohibited.
- **Mobile devices** connected to Federal agency IT systems must activate security lock option.
- **Distribution of spam**, personal, commercial, religious, political or charitable communications are forbidden.
- **Offensive, discriminatory and slanderous statements** are not allowed.
- **Hacking and introducing virus programmes** into IT systems are also covered.

There are also provisions on Internet security, aimed primarily at preventing internet use for activities which are inconsistent with public morals and good conduct. These include activities like

accessing banned sites, promoting racism or contempt of religion and being involved in activities which could harm IT systems. There are also provisions aimed at ensuring system security including virus control, the use of hardware and software assets and Federal Authority network and IT equipment. These create restrictions around installing unlicensed or non-standard software, and failing to monitor mail for viruses and malware.

Finally, there are storage and back-up provisions e.g. back-ups are required before and after software and application changes and external data storage mediums cannot be used without consent.

As well as Federal Government rules, there are also rules like Dubai Executive Council Decision No. 13/2012 Regarding the Information in the Government of Dubai (Dubai Information Security Resolution) which have been passed in the Emirate.

This Decision refers to 'Government Bodies' as being 'Government departments, entities, public institutions, councils and authorities, including free zone authorities and any other authority affiliated with the Government of Dubai'. However, it does not provide clear guidance on the type of 'entities' it applies to, so there may be ambiguity (e.g. if the entity is a Dubai Government owned company).

Meanwhile, the Abu Dhabi Government Information Security Policy and related Abu Dhabi Government Information Security Standards (known as the 'AD Information Security Policy') applies to entities 'wholly owned' by the Government. This has requirements for ensuring critical Government information is secure regardless of the medium it is in. All Abu Dhabi Government entities must:

- categorise their information assets (including information systems) based on the importance and the asset's critical nature;
- develop an Information Security Programme Plan; and
- build required capabilities to monitor information systems and manage information security incidents in the entity.

They must also regularly report to the Abu Dhabi Systems and Information Centre (ADSIC) who are responsible for assisting Government entities in implementing their respective Information Security Programme Plans.

CYBER CRIMES LAW

Federal Law No. 5/2012, referred to as the Cyber Crimes Law, provides for a range of offences largely focusing on information security. This law prohibits unauthorised access to an IT System to obtain Government or commercial information. This prohibition specifically mentions Government information. Additionally, it refers to information relating to financial, trade or economic establishments licensed in the UAE. There is a prohibition on circumventing an IP address in order to commit or conceal a crime.

The scope here is potentially very broad as it could refer to masking IP addresses from which a major hacking attack is launched but could also potentially extend to the likes of using an off-shore VPN to access pirated or unlicensed content from abroad, which may be of less interest to the authorities on a day-to-day basis, but would still appear to be covered.

Although, the Cyber Crimes Law prohibits obtaining, IT system passwords without permission, it does not specify that obtaining these passwords has to occur via an IT system. The language seems broad enough to cover obtaining it via an IT system but there is also a broad prohibition on making available (whether directly or by procuring, including by importation or sale, any means or information designed to commit/facilitate/incite others to commit crimes specified under the law.

Unauthorised interception of communications via an IT system is also prohibited which seems to mirror the provision on intercepting communications in the UAE Penal Code and (in the case of phone calls) the UAE Telecommunications Law. The act of disclosing information gathered this way is also covered. 'Wikileaks' type situations are captured by a prohibition on unauthorised disclosure of confidential information via an IT system. This would include cases where workers who obtain confidential information in the course of their employment release it without authority.

EXTRA-TERRITORIAL APPLICATIONS

There is a provision on the extra-territorial application of the Cyber Crimes Law, which (as paraphrased) states:

"Without prejudice to the provisions of Chap-

ter Two of Part (2) of Book (1) of the Penal Code, the provisions of this Decree by Law shall apply on any person who committed any of the crimes mentioned abroad, if its subject was an [IT System] of the Federal Government or one of the Local Governments of the Emirates of the State or any of the public authorities or institutions belonging to any of them." This focuses on cases where an offence involves UAE federal/local Government IT Systems, or IT systems of Government related entities. It does not appear to extend to cyber crime scenarios which are not linked to UAE Government or related entities. There are also provisions in the Penal Code on extra-territorial application, which generally provide that a crime shall be deemed committed on the State's territory if one of the acts constituting it has been committed thereon or if its results have been or were intended to be produced thereon. So, it may be possible to argue such extra-territorial provisions in the UAE Penal Code apply generally to offences created by the laws of the UAE, including the Cyber Crimes Law. Only the Public Prosecutor may institute a criminal action against an individual who has committed a crime abroad. If the Public Prosecutor institutes an action against an individual abroad, the issue of whether the specific (cyber) crime would be considered committed on the state's territory would be subject to a technical expert's determination. From a practical perspective, whether a Public Prosecutor decides to institute a criminal action against an individual who has committed a crime abroad will likely depend on the facts. If an individual outside the UAE hacks into a UAE bank's IT network and misappropriates customers funds, they may be more interested in doing so than, if someone outside the UAE sends spam email to UAE residents.

The Police and the Public Prosecutor are primarily responsible for investigating complaints involving alleged cyber crimes in the UAE. However, the UAE Computer Emergency Response Team (aeCERT) and the National Electronic Security Authority (NESA), are understood to be addressing cybercrime at a higher level. aeCERT established in 2008, is one of the Telecommunications Regulatory Authority's (TRA) most important initiatives and aims to provide a safer cyber environment to UAE internet users. It tries to improve information security standards and practices and protect IT infrastructure in the Emirates. Meanwhile, NESA estab-

"There is no comprehensive legislation in the UAE specifically designed to regulate personal data."

lished by Federal Law No. 3/2012 is responsible for electronic security generally in the country. It has supervisory authority over federal and local government entities and can issue legislation on information security. It is also responsible for organising communication network, UAE information systems protection, for improving systems and processes involving information systems and digital/electronic exchange of information. NESAs suggests digital security policy, prepares a national plan for dangers or threats, ensures public and private sector communications networks are efficient and fights various IT crimes. There seems to be some overlap between aeCERT and NESAs roles. However, as NESAs was established more recently, it could become the more dominant entity.

DATA PROTECTION IN THE UAE

There is no comprehensive legislation in the UAE specifically designed to regulate the collection, processing, transfer and/or use of personal data. Data protection issues are considered with reference to broad privacy provisions found in a variety of laws including the Penal Code (specifically Article 379) which generally prohibits the disclosure or use of secret information without the consent of data subjects, or some other legal authorisation. This is often used as the basis for legal

“Data protection issues are considered with reference to broad privacy provisions found in a variety of laws including the Penal Code.”

analysis on processing personal data in the UAE. However, this general prohibition, was not drafted with modern data protection in mind. The legal analysis, typically involves trying to determine if the information was likely to be considered ‘secret’ (which may not be the case), or if adequate consent has been obtained. Depending on the facts, it may be reasonable to conclude that relevant authorities are unlikely to consider Article 379 to be applicable in the context of

commercial data protection queries. Anecdotally, it seems Article 379 regularly forms the basis of ‘domestic’ instances of breach of privacy (e.g. claims about circulating indiscrete photographs on social media). However, we are not aware of criminal complaints or prosecutions involving use or disclosure of ‘secrets’ arising from mundane commercial personal data processing.

FREEZONES

The Dubai International Financial Centre, a free-zone established in Dubai, has a European-style data protection regime. The DIFC Data Protection Law (DIFC Law No. 1 of 2007), as amended, is applicable within the jurisdiction of the Dubai International Financial Centre. It contains requirements relating to the processing of personal information, including the transfer of personal information out of the DIFC, and provides for a complaint process and penalties for non-compliance. The DIFCs Commissioner of Data Protection is primarily responsible for

enforcing the Data Protection Law, and the DIFC Courts also have a function. The Commissioners broad powers, extend to promoting awareness and good practice, considering complaints and issuing admonishments and fines. Under the Data Protection Law, Data Controllers must notify the Commissioner of the type of Personal Data it processes, and the nature of its processing. This happens when they first register in the DIFC and each time registration is renewed. DIFC entities must also notify the Commissioner when they change the way they process Personal Data. Transfers outside the DIFC are permitted in certain circumstances, e.g. if the recipient’s location is considered, by the Commissioner, to provide adequate data protection, transfer is permitted. The Commissioner has a list of

permitted jurisdictions, mainly European countries. If a jurisdiction is not considered adequate, transfer is only permitted if conditions are met, one of which is the Data Subject’s consent, or if the Commissioner has issued a permit allowing the transfer. Interestingly, the UAE outside DIFC is not considered a jurisdiction with an adequate level of data protection. The Dubai Healthcare City’s Health Data Protection Regulation No. 7 of 2013 (the DHCC Health Data Protection Regulation 2013) can also be considered a ‘European-style’ data protection regime. It is less comprehensive than the DIFC Data Protection

Law, and focuses specifically on “Patient Health Information” (including personal information and medical information which relates to a patient’s physical or mental health). The DHCC Health Data Protection Regulation 2013 applies to entities licensed in the Dubai Healthcare City free zone. Abu Dhabi Global Market, a new financial services free zone established in the emirate of Abu Dhabi, has recently issued a European-style data protection regime based largely on the DIFC Data Protection Law. It contains requirements relating to the processing of personal information, including the transfer of personal information out of the ADGM free zone, and provides for a complaint process and penalties for non-compliance. There is currently no federal ‘Commissioner of Data Protection’ type role in the UAE. It is possible the TRA should be the authority primarily responsible for developing data protection rules and regulations at a federal level. The Telecoms Law states it shall exercise its functions and powers to among other things ‘encourage, promote, and develop the telecommunications and information technology industries in the State’. It is also responsible for data protection issues in the context of telecommunications subscribers. NESAs may develop a role in this area, although the extent to which they will become heavily involved remains to be seen.

TECOM

Finally, under Dubai Law No. 1/2000 the TECOM Authority is responsible for researching and advising the Dubai government on the regulation and encouragement of technology, electronic commerce and media in Dubai, including on data protection.



Nick O'Connell
Partner
Al Tamimi & Co

Maximilian Schrems v Data Protection Commissioner

Schrems caused regulators to rethink the approach to EU/US personal data transfers. **Elizabeth Robertson** and **Rosalind Meehan** of **Jones Day** look at its implications for the UAE.

On 6 October 2015, in Case C-362/14 Maximilian Schrems v Data Protection Commissioner, the European Court of Justice ("ECJ") invalidated the European Union–United States data protection "Safe Harbor," which had been implemented pursuant to an agreement between the US Government and the EU Commission in 2000. The "Safe Harbor" enabled the US to satisfy the EU Directive's requirements on the transfer of personal data to jurisdictions outside of the European Economic Area (EEA). The Safe Harbor had been an often-used mechanism, with

more than 4,000 US businesses signed up to receive electronically stored personal data from the EU. The Schrems case was filed by an Austrian law student, Maximilian Schrems, challenging an Irish Data Protection Commissioner's determination that the existence of

transfers made under the Commission decisions adopting Standard Contractual Clauses for data transfers from the EU to other jurisdictions (Decision 2004/915/EC and Decision 2010/87/EU) (the "SCCs").

EU IMPLICATIONS

Overnight, as a result of this decision, it became clear that the rubric for transfers of personal data between the EU and the US had to be fundamentally re-thought. It was also clear that the response to Schrems highlighted one of the big issues faced by the EU Directive – that national data protection authorities may provide different and conflicting advice on what businesses needed to do to continue transferring personal data to the US. For example, the SDPA (the Spanish data protection authority) has given Spanish businesses relying on the Safe Harbor until 29 January 2016 to replace their transfer measures, noting that transfers under the SCCs require an SDPA authorisation.

However, the UK Information Commissioner has indicated UK data exporters should review arrangements with their Safe Harbor data importers to confirm the importers are in fact providing adequate protection. If so, the Safe Harbor principles can remain part of a compliant regime. As an alternative, the SCCs may be used without the need for an authorisation. Meanwhile, the EU's Article 29 Working Group, which aims to set EU-wide standards on data protection issues, has confirmed that the SCCs remain in place to support data transfers to the US, but this is subject to the SCC provisions that allow national data protection authorities to review the adequacy of the protections surrounding the data transfer itself.

WHAT ABOUT THE UAE?

The Safe Harbor invalidation and the review of SCCs is not just an EU/US issue. It also has implications for EU/UAE data transfers and transfers from some freezones in the UAE to the US. Because most data transfers from the EU to the UAE are based on SCCs, any general review of the SCCs will affect those transfers. Unlike the EU, the UAE does not

Case Detail

Citation

Case C-362/14, (2015) All ER (D) 34 (Oct)

Hearing date

6 October 2015

Court

European Court of Justice

the Safe Harbor precluded the Irish agency from stopping Facebook's data transfers from Ireland to the US through the Safe Harbor, even though Facebook was allegedly providing information to the US intelligence services in violation of EU data protection laws. The ECJ invalidated the Safe Harbor on the grounds it failed to provide adequate protection to personal data transferred from the EU to the US, as was required by the EU Directive. The ECJ also made clear that data protection authorities in EU Member States are entitled to examine whether a data transfer to a third country complies with the EU Data Protection Directive requirements, even if the transfer is claimed to have been made under the terms of a Commission decision. This would include the right to review

have a comprehensive federal data privacy law. Instead, personal data and privacy protections are contained within other laws, including the UAE Constitution, the UAE Penal Code, the UAE Electronic Transactions and E-Commerce Law, the UAE Labour Law, the UAE Cyber Crime Law and the Medical Liability Law. If EU regulators look at the UAE system, they may not be persuaded these various laws provide the level of comprehensive protection required by the EU Directive. As a result, UAE businesses will want to carefully watch any systematic review of the SCCs that base a finding of adequate protection on a recipient country having a legal framework that matches the EU data protection's framework.

FREEZONE IMPACT

UAE businesses will need to argue convincingly that the combination of UAE laws with the measures the individual businesses take under the SCCs provide the necessary adequate protections to support data transfers from the EU to the UAE. The Schrems case will also have an effect in three UAE freezones: the Dubai International Financial Centre ("DIFC"), the recently established Abu Dhabi Global Market ("ADGM"), and the Dubai Healthcare City ("DHCC"). Before Schrems, these freezones enacted specific data protection and privacy regulations, namely the DHCC's Health Data Protection Regulation No. 7/2013, and the DIFC's Data Protection Law DIFC No. 1/2007 (amended by DIFC Law No. 5/2012) and Data Protection Regulation (Consolidated Version No. 2 in force on December 23, 2012). The ADGM also recently enacted the ADGM Data Protection Regulations 2015, which came into force on 21 October, 2015. Like the EU Directive, these regimes restrict the transfer of personal data to recipients located outside of the freezones, again based on the receiving jurisdiction providing adequate protection. The adequate protection for transfers to the US was the Safe Harbor, so by invalidating the Safe Harbor in the EU, the ECJ may have also (and potentially unknowingly) invalidated its use in these UAE freezones.



Rosalind Meehan
Trainee Solicitor, Jones Day

However, as in the EU, the freezone regulators' approach to Schrems is not uniform. On 26 October 2015, the DIFC Data Protection Commissioner issued guidance on the case's implication, which noted the EU Directive continues to be a model for general guidance in the administration of the DIFC Data Protection Law and invalidation of the Safe Harbor had created a cause for reconsideration of the adequacy status previously afforded to US Safe Harbor recipients. They recommended personal data transfers to the US should rely on the alternative data transfer mechanisms provided for in Article 12 of the Law until there is more clarity from the EU-US negotiations on improving the Safe

Harbor framework. Article 12 has similar exemptions to those in the EU Directive, where the data subject has given written consent to the transfer, where the transfer is necessary to perform certain contracts, or where the transfer is necessary to comply with legal obligations. Although Article 12 does not expressly provide for the use of the SCCs, the Commissioner has previously issued guidance that the use of these will be taken as evidence that an organisation is applying adequate safeguards when the Commissioner is considering whether to grant a permit.

For businesses operating in DHCC, Part 9 of the Health Data Protection Regulation states personal data transfers may only be made to an outside jurisdiction if that jurisdiction is listed as acceptable under the DIFC Data



Elizabeth Robertson
Partner, Jones Day

Protection Law or has written DHCC Central Governance Board approval. If guidance is issued that the Safe Harbor invalidation removes the US from the list, DHCC businesses will need the written approval of the DHCC Governance Board to make US transfers. For ADGM businesses, the ADGM Registrar has yet to issue guidance following the invalidation of the Safe Harbor by the ECJ, so it is still unclear whether the US will be deemed to be a jurisdiction with

an adequate level of protection for businesses operating out of the ADGM. However, Section 4(2) of the Regulations does appear to offer scope for self-assessment by data controllers as it provides a non-exhaustive list of circumstances in which the level of protection may be deemed adequate. These include the nature of the personal data, the purpose and duration of the proposed processing, the country of origin and final destination, and any relevant laws to which the recipient is subject. Businesses may therefore be able to make a decision themselves whether the recipient of the data transfer is subject to an adequate level of protection. As an alternative, businesses may be able to use the standard form ADGM data transfer agreements, which are annexed to the Regulations. The effect of Schrems has been to move data transfers regulated by the use of the Safe Harbor to being regulated under SCCs. To show the SCCs provide adequate protection to avoid invalidation under the logic of Schrems, EU data protection authorities will want to demonstrate the SCC process is more robust than the Safe Harbor regime. With the ECJ confirming they have the authority to do so, EU data protection authorities will not shy away from looking at the protections supporting high profile data transfers and will encourage EU-based data exporters to look carefully at the practices implemented by their data importers. Now is a good time for every data importer in the UAE who has signed an SCC to review their own compliance, and if necessary, to update the protections provided to personal data imported from the EU. Recipients of data from the DIFC, the ADGM, or the DHCC must also be aware that rules on data exports may be tightened.

DDoS Attacks & Cyber Extortion: Growing Risks

With evidence of growing risks of cyber extortion, **Monty Raphael QC** of Peters & Peters, Chair of the International Bar Association Cybercrime Sub-committee considers the potential risks to law firms.



“An organisation’s website is essential to its ability to compete. In the digital age, websites are our most important marketing tools. They are a first port of call for our future customers and an important source of information for existing ones. A reliable web presence, is fundamental to the key business functions of companies who fall within the wide-ranging definition of ‘online service provider’, but it is also integral to the success of companies who provide services offline. Whether you’re an online bank, a consumer goods manufacturer or even a law firm, a website that doesn’t work properly means bad client service.

“Regardless of your ethical stance, paying extortionists identifies your company as one that is willing to negotiate with criminals.”

Unfortunately, this is just as obvious to cyber criminals as it is to digital marketers. As cheap, pre-packaged cyberattacks become increasingly available on the dark net, it is easier than ever for hackers to target company websites, disrupt or disable their services and demand a ransom in return for restoring them to normal. Usually, this is done by a Distributed Denial of Service (DDoS) attack, where multiple systems are

used to overwhelm the intended victim’s website with applications, causing a denial of service. Once a criminal has established their capacity to carry out such an attack, the threat alone may be enough to persuade their victims to pay up.

There is good reason to believe such attacks, combined with extortion, are on the rise. The Kaspersky DDoS Intelligence Report Q3 2015 identified - DDoS attacks targeting financial organisations for the purpose of extortion - as a main trend and focused in particular on the activities of DD4BC, a criminal organisation alleged to be responsible for numerous attacks on banks around the world. However, banks are far from being the only targets. Recently, there have been high profile attacks on email

providers and other online companies, allegedly carried out by a cyber gang known as the Armada Collective.

Suffering a DDoS attack is expensive. The Imperiva 2014 DDoS Impact Report, which surveyed 270 North American organisations, found the average cost of an attack was US\$40,000 per hour. As a result, simply paying the ransom often works out as far cheaper than withstanding a lengthy attack. In fact, the Kaspersky report stated that the financial institution targets of the DD4BC criminal group were asked to pay 25 – 200 bitcoins, the equivalent of \$6,500 - \$52,500, so it is easy to see how in some circumstances, giving in to blackmail may appear to make commercial sense.

Of course, circumstances are never that simple. Regardless of your ethical stance, paying extortionists identifies your company as one that is willing to negotiate with criminals, a potentially lucrative target for other would-be attackers. There is also no guarantee of safety from non-financially motivated follow up attacks. For example, encrypted email provider ProtonMail recently paid a criminal organisation to stop a DDoS attack on their server, only to be then hit by a far more sophisticated and damaging attack, perpetrated by another attacker. This attacker made no ransom demands and it is unclear they they were motivated by amusement, glory or a desire to punish ProtonMail for giving in to the first attacker’s demands. Over the past few years, law firms and their regulators have demonstrated an increased awareness of the cyber risks that face the legal profession. However, that awareness has focused almost exclusively on data breaches and online fraud. This needs to change. When it comes to DDoS extortion attacks, law firms face the same risk as many other businesses. That risk is growing. Although the majority of us do not yet offer online services, we rely on our websites to communicate with the outside world. In addition, as the legal profession begins to exploit opportunities for growth provided by technology, that reliance, and our attractiveness as targets, will increase.

It is only a matter of time before one of us falls victim.

HADEF & PARTNERS

Abu Dhabi | Dubai

A FIRM OF TALENTED AND DIVERSE
LAWYERS A FIRM WITH DEPTH OF
KNOWLEDGE AND STRENGTH IN THE
MARKET PLACE A FIRM THAT BUILDS
LASTING RELATIONSHIPS

Banking & Finance
Commercial
Corporate
Dispute Resolution
Employment
Engineering & Construction
Financial Services
Government Regulation
Hospitality & Tourism
Insurance
Intellectual Property
Maritime, Transport & Trade
Mergers & Acquisitions
Private Equity
Projects, Infrastructure & Energy
Property
Restructuring & Insolvency
Technology, Media & Telecommunications

www.hadefpartners.com

To Post... or Not to Post?

In the time it takes you to read this article, there will have been over 2,500,000 tweets on Twitter and nearly 750,000 Instagram photos posted. **Payam Beheshti & Victoria Hambly** of **Clifford Chance** look at the interplay between privacy and social media.

The recent explosion of online activity has led to UAE legislators introducing new laws to directly protect our on-line privacy and prevent the use of legislation which pre-dates the rise of social media in ways the original lawmakers could not have imagined. However, despite this reform, a very public struggle between the rights to freedom of speech and the right to privacy has unfolded in the Emirates.

WHAT ARE WE TRYING TO PROTECT?

Generally, privacy means the right of individuals to keep certain information about themselves to themselves. In any jurisdiction, privacy may be regarded as a societal norm or a protected legal right but it will always be a culturally relative concept. The various ways different people interpret the concept of privacy, comes to the fore particularly in the UAE where people from a wide range of cultures live, work and socialise together. In fact, the UAE provides a unique location in which to test the traditional Western-centric concept of privacy in a legal system which was founded on and developed by different standards.

In many jurisdictions, it is not uncommon for the right to freedom of expression, to be raised as a defence to claims of breach of privacy, e.g. in cases where paparazzi photographers try taking and publishing images of celebrities. In practice, navigating the line between these two culturally relative rights, that of privacy and of freedom of expression becomes even more complex in a culturally diverse place like the UAE, where the boundaries of what is permissible under the protection of the right to freedom of expression before you start to encroach into your fellow residents' privacy rights is particularly difficult to ascertain.

A clear example of these difficulties arose recently when an Australian expatriate in Abu Dhabi was fined and deported for 'writing bad words on social media' after posting a photo on Facebook which, had it been posted in her home country, would not have made readers think twice about a possible breach of privacy there. The photo showed a car, without a disabled badge, parked across two disabled parking bays. The picture did not show the car registration plate, any names or identifying features. So it is clear there is a need in multicultural societies like Dubai and the wider UAE to establish a framework which can be easily followed by all residents. This is particularly important when the risks of getting it wrong and falling foul of UAE privacy laws can lead to large fines, jail time and even deportation.

HOW IS PRIVACY PROTECTED?

In the UAE there are a suite of laws which protect privacy as a fundamental right, e.g. the UAE Constitution entrenches the right to confidentiality of communication (whether by post or otherwise) in Article 31. The UAE Penal Code (Federal Law No.

3/1987) also sets out a number of defamation and privacy offences such as Article 372 which prohibits publishing anything which could expose the victim to public hatred or contempt, while Article 373 prohibits false accusations which cause dishonour or discredit someone. In addition, Article 378 prohibits publishing of any news, pictures or comments which may reveal the secrets of peoples' private or family lives, even if the published material is true and in the public interest. However, these Penal Code offences have a slightly more limited scope than the new Cy-

bercrime law because the person publishing the statement must have had an intention to reveal private information or to cause harm.

In contrast, the Cybercrime law penalises a much



Payam Beheshti
Senior Associate, Clifford Chance



wider range of activity online. For example, Article 21 makes it an offence to 'assault the privacy of a person' online in any of the following ways:

- Overhearing, interception, recording, transferring, transmitting or disclosing conversations, communications or audio or visual materials;
- Capturing pictures of third parties or preparing electronic pictures or transferring, exposing, copying or keeping those pictures; or
- Publishing electronic news, pictures, photographs, scenes, comments, statements or information even if they are correct and real.

Given the ease of making recordings or taking photographs and publishing them on social media, simply at the touch of a button, it is possible to fall foul of this law. The law also includes certain

other actions, such as accidentally overhearing a private conversation or privately storing photographs taken of others even if they are never published, which are such passive ac-

tions it is not clear how people can best avoid committing them, particularly as unlike the Penal Code offences, the intention to assault an individual's privacy is not required. Each of these offences carry serious penalties including fines in the region of AED 150,000 to AED 500,000, deportation of foreign nationals and/or imprisonment.

COULD MY NEXT SOCIAL MEDIA POST BREACH PRIVACY LAW?

The scope of UAE privacy laws can mean that a seemingly innocuous social media post could theoretically constitute a breach of privacy, defamation and be deemed an offensive publication all at once. So should we stop using social media?

From recent local news reports, it appears a number of non-malicious acts have been caught by these

laws. There are a number of cases which highlight the need to be cautious. A man was prosecuted for defamation for posting a video of a friend and his family sleeping on Instagram without consent. An American citizen who published a parody of Dubai youth culture online was also charged with infringing another cyber security provision which makes it an offence to publish information which could expose state security or prejudice public order. In addition, a group of public officials are also currently awaiting trial for breach of privacy laws for installing CCTV cameras without adequate cause. Recent reports even suggest the Dubai Police considers these offences can even be extended to the simple act of using offensive 'emojis' online.

THE OFFICIAL POSITION?

The UAE Telecommunications Regulatory Authority (TRA) has recently published guidance in a white paper on the appropriate usage of various social media and online communication platforms. The guidance suggests for people to take appropriate caution when posting material online and consider if a post could cause offence or breach an individual's privacy. They also outline the requirement to obtain consent before posting photos of, or tagging another person on social

media, and highlight the importance of ensuring your own security settings are up to date and have not been shared with others. These official publications and the prevalence of public officials' usage of social media in the UAE show that keeping an online presence isn't being discouraged as such. However, keeping an appropriate balance between protecting citizens' privacy and not restricting an individuals' freedom of expression is not an easy task. It is encouraging to see the UAE being proactive in creating new laws which address the needs of our increasingly online lives, although, we should also heed the warnings which have been given and remain sensitive to our cultural environment.



Victoria Hambly
Associate, Clifford Chance

"In multicultural societies like Dubai a framework which can be easily followed by all the residents is needed."

Cybersecurity and Data Protection A Broader View

As cybersecurity and data protection, are global issues, **Sana Saleem** of **Al Tamimi & Company** looks at how these issues are being tackled internationally and by other jurisdictions.



“The International Organisation for Standardisation has developed various information security standards which set out a broad framework for the management of information security.”

First it is important to make sure the terminology is clear.

The term ‘cyber security’ can sometimes be used interchangeably with the term ‘information security’. Information security relates to processes and methodologies designed and implemented to protect information or data from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

Some people may see cyber security as being specifically associated with information security in the context of ‘cyberspace’, which can be broadly understood as referring to the internet, or the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure.

However, we will generally use the terms interchangeably, with ‘cyber security’ being used more to refer to information security in the context of the internet, and particularly in reference to criminal offences associated with the use of information technology tools, networks and systems.

DATA PROTECTION AND CYBERSECURITY

Data protection primarily relates to the administrative or organisational protection of personal data relating to individuals by entities which hold such data for legitimate purposes. In some ways, it can be understood as a ‘consumer protection’ type concern.

The relationship between data protection and cyber security is essentially that personal data is one of many types of information or data which needs to be protected from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

DEFENCES AGAINST CYBER SECURITY RISK

Information security mechanisms and procedures often involve a balance between security, cost and the usability of an organisation’s technology infrastructure.

The various ways of defending against threats to information security can be broadly categorised as either being:

- technology-based defences (use of encryption, appropriate structuring of IT systems or penetration testing of IT systems);
- process based defences such as adopting standards that enhance security;
- people-based defences including having adequate training on security in an organisation.

INTERNATIONAL STANDARDS

An important aspect of cyber security and risk management is defining appropriate procedures and protection requirements for the information. The International Organisation for Standardisation (ISO), the world’s largest developer of standards has various information security related standards which set out a broad framework for the management of information security.

Relevant ISO standards include:

- **ISO 27001** Information Technology – Security Techniques – Information Security Management Systems – Requirements. This specifies the requirements establishing, implementing, maintaining and continually improving on information security managements systems within the context of the organisation.
- **ISO 27002** Information Technology – Security Techniques – Code of practice for Information Security Management. This gives guidelines for organisational information security standards and information security management practices.
- **ISO 27017** Information Technology – Security Techniques – Code of practice for information security controls. This is based on ISO-IEC 27002 for cloud services.
- **ISO 27018** Information Technology – Security Techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

It is not uncommon for organisations in various sectors (including the commercial and governmental sectors) to require specific information security standards, such as those issued by the ISO to be followed within their organisations.

It is also not uncommon for technology customers to require technology vendors they are purchasing from to comply with specific information technology standards when delivering information technology products and services.

THE BASICS OF DATA PROTECTION

In the 1970s, with the arrival of powerful computer systems, which were capable of automatic data processing, large quantities of data were able to be processed and transmitted within seconds.

This led to demands for specific rules to be created governing the collection and handling of personal information.

There was a belief that privacy concerns needed to be balanced with the risk that restrictions on data flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

As a result, the early regulations tried to tackle these issues.

DATA IN QUESTION

When considering data protection, the data in question is ‘personal data’.

This broadly means information which relates to an identifiable natural person.

SENSITIVE PERSONAL DATA

However, within ‘personal data’, there is a data sub-category often called ‘sensitive personal data’. This could include information about things like:

- racial or ethnic origin,
- political opinions,
- religious beliefs,
- membership of trade unions,
- physical or mental health,
- sex life, and
- criminal records.

In modern data protection regimes, the processing of sensitive personal data is often subject to

stricter requirements, reflecting the sensitive nature of this type of information.

WHAT IS PROCESSING?

The 'processing' of personal data can include various activities, including obtaining, recording or holding the information or data, or carrying out any operations on the data.

This may cover organisational adaptation or alteration of data, retrieval, consultation or the data's use, disclosure by transmission, dissemination or otherwise making it available.

It may also involve alignment, combination, blocking, erasure or destruction of data.

The concept of data protection was developed to strike a balance between an individual's right to privacy and the ability of organisations, including community, commercial and government organisations, to use personal data for reasonable purposes.

OECD GUIDELINES

In 1980, the Organisation for Economic Cooperation and Development (OECD) issued Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (known as the OECD Guidelines).

The OECD Guidelines were intended to advance the free flow of information between OECD member countries while avoiding the creation of unjustified obstacles to the development of economic and social relations among these countries.

They set out specific principles for the protection of personal data, including:

- **Notice:** data subjects should be given notice when their data is being collected;
- **Purpose:** data should only be used for the stated purpose and not for any other;
- **Consent:** data should not be disclosed without the data subject's consent;
- **Security:** collected data should be kept secure from any potential abuses;
- **Disclosure:** data subjects should be informed about who is collecting their data;
- **Access:** data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- **Accountability:** data subjects should have a method available to them to hold data collectors accountable for not following these principles.

Directly or indirectly, modern data protection laws are often generally based in principle on these concepts which were expressed in the OECD Guidelines. However, the OECD Guidelines, were non-binding.

THE EUROPEAN APPROACH

In Europe there was concern that data privacy laws varied widely from country to country. So in 1995,

the European Commission issued Directive 95/46/EC (known as the EC Data Protection Directive), which provided a standard upon which EU Member States were required to base their own domestic data protection legislation.

The EC Data Protection Directive was intended to harmonise EU Member States' data protection laws in order to provide consistent levels of protections for citizens and ensure the free flow of personal data within the EU.

However, as diverging approaches to data protection have developed in various EU Member States since the Data Protection Directive was issued in 1995, but also because of the need to address significant technological and societal changes

which have occurred since then, such as the development of the internet and social media, the EU is currently updating its approach to data protection.

The draft General Data Protection Regulation, which should introduce a single framework of data protection throughout EU, is currently working its way through the EU legislative process.

If passed in its current form, it would introduce a number of new data protection concepts, and extend to processing, outside of the EU, of EU residents' personal data.

A main difference between the General Data Protection Regulation and the EC Data Protection Directive, would be as a Regulation, it would basically be adopted directly in the EU Member States, rather than acting as guidance upon which each state would use to develop its own legislation.

OTHER DEVELOPMENTS

Meanwhile, in July 2013, the OECD Council issued the Recommendation Concerning the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

These Recommendations have revised the OECD Guidelines in order to strengthen online data protection rights and boost the digital economy.

OECD MEMBERS

Data protection has received considerable attention in Europe, and many OECD member countries outside Europe have also introduced data protection legislation.

US DEVELOPMENTS

However, like the UAE, the United States does not have a unified data protection regime.

Instead, privacy has been regulated in an ad hoc manner, in certain industry sectors (e.g. patient health information in a healthcare context) or as local legislation in certain states.

To some degree, this could be a reflection of a lower appetite for government regulation, although things seem to be changing there too with a recent "State of the Union" address by US President Obama which focussed on privacy (along with information security issues), and could indicate an appetite for change there too.



Sana Saleem
Al Tamimi & Company

"Like the UAE, the US does not have a unified data protection regime. To some degree this could be a reflection of a lower appetite for governmental regulation."

Data Trends

With levels of data collection and processing increasing, **Dino Wilkinson** of **Norton Rose Fulbright LLP** considers the regional trends.

The collection and processing of data by a wide range of organisations is part and parcel of modern life. However, many privacy advocates are growing increasingly concerned about the ability for data to be used to monitor, make predictions about and substantially impact the lives of individuals. It is this which is acting as a driver for new and amended data protection legislation around the world.

Globally, the European regime deriving from EU Data Protection Directive 95/46/EC is widely

viewed as a high water mark for data protection legislation. European authorities consider privacy to be a fundamental human right and plan to further strengthen law in this area with the introduction of the General Data Protection Regulation, which would unify data protection across the EU and could see sanctions for companies in breach of up to 5% of the company's annual world-wide turnover.

UAE FREE-ZONE TRENDS

In the Middle East, there are relatively few comprehensive national data protection regimes. The UAE and other GCC states have not yet implemented any such wide-ranging privacy laws at national level. However, the UAE's financial hubs of Abu Dhabi Global Market (ADGM) and Dubai International Financial Centre (DIFC) have implemented European-style data protection laws, while Dubai Healthcare City (DHCC) has regulations governing the use of patient data.

These freezones have recognised that, in addition to safeguarding the rights of individuals, a data protection regime provides a framework to allow commercial organisations to collect and use personal data for legitimate purposes. The data

protection legislation in these centres has provided a degree of certainty for the businesses operating within them.

A number of jurisdictions around the world follow the European lead by imposing restrictions on the export of personal data outside their jurisdiction unless there is an 'adequate level' of protection offered in the recipient jurisdiction.

In fact, the rules in ADGM and the DIFC both contain a similar prohibition on transfers outside those respective zones. Since 2000, the EU Commission's 'US Safe Harbor' decision had permitted the transfer of personal data between European companies and the US by establishing that an adequate level of data protection was ensured by the EU-US Safe Harbor scheme.

On 6 October 2015, the European Court of Justice ruled in Case C-362/14 (the Schrems case) that the EU-US Safe Harbor scheme was invalid. The impact of the Schrems case has not been limited to Europe. In jurisdictions that adopted data protection laws modelled on the European system, such as the mentioned UAE freezones there is considerable uncertainty and there have been some changes to policy and legislation.

QFC TRENDS

The Qatar Financial Centre (QFC) Data Protection Regulations 2005 also include a restriction on transfers of personal data to recipients located outside the jurisdiction unless 'an adequate level of protection for that Personal Data is ensured by laws and regulations that are applicable

to the Recipient'. Unlike the DIFC and ADGM, the QFC Regulatory Authority has not prescribed a list of jurisdictions offering adequate protection for these purposes. Instead, Article 9(2) and the accompanying QFCA Data Protection Rules confirm that the data controller is responsible for making this assessment. The Rules recommend that data controllers consider all relevant circumstances including whether the jurisdiction in question is 'the subject of any finding or presumption of adequacy by another data protection regulator or other relevant body (such as the European Commission).



Dino Wilkinson
Partner, Norton Rose Fulbright

“In jurisdictions that adopted data protection laws modelled on the European system, there was considerable uncertainty and there have been some changes to policy and legislation.”



Although, so far as we are aware, no formal announcement has been made by the QFC regulator to date with specific reference to Schrems, it seems likely QFC entities will have to re-assess any prior findings of adequacy that they have made which relied on the Safe Harbour certification as the previous European Commission finding of adequacy has been invalidated.

“The UAE wants to position itself as a competitive knowledge economy with a number of initiatives under the Vision 2021.”

SMART CITY

The UAE wants to position itself as a competitive knowledge economy with a number of initiatives under the Vision 2021. For example, the Telecommunications Regulatory Authority (TRA) is co-ordinating the implementation of the National Plan to support smart govern-

ment initiatives with part of its remit looking at a ‘Smart Data’ strategy which would involve the sharing of data between government entities and a new open data regime.

In Dubai, the Dubai Open Data Committee was formed in 2014 to integrate and synchronise Dubai’s services on different levels. Part of its stated aims is to strike a balance between making data available and maintaining data security in line with the vision of the leadership to transform Dubai into a smart city.

These open data initiatives are part of a push to make information available for re-use by anybody with an interest in doing so. Typically this could be

entrepreneurs looking to utilise data sets for new purposes, public interest groups seeking information or citizens looking for data about their home city or country. A fundamental premise of open data is it may be freely used, re-used and distributed by person subject only, at most, to a requirement to attribute and share the results. It is also key that the focus is on non-personal data. This means that any information that identifies an individual should not be made freely available as part of open data.

As this area develops and more smart initiatives are introduced in the UAE, it will be important for legal and reputational reasons the authorities ensure that personal privacy is not adversely affected by this move. In order to help ensure this, the Dubai Open Data Law was announced in October 2015 and it is likely that we will see more legislation in this area being issued in the future in order to safeguard the rights of individuals and establish the boundaries for data use.

FUTURE LEGISLATION

A key turning point for the UAE and other GCC states would be the introduction of national privacy legislation. While there has been no official announcement or consultation on laws in this area yet at a federal level, several GCC states are known to be considering the implementation of data protection regulations. This would be an important step in the development of the region and would help to ensure individual privacy is protected while establishing a framework which would allow organisations to use personal data for legitimate purposes.



Key Precedent

Do I have the right to be forgotten?

The Internet, multinational firms and the rights of the individual, all make privacy and data protection considerations more complicated. *Sogol Kaveity* looks at the lessons from C-131/12.

Mr. CostejaGonzaláles did not like the fact that Google had made personal information about his house being repossessed following an auction notice in 1998 available to the public. In fact, he felt access to this information infringed his right of privacy and data protection.

As a result, he filed a complaint, claiming he had the 'right to be forgotten', in light of the time that had passed. In May 2014, in ECLI:EU:C:2014:317, C-131/12, the European Court of Justice ruled on the matter.

THE FACTS

On 5 March 2010, Mr Gonzaláles, a Spanish national, lodged a complaint with the Spanish Data Protection Agency against a local Catalan newspaper 'La Vanguardia', Google Spain and Google Inc, based on the fact that when his name was entered in the Google search engine, two articles from the newspaper in 19 January and 9 March 1998 would come up. These stories were about the auction of his house in order to recover social security debts at that time.

Gonzaláles asked first that the Catalan newspaper be required to remove or alter these articles. Then that both Google Spain and Google Inc be forced to remove or conceal personal data about him and that this personal information cease to be included in the search engine.

He argued that as the auction-proceedings had been fully resolved for a number of years the reference to them was now entirely irrelevant and an infringement of his right to privacy.

The Spanish Data Protection Agency had then taken the view that it had the authority to require withdrawal of this information and prohibit access to it.

However, Google Spain and Google Inc brought actions against this decision, and as a result the Spanish court referred the

case to the European Court of Justice for a preliminary ruling.

The questions were:

- **Applicability:** Did the EU Data Protection Directive apply to Google?
- **Territoriality:** Did the Directive apply to Google Spain as Google Inc is established in the USA?
- **Was there a right to be forgotten and what was its legal standing:** Did an individual have the right to request a search engine remove his personal data?

THE DECISION

On applicability, the Court ruled that search engines are controllers. Using a search engine to search an individual's name results in obtaining a list about an individual, enabling users to establish a more or less detailed profile of that person.

On territoriality, it was decided that EU data protection law did apply to Google. Personal data is processed on a Member State's territory when a search engine operator sets up a branch or subsidiary in that state in order to promote and sell advertising space offered by their search machine.

Finally, the Court decided an individual has the right to be forgotten when such personal data is inaccurate, inadequate, irrelevant and excessive in relation to the data processing purposes.

THE APPLICATION

In this case because of the time that had elapsed, since the auction, there was a right to be forgotten and interfering with data protection could not simply be justified by Google's economic interest. However, the right to be forgotten is not absolute.

A balance must be sought against freedom of expression and media, and the public interest. Google was required to make a case-by-case assessment when applying the European Court of Justice's judgment.



Barber&Co

SOLICITORS

Lexcel
Practice Management Standard
Law Society Accredited

For all your legal services



Barber & Co Solicitors was formed in 1996 by the Principal Solicitor, Mr. Arif Barber. The head office is located in Preston with a branch office in Darwen.

Our specialist solicitors (one of whom is a judge) are there to help you deal with a wide range of legal issues facing individuals and businesses in the UK and UAE.

WEB : www.barbercosolicitors.co.uk | **TEL :** 00 44 (0)1772 203520 | **E-MAIL :** a.barber@barbercosolicitors.co.uk

A woman with dark hair, wearing a black hijab and a black abaya, is seated in a black leather office chair. She is smiling and looking directly at the camera. Her hands are clasped together on a light-colored wooden desk in front of her. She is wearing a silver watch on her left wrist and a ring on her left ring finger. The background is a plain, light-colored wall.

“The fact that lawyers are exposed to a multiple of legal systems is amazing.”



“Arbitration provides assurance for foreign companies to invest in the UAE.”

The eldest of five children, Diana Hamade Al Ghurair comes from an intellectual background. Both of her parents were graduates and her father practiced law full time which meant he was rarely at home. However, Diana’s memories of him at home are of watching him work into the early hours in the morning in order to meet deadlines and submittals of pleas. Hamade’s mother meanwhile, had studied English Literature which meant Jane Austen and Leo Tolstoy were writers she chose to share with her children.

Although Arabic is Hamade’s mother tongue, she grew up in a multi-lingual house. Her father spoke French and her mother spoke English at home. As Hamade recalls, “My parents sent me to London for summer school to learn English from fourteen to sixteen and I stayed with English families. My parents were keen on providing me with the best education possible.”

At first Diana wanted to study journalism and be a TV presenter. However, her father didn’t think that was a good idea. He preferred her to study law.

“Studying law was not my first choice, my father forced me to go to law school,” Hamade confesses. “He believed I would be a great lawyer.”

In high school, Hamade ranked in the top ten of United Arab Emirates high school students, which helped. “I was given an open invitation by H.H. Sheikh Zayed Bin Sultan Al Nahiyen, late President of the UAE to attend law school in Al Ain University. While I was there there, I double majored in Sharia and Law and there were six women studying at the Faculty of Sharia and Law.” Hamade graduated with honours in 1990. She, then went on to continue her legal education and obtained LL.M. in International Commercial Law at Aberdeen University, in the UK in 1991. “During my studies in the UK I learnt common law rather than the civil law system we have in the UAE. That was challenging and intriguing. I also studied arbitration extensively in Aberdeen, which was relatively new then.”



CAREER

On her return to Dubai after completing her studies, she worked as an intern with Chadbourne Park & Afridi and Clifford Chance. However, after finishing her internships, Diana went on instead to open a translation office and at the same time, worked for Dubai TV. "My dream of becoming a TV presenter finally became a reality but I felt it was not exactly what I wanted to do for the rest of my life," she adds.

Between 2002-2005, Hamade joined the Dubai Chamber of Commerce where she had her first experience as an in-house counsel. "I remember the first contract I saw, and knew immediately that I loved the law. This was when I started my legal career," she explains. The move to the DIFC Authority, then enhanced her legal skills. "I had more laws to draft and more rules to review," she explains.

Then finally, in 2008 Diana opened her own law firm. She started with one lawyer and one secretary, but now has twelve people working for her (six lawyers and six staff members). Hamade's practice focuses on litigation and arbitration with a very small amount of criminal law cases. Hamade explains, "I am very selective in taking clients. I have to feel comfortable, I don't defend everybody."

INDULGING THE LAW

Hamade does not do marketing, but rather her practice is primarily built on word of mouth. People seek her advice and assistance. She makes many appearances at conferences and on radio and TV shows. For example, she regularly appears on MBC's the morning show to talk about legal issues in Arabic, and she has also appeared on BCC and CNN to discuss certain legal matters. She has also been a columnist for The National, and The Brief. In addition, Hamade writes for Al Sada Magazine and she recently wrote the UAE litigation chapter in the International Comparative Legal Guide and also contributed the International Family Law Guide. Hamade explains, "I don't do these appearances as an advertisement, but merely to share information. I love getting involved in debates and engaging with others in legal discussions. When I am at a conference, and people ask me questions I don't know, I make it a point later to study and examine the subject for my own knowledge and enrichment. The intellectual challenge intrigues me."

When Hamade was asked about her remarkable career and the dedication it takes to get to her position, she answers, "I never take myself seriously. I do everything in my life for fun. The competition is severe, but with a lot of hard work and sleepless nights and effort so you are always prepared will see you rewarded by success. The biggest challenge is to wake up the next day, and still be out there."

TWO LEGAL SYSTEMS

"The quality of UAE legal system is amazing. The Government is catering for everyone in this country

in order to provide them with the best service of the law. The Government is determined to give everyone a judicial system that adapts to their needs and backgrounds. It is amazing too to see that the judiciary is in line with the Government's vision. However, the biggest challenge people face in court is the language. The Dubai Government's vision was effectively realized with the set-up of DIFC courts. These courts were established to abolish the language barrier, but they do not cover criminal law or family law, just civil and commercial law."

Hamade was a member of the panel, which advised on the probate registry and inheritance for non-Muslims in DIFC courts. She was also asked by the DIFC courts to help with drafting the law on probate registry of non-Muslim wills.

"This is a great step, as the judiciary now enables non-Muslims to execute their wills in Dubai, and this will aid foreign investment."

Hamade is licensed to appear in all UAE courts. "The way lawyers here are exposed to multiple legal systems is amazing. As well as the courts in Sharjah, Fujairah, Ajman, Ras al Khaima and Um Al Quwain, having two different courts in Dubai (Dubai courts and DIFC courts), can make it very confusing for me as a lawyer to plea. In one day, I might appear in front of a sharia judge on an inheritance case where we debate and argue about Islamic jurisprudence. Then after that I have to appear in front of the civil court on a property case arguing the property law and civil transaction law. Then I have to go to DIFC courts to apply common law. As a result, the new generation of lawyers has to study both civil and common law so they can integrate the two systems into their practices."

At a Glance: Diana Hamde

Diana Hamade was born in Beirut and raised in Dubai. She graduated from Al Ain University with honours in 1990 and continued her legal education in the United Kingdom at Aberdeen University, where in 1991 she received LL.M. in International and Commercial Law. Since 2008 she has been the owner of International Advocate Legal Services in Dubai. She previously worked at the Dubai Chamber of Commerce from 2002 to 2005 and joined the DIFC authority from 2006 to 2008. Hamade has been awarded best legal writer by The National in 2011, and most influential female lawyer in the UAE by The Brief in 2012.

She is a member of the Arab Regional Forum Committee and a fellow of the International Academy of Matrimonial Lawyers and the Society of Trust and Estate Practitioners. Diana Hamade is married to Mr. Hamad Majid Al Ghurair and has three children.

"The way lawyers here are exposed to multiple legal systems is amazing."

THE VALUE OF LOCAL FEMALE ADVOCATES

Tina Brown recently invited Diana to speak at her forum 'Women of the World' in Dubai as a justice speaker, discussing women rights. There are about 100 local female advocates in the UAE and around ten of them own a law firm. When asked if women are discriminated against in practising law, she answers, "Women are not in any way discriminated upon in getting a law degree. On the contrary, the Government supports us by providing us with educational opportunities, and with personal privilege.

Clients prefer to go to a female lawyer. A lot of people believe a female will do her best just because she is challenged, and that's true, because I know from my own experience. I have to prove to the world that I am doing it right, so I make ten times the effort. I feel this every day, everybody questions me and because of that I put in more effort. I know that men trust women with what they do because women are very persistent." As a result, the majority of Hamade's clients are men and she says, "Men trust me be-

cause they know a female lawyer will always stand by their side."

ARBITRATION SYSTEM

Hamade feels in civil or commercial cases court fees are reasonable compared to the English legal system, where fees can be enormous and the losing party pays everything. Family law cases are free but Hamade thinks legal aid is what is missing in the UAE. "The challenge lies in legal representation. Except in criminal cases, we don't have a legal representation assistance system. This disadvantages women in family cases. Legal representation should be considered a high priority. Other countries provide legal assistance to their nationals and I would like to call upon the Government to provide legal assistance to the nationals who cannot afford it here. It is totally wrong to presume that all nationals can afford legal representation."

ACCESS TO JUSTICE

"We need a law to regulate the arbitration system," says Hamade. "There are twelve provisions in the civil procedure law that cover arbitration. The UAE has also signed the New York Convention and this gives foreign arbitral awards outside the Emirates a much better status because they are immediately enforced according to the New York Convention rules. However, a UAE arbitral award has no legal

standing, so the arbitration is now lawless."

"The UAE arbitration law has been pending for fifteen years and we have had seven drafts. A new law will make arbitration a valid ADR process with an enforceable judgment. Currently, everything goes for validation to the court and the court can look into the whole dispute again. They may even dismiss the arbitral, even though the parties have paid millions on arbitration. Of course the party who has to pay will ask the judge to invalidate. Arbitration provides assurance for foreign companies to invest in the UAE."

COMPANY LAW

However, Hamade also thinks the Government has done a lot to attract investors. "Investment has been flourishing because of the Government's vision around attracting businesses," she says. "We have the least bureaucratic system in the Middle East and South East Asia. Dubai is a hub in terms of rules and businesses. You can set up a business in two days. There is no bureaucracy." Recently the UAE passed the new commercial companies law (Federal Law No. 2/2015), which had been on the shelf for over a decade but Hamade also thinks the bankruptcy law, which is also being discussed, will also safeguard the business environment in the country. "However, what we are still missing and badly need is local family business succession laws," she adds. "If a pater familias dies, the business is inherited through the application of sharia law and this basically subjects the company to destruction. We need a law that will protect the family business sector from becoming dysfunctional. Currently, there are steps being taken towards putting in place family succession laws, but no law has yet been written. The UAE needs onshore family succession laws to keep local family companies from being dissolved. This is a huge threat to the economy given that 80 % of the companies here are such companies."

LAWYER SKILLS

When asked about what skills the lawyer should have, Hamade answers distinctly, "Debating and pleading". Although she feels UAE legal education is more based on tradition. "I wish that law schools would teach law students how to plea through moot courts," she adds and she also thinks law students should be taught to do proper research.

LAW STUDENTS

"Law students have to know exactly what the material is covering by knowing exactly where to look for it. The ability to relate makes you the greatest lawyer. We need to start training the students in law school and the time to start this training is now. It is time to take it seriously," she concludes.

FUTURE PLANS

As to her practice future plans, she may consider a merger, but so far she is enjoying her boutique solo practice.

"Law students have to know exactly what the material is covering by knowing exactly where to look for it. The ability to relate makes you the greatest lawyer. We need to start training the students in law school and the time to start this training is now. It is time to take it seriously."



“We need a law to regulate the arbitration system.”



Driving Change for Clients Around the World.

Through hazards and risk, serving clients where they need us is how we play. Jones Day is a global law firm with more than 2400 lawyers resident in 19 countries and 42 offices throughout the United States, Latin America, Europe, the Middle East, and Asia. Our award-winning client survey rankings reflect how our 25 practices and our worldwide offices cover the spectrum of transactional, litigation, and regulatory matters facing our clients, no matter where they are. And when these matters have an interdisciplinary or cross-border dimension, we are well positioned to bring together the right team of lawyers, wherever they are located in the world, to meet our clients' business objectives, and we work seamlessly to bring the best of the Firm to every client engagement. Whatever direction, in any conditions, let Jones Day help shape the shots.



One Firm WorldwideSM

2400 Lawyers. 42 Locations. 5 Continents. www.jonesday.com



Mastering the legal game

In the first of his series on law firm management, former student of law, entrepreneur and academic **Professor Sebastiaan Kodden** of **Nyenrode Business University** in the Netherlands explains how theory can help legal practice.



In his book 'Outliers' written in 2009, the American bestselling author Gladwell endorses the theory of the Swedish psychologist Anders Ericsson that you can only be successful after you have done 10,000 hours of practice.

Gladwell's book and Anders Ericsson's 10,000 hour theory inspired me to start writing articles and books as I had already completed three times as many as these hours both of practical experience and theory.

However, I still needed to find answers to questions like, "What management theories have actually proven to be valuable for legal professionals over the past few years?" or 'Why do some things go right and other things fail in legal service firms' practice?"

IMPROVEMENT AT THE HEART

"To improve yourself, you need a vision first and you have to learn from your mistakes in order to continue to develop yourself," a former Olympic coach once told me. "Inspiration is good, perspiration is better."

Developing vision, determining your destination or the inspiration, but also putting in the required hours, the perspiration, are key concepts I will deal with in my forthcoming articles in this magazine.

I will look at them from the perspective of 'The Positive Psychology' and the inspiration of Professor Kurt Lewin (recognised by many as the founder of social psychology).

"There is nothing so practical as a good theory," Lewin once said. As a young entrepreneur I was intrigued by his quote and it encouraged me after completing my legal studies to continue studying Business Administration, which eventually led to a new career. So, indeed, there is nothing so practical as a good theory.

ENGAGEMENT ISSUES

Leadership theories and the concept of Work Engagement were at the core of my doctoral research at Nyenrode Business University. In my forthcoming articles, I will write about the results of my research into the effects of employee engagement on knowledge productivity within legal service firms, which I hope will provide legal professionals and managers with concrete and tested reference

points and ways to adopt a positive attitude to life as the Positive Psychology recommends. There is good reason to write these articles, as fewer and fewer legal professionals worldwide experience a high level of work engagement and passion in their job.

THE IMPACT OF TURBULENCE

But why are so many legal professionals less engaged in their work? One answer is the legal profession nowadays faces a lot of turbulence. As a result, in many firms this leads to a feeling of high uncertainty and fear among legal leaders and legal professionals.

In such situations, I unfortunately find legal leaders exercising more management controls and applying more management by excel, to try to overcome their fears and this perceived lack of control.

However, with legal professionals this in turn leads to less drive and enthusiasm, which is one of the most important conditions required for adequate performance in the profession.

As a result, the most commonly used management style nowadays actually decreases performance, from both employees and the entire firm. Sadly, this in turn leads to more turbulence, more uncertainty and more checks. It is a vicious cycle.

CURB YOUR FEARS

Like athletes, good legal leaders know how to curb their fears. They are able to 'let go' and deliver ultimate performance.

They find a way out of that vicious cycle and instead develop an environment of positive energy. Legal firms that truly invest in their people instead of all kinds of digital innovation and management controls can actually display durable growth.

BACK TO PRACTICE

Practice is not always easy and this is something that has not only been demonstrated in the legal industry, but also by various great athletes, coaches and fellow entrepreneurs I am lucky enough to have worked with over the last couple of years. I will use some of their insights in order to address the many required trends in mastering the legal game. As when it comes down to it there is nothing as practical as a good theory.



UAE Business Hub

Justice Omar Al Muhairi

As part of series on the mechanics of investing in the UAE, **Justice Omar Al Muhairi** talks about a day in the life of a DIFC court judge and the benefits of using the DIFC courts for litigation.

HOW DOES YOUR DAY START?

"Usually at five in the morning, I pray, then do some sport, either walking or running for 45 minutes. Then I have a traditional breakfast with my children which consists of oatmeal, milk and honey. Then I take them to school. Although on the way, we usually play a Question and Answer game."

DESCRIBE A TYPICAL DAY IN THE DIFC COURTS?

"I reach my office at eight, say 'Good morning' to the staff. Then I read emails, access to the Case Management system and follow-up on the cases which have been assigned to me. If I have a hearing that day, I review the case before it. Usually the hearings start from 10 am and goes on until 5:00 pm with an hour break. On days where there are no hearings, I spend my time writing judgments or reading either important judgments and or legal books."

WHERE DID YOU STUDY?

"I studied at both the Dubai Police Academy in Dubai and SOAS, University of London."

WHERE DOES YOUR PASSION FOR THE LAW COME FROM?

"From my Grand Father. He used to sit in his Majlis (which is a large room people gather in). I'd see him every day solving people's differences by mediation. He taught me a lot of wisdom."

HOW DO YOU SPEND YOUR FREE TIME?

"On the beach. Every two weeks I go fishing in my boat."

WHY DID YOU DECIDE TO MOVE FROM THE DUBAI COURTS TO THE DIFC COURTS?

"I saw the DIFC Courts as a chance to grow as a professional."

HOW DID YOU FIND THE MOVE?

"It did not feel any different as I live and

work in Dubai which is an international city, where over 200 nationalities live and work, with different cultures, languages and religions."

WHAT WERE THE CHALLENGES OF MOVING FROM A CIVIL LAW TO A COMMON LAW SYSTEM?

"As an Arabic speaker, I found the English language a challenge, but I studied hard. I attended an English course for lawyers at SOAS, London University for a year. I also attended a conversion course designed to help civil lawyers become common law lawyers at the same college. However, the second challenge was the common law system structure and methodology, but I am narrowing that gap too with continuing training in the London Commercial Court and Singapore Supreme Court."

"I also keep reading principle cases, new cases and text books."

WHAT ARE THE DIFC'S OBJECTIVES?

"The DIFC was established to be a recognised hub for institutional finance and a regional gateway for capital and investment. The aim was to bridge the gap between the world's major financial centres."

The DIFC has its own laws and regulations and even its own courts and a facility for arbitration. It is independent of the UAE's civil and commercial laws, but is still subject to UAE criminal law."

HOW ARE THE DIFC LAWS PUT IN PLACE?

"DIFC Law is Dubai Law, so the Ruler of Dubai issues both the laws in Arabic and English."

WHY SHOULD PARTIES OPT FOR THE DIFC TO RESOLVE DISPUTES?

"The DIFC Courts are an English language common law court in the Middle East. We are independent, transparent and cost-effective for those taking disputes. The UAE's unique English language common-law judicial system is regarded as one of the most efficient

and modern legal systems in the region. Based on international best practice, the Courts are every businessman's best friend as good ways to resolve commercial legal disputes, and enforce judicial decisions. The Courts are administered by internationally recognised judges and proceedings."

IS DUBAI'S LEGISLATIVE SYSTEM INVESTOR FRIENDLY?

"In terms of law and regulation, the Dubai Government established many freezones which have different laws and regulations to non-freezone areas, such as the Dubai International Financial Centre (the DIFC), the Jebel Ali Free Zone and Dubai Media City. One hundred percent foreign ownership of companies is allowed when doing business in these freezones. Whereas in non-freezones it is 49 per cent for most companies incorporated outside these areas. There are no tax, no restrictions on the repatriation of capital and profits, and freedom from currency restrictions and import duties. Freezones have been fundamental in developing Dubai's reputation as an attractive place to establish a business."

WHICH INITIATIVES MAKE DUBAI INVESTOR FRIENDLY?

"Dubai is one of the few cities in the world that has undergone a rapid transformation from its humble beginning as a pearl diving centre to one of the fastest growing cities in the world. Today, it is a tourism, trade and logistics hub. It has also earned itself the reputation for being the gateway between the East and West. It is even considered the dynamic nucleus of the Arabian Gulf. It is also one of the most cosmopolitan countries in the world and is safe, politically stable and centrally located, with a good education system, healthcare facilities and modern infrastructure."

WHAT IS THE STRUCTURE OF THE DIFC COURTS?

"The DIFC Courts operate a Court of First Instance and a Court of Appeal. They cover civil or commercial cases and disputes arising from or related to a contract which has been fulfilled or a transaction that has been carried out, in whole or in part, in the DIFC or an incident that has occurred in the DIFC. The DIFC Courts consist of at least four Judges, one of whom is the Chief Justice. The Courts carry out their func-

How To: Initiate A Claim With The DIFC Courts

Parties do not need to come to the Courts as all applications are made through the Courts' e-Registry, a 24/7 on-line, secure back-office system. Alternatively, applications can be made at the Court offices, which are in the DIFC.

tions in an independent manner, in accordance with the provisions of DIFC laws and regulations.”

“They have jurisdiction over civil and commercial matters only but no jurisdiction over criminal matters.”

HOW EXPENSIVE ARE THEY?

“Fees vary from court to court. The fees charged at the DIFC Courts reflect the investment made in the world-class, expert systems in place here. The Court’s efficiency can be measured in its faster-than-average settlement periods.”

“These are driven by best-in-class technology and judicial expertise. In my view our fees are lower than some international commercial courts. For example, average legal fees are 5% of the value of the claim and/or the property with a minimum of USD 1,500.”

COULD YOU EXPLAIN THE OPT-IN CLAUSE?

“Originally the DIFC Courts were established to hear only cases relating to the DIFC.”

“As a result of their success and far-reaching reputation for swift and efficient justice, their jurisdiction was extended in October 2011. Dubai Decree No. 16/2011 opened the Courts’ remit to hear, any civil or commercial case in which both parties select the DIFC Courts’ jurisdiction, either in their original contracts or agreements or post-dispute. They also cover any civil or commercial case related to the DIFC. The DIFC Courts apply the law governing the contract in question.”

“Otherwise, they apply the DIFC’s common law system, based predominantly on that of the United Kingdom.”

“This allows parties with no connection to the DIFC to explicitly agree to submit to its jurisdiction, either before or after a dispute arises, if they wish to do so.”

ARE DIFC JUDGEMENTS ENFORCEABLE OUTSIDE THE DIFC?

“Yes, DIFC Courts’ Judgments are enforceable in all UAE Courts and GCC Courts as UAE is a party of GCC Convention.”

“They are also enforceable in Arab Countries and countries where the UAE has entered a treaty.”

“The DIFC Courts can also sign MOUs with other Commercial Courts, like London Commercial Courts, Singapore Supreme Courts, and South Korean.”

DOES THE DIFC RELY ON PRECEDENT IN ITS JUDGEMENTS?

“We have our own Precedent. As common law Courts we rely on other Common law jurisdictions’ precedents. We also consider UAE Courts Judgments, and these become binding if that Judgment is issued by UAE Federal Supreme Courts as the highest Judicial body in UAE.”

ARE CASES HEARD IN PUBLIC?

“The general rule is that all cases are heard in public, except if the Courts decided in the interest of justice for the case to be heard in private, or the parties wish this and have persuaded the Courts to do so. There are also some types of cases which are heard in private, such as Arbitration claims.”

“DIFC Courts’ hearings are open to the public and the media. Hearings are also available on the Courts’ website live.”

CAN PARTIES SUBMIT CLAIMS WITHOUT THE OTHER PARTY KNOWING?

“As a General Rule all proceeding must be served to the other party. However, if the application is for an interim remedy at first it is possible to hear it, but the Court order must be served within a reasonable time to other party.”

“The Court will then fix a return date for a proper hearing. The e-Registry platform offers web-based

case management and practitioner administration, eliminating the need for paper-based applications and records.”

HOW LONG DO CASES TYPICALLY LAST?

“At least 80% of First Instance cases with a trial of less than five days are offered a trial within six months from the date of their case management conference.”

“If the case is more than five days, then at least 80% are offered for trial within nine months from the date of their case management conference. At least 80% of all Court of Appeal cases are heard within four months of the grant of permission to appeal.”

ARE JURISDICTIONAL DISPUTES FREQUENT?

“Yes. They are mostly local but we have had one case which was international.”

“The easiest jurisdictional disputes to resolve are the ones with the jurisdiction of the DIFC Courts or the Dubai Courts. The DIFC Courts are a court of Dubai so we work in harmony with the Dubai Courts. In 2009 we established a joint committee between both Courts and signed Jurisdiction protocol and enforcement protocol. This committee meets quarterly to discuss collaboration initiatives.”

IN TERMS OF LAW IS DUBAI READY FOR EXPO 2020?

“Dubai is always ready. I would like to see Dubai Tourism Courts for Expo 2020, as the tourist sector is huge. This will send a positive message to investors that their investment is safe.”

WHAT IS YOUR ADVICE FOR THE NEXT GENERATION OF LAWYERS?

“To be patient. Accept any opportunity then learn how to do it. I say to them read to lead.”

“A practitioner who speaks English and has at least two years’ experience as an Advocate in Courts, Arbitrations or Tribunals may be admitted to appear and plead before a DIFC Judge at hearings on any matter other than a Court of First Instance trial or an appeal to the Court of Appeal.”

WHAT IS REQUIRED TO BECOME A DIFC JUDGE?

“Judges are appointed for a specified period of not over three years, but may be re-appointed, if the period does not extend beyond the day the Judge turns 75.”

“If a Judge has turned 75 years of age or the period of appointment has concluded, a Judge holding office can continue in office for as long as it is necessary to deliver judgment or perform any other necessary in relation to proceedings which started before they turned 75 or before the conclusion of their appointment. A person is qualified to be appointed as a Judge if they have been the holder of high judicial office in any jurisdiction recognised by the UAE Government and they have significant experience as a qualified lawyer or judge in the common law system. A Judge is not eligible for appointment if they have any commercial association which could create a conflict of interest with any DIFC body or any subsidiary of a Centre Body other than the DIFC Judicial Authority, any licensed Centre Establishment or other institution which is part of or which is licensed to carry on any busi-

ness in the DIFC; or if anyone they are employed by is any Centre Body or any subsidiary of a Centre Body other than the DIFC Judicial Authority or any person referred to in the relevant rules. A Judge must take an oath of office before the Ruler or his delegate before starting his duties."

WHICH CODE OF CONDUCT DO PARTICIPANTS IN THE DIFC COURTS ADHERE TO?

"The DIFC Courts were established to uphold the laws of the DIFC and advance the rule of law by ensuring the just and effective resolution of disputes within the Court's jurisdiction. The DIFC Courts is the first court in the region to issue a Mandatory Code of Conduct for Legal Practitioners in the DIFC. By registering to practice in the Court, each individual registered as a legal practitioner undertakes to act with integrity and independence in support of the Court and the wider community it serves."

"In the UAE it is a criminal offence to publish news, pictures or comments about the secrets of people's private or family lives."

WHAT ARE THE DIFFERENCES BETWEEN COMMON AND CIVIL LAW?

"They are two Gates for one Justice. The source of law is what differentiates

Common and Civil legal traditions. The most important source of law is judicial cases, which give judges an active role in developing rules."

"In the civil law system, the statutes and codes cover the circumstances but the Judges have a limited role in applying the law to the case in hand. However, past judgments are basically loose guides. In addition judges lean

towards investigating when it comes to court cases. On the other hand, common law system judges act as arbiters between the parties who present their arguments.

WHAT IS THE MOST SIGNIFICANT PROGRESS THE DIFC COURTS HAVE MADE?

"The DIFC Courts have made a lot of

progress starting from the expansion of their jurisdiction. Other milestones have included the first female judge, the first Pro Bono Programme, the first small claim tribunal and first e-Registry system. All enforcement requests made by the DIFC Courts to other courts in the UAE, Middle East and beyond have been accepted and we have accepted all requests made from other courts to us."

HOW HAS THE DIFC BEEN ABLE TO STRIKE A BALANCE BETWEEN RESPECTING THE CONSUMER PRIVACY OF PERSONAL DATA AND COMPANY INTERESTS?

"The privacy of an individual is protected under the UAE Penal Code, it is a criminal offence to publish news, pictures or comments about the secrets of people's private or family lives."

"It is also an offence for anyone who is, by reason of profession, craft, circumstance or art, entrusted with a secret, to disclose it, or use it for their 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 is about."

"The DIFC issued its own data protection law specific laws. These apply to specific types of personal information which 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. There are also restrictions on data transfer from within the respective Financial Centre to places outside of the DIFC."

"The data protection law applies only to activities within the DIFC or transfers from DIFC to outside the Financial Centre."

HOW WOULD YOU SAY THE DIFC DEFINES EXCESSIVE PERSONAL DATA PROCESSING REQUESTS?

"The definition of personal data is that covering any information referring to an 'Identifiable Natural Person' and refers to information being processed by means of equipment operating automatically in response to instructions given for that purpose."

"It covers information which is recorded with the intention it should be processed by means of such equipment or which is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System."



Making Emerging Markets Less Risky Business

As the UAE sits on the top list of countries where multinationals locate their investment vehicles, **Paul Werné** and **Paul Andrews** of **Etisalat Group** review the dos and don'ts of investing in emerging markets.

The UAE has experienced decades of growth and development, accompanied by a strong increase in its presence in emerging markets. This is predominantly a result of the investment activities of sovereign wealth funds. Locally owned public or privately-owned corporations, the UAE's multicultural, and business friendly environment, easy access to capital and proximity to promising emerging markets in the Middle East, the Indian subcontinent and Africa, have also put the Emirates at the top of the list of countries where multinational organisations consider locating their outbound investment vehicles. However, whatever the economic attraction of some emerging markets, there are key factors which can either lead to an investment's success or failure, which need to be considered.

THE LIE OF THE LAND

No one 'emerging market' is quite like any other. The term 'emerging markets' is often used broadly to refer to markets whose economy,

capital markets and business environments do not reach the standards of modernity, clarity and reliability of a 'mature' country or the expectations of the business world's global players.

This broad definition covers a multitude of countries, each with its own legal norms and traditions. The historical experiences of some emerging markets, such as colonisation or exploitation of natural resources, has led many of them to form highly protectionist regimes resulting in restrictions on the activities that can be carried on by foreigners and limitations on the expatriation of overseas payments of cash to related parties. In contrast (particularly in Africa) the need to make exports easy and to attract foreign capital has led many countries to adopt business-friendly legislation, although its implementation may still be marked by distrust, and a high level of bureaucracy or protectionist attitudes.

Many such countries are party to international treaties or World Bank programmes which further favour international investments. However, the legal uncertainty that exists in many of these countries means that investments requires a level of attention even greater than that needed with an investment in a developed market.

Often, the legal regime has been established by reference to 'mature' jurisdictions, usually the former colonial powers (mostly the UK and France) and is modern and well drafted. Despite this, practice can still differ from the word of the law and the quality of the legislation may not be matched by the local authorities' or courts' capacity to enforce it, resulting in unclear processes and reduced transparency.

THE IMPORTANCE OF PROPER PLANNING

If you ask anyone what will best influence the success of an emerging market transaction, they tend to focus on macro factors like political stability, security, prevalence of corruption, predictability of the legal and fiscal environment or strong inter-governmental relations. However, other factors are just as important:

- **The choice of the right investment vehicle.** The UAE has entered into a reasonable number of bilateral (or multilateral) investment treaties (BITs) but other countries have a more developed or targeted network of such treaties. The choice of the right inbound location and investment vehicle needs to be factored into the very structure of the investment. History has shown that BITs are an effective deterrent and a useful enforcement tool against prejudicial actions by foreign authorities.
- **The proximity of legal culture.** Common Law, Civil Law, or Sharia inspired legislation can vary greatly from one another.
- **Understanding the mechanics of how contractual decisions are made** and what will (or will not) influence a decision-making process.
- **The choice of the investment structure.** Invest-

“No one ‘emerging market’ is like any other such market.”



ments in emerging markets are often Capex hungry and in an environment where money is not readily available (or convertible) structuring the equity, debt and their repatriation is key.

KEEP YOUR FRIENDS CLOSE...

As previously mentioned, many countries have foreign ownership limits which necessitate the involvement of local partners. In other cases, local knowledge and influence are seen as key to the venture's success. Interference by governments, regulatory bodies and established competitors, can lead to the need for support from influential local individuals or businesses. In such cases, partner selection is critical and must be done with an eye to sustainability and compliance.

“Local knowledge and influence is key to the venture's success.”

Some emerging markets have proved to be resilient and adaptive to change. Others have been almost constantly going through political turmoil. Established bodies and respected, politically neutral, businessmen may offer better protection in

the long run than politically powerful individuals. But the complexities of political, social and business life in the country should never be left entirely to the partner as becoming dependent on a local partner can result in bigger problems than the ones the partner was supposed to solve in the first place. The mark of success for a foreign investor is that he is eventually viewed as having become 'local'.

MANAGING RISK

In markets where international standards are irregularly applied, investors must take a pragmatic approach to risk.

A higher level of risk tolerance is required, and

reliance on the court system for protection or justice may be a less effective strategy than in more developed jurisdictions. In countries, where legal knowledge, in countries where access to legal information is often difficult, so the investor needs to opt for:

- advisors who understand the local business culture and legal environment.
- a 'developed country' governing law to rule the agreement (e.g. English or French law), but pay close attention to areas where this choice of law won't apply.
- the right forum for dispute resolution. This tends to be arbitration, but that only solves one half of the problem and puts the rest on the exequatur side. Check if the host country has ratified the New York Convention or another respected regional convention, and what the local legislation and history reveal in this respect. In many countries hostility against 'expatriated' legal proceedings is growing and that is something to monitor.
- simple deal structures. Complex deals are more difficult to get over the line and transactions take longer to complete in less developed markets.
- the right monitoring of the political and administrative environment. In many fields (e.g. banking or telecoms) regulatory authorities are often sophisticated and modern, and have political importance. In other fields, they might lack the sophistication, but the degree of influence may remain unchanged.

DON'T ASSUME

A final word of caution, the investor should never assume social, environmental, ethical or human rights issues can be neglected just because they believe this is what local businessmen seem to be doing. The contrary is true and your international reputation can depend on it.

Clients say:

“They are clearly leaders in their field. They are technically very good, efficient and commercial.”

Chambers Global 2015

40 years in the Middle East



40 YEARS
MIDDLE
EAST



Al Reyami Case

Case Detail

Case Name

Al Reyami Group LLC v BTI
Befestigungstechnik GmbH & Co KG

Citation

Case No 434/2014

Hearing date

November 2014

Court

Dubai Court of Cassation

The Dubai Court of Cassation's decision in the Al Reyami case has been widely praised **Sami Tannous** and **Antonia Birt** of **Freshfield Bruckhaus Deringer LLP** explain why.

The original dispute arose under an exclusive agency agreement concluded in May 2007 between a German roofing and power tools producer (BTI Befestigungstechnik GmbH & Co KG) and a UAE distributor (Al Reyami).

In 2011, a sole arbitrator appointed under the ICC Rules, seated in Stuttgart, found in favour of BTI and awarded €300,000 in compensation.

WHAT HAPPENED?

BTI began enforcement proceedings in Dubai. The Court of First Instance allowed the award's enforcement in 2012 and this decision was then upheld by the Court of Appeal in 2013.

However, Al Reyami then appealed to the Court of Cassation.

THE CHALLENGE

Al Reyami challenged the enforcement of the award on the following grounds:

- the arbitrator's failure to

review the arbitration agreement;

- the alleged invalidity of the arbitration agreement due to the change of the hearing venue to France from the agreed seat in Germany;
- the failure of BTI to submit to the court the entire agency contract between the parties, including its appendices; a legal translation of all clauses of the contract between the parties; a partial decision of the arbitral tribunal relating to the arbitral procedure; and evidence that Germany had acceded to the New York Convention; and
- the claimed non-arbitrability of disputes arising under agency contracts, since the contract was executed in the UAE.

DUBAI COURT OF CASSATION DECISION

The Dubai Court of Cassation upheld the decision of the Court of First Instance and the Court of Appeal

and ratified the arbitration award. In the process it rejected all of Al Reyami's objections as being 'entirely incorrect'.

It cited Article 212 of the UAE Civil Procedure Law which states that awards not issued in the UAE are subject to the rules applicable to foreign arbitral awards.

The Court also quoted Arti-

"It cited Article 212 of the UAE Civil Procedure Law which states that awards not issued in the UAE are subject to rules applicable to foreign arbitral awards."

cle 238 which provides that international treaties which have become effective in the UAE by legalisation are to be considered as domestic law that must be applied and enforced by the judiciary.

Accordingly, the Court of Cassation re-confirmed the application of the 1958 New York Convention

for the Recognition and Enforcement of Foreign Arbitral Awards (the New York Convention) and the fact that only the grounds under Article V of the New York Convention could be relied on to challenge a foreign arbitration award.

In the Al Reyami case no such grounds had been established.

The decision has been widely praised for re-affirming the Dubai courts' pro-enforcement stance towards foreign arbitral awards.

The decision is a positive and welcome re-affirmation that only the grounds listed in Article V of the New York Convention are relevant to the court's consideration of whether to enforce a foreign arbitral award.

Moreover, the Court of Cassation's confirmation that defences based on the non-arbitrability of exclusive agency/distribution agreements do not, in the context of a foreign-seated

award, warrant a finding that public order has been violated under Article V(2)(b) of the New York Convention, is welcome given the position under domestic law.

OTHER RELEVANT DEVELOPMENT

In a further promising development, in 2015 the Dubai Court of Appeal ordered the ratification and enforcement of a London arbitration award pursuant to the New York Convention.

The Court of Appeal overturned

a decision of the Court of First Instance which had denied enforcement on the basis of the UAE Civil Procedure Law, which applies to domestic arbitration, and which had ignored the New York Convention.

This case is of particular interest because it concerned a dispute between a Hong Kong shipping company and a Dubai-based charterer, based on an unsigned contract negotiated by email. An appeal to the Court of

Cassation is pending.

UNMERITORIOUS CHALLENGES CONTINUE

The Dubai Court of Cassation's consistent recognition of the UAE's treaty obligations under the New York Convention is re-assuring.

However, nearly ten years after the UAE ratified the New York Convention, recalcitrant award debtors continue to pursue unmeritorious challenges to the enforcement of foreign arbitral awards, dragging award creditors through three layers of the UAE domestic courts, wasting time and money.

As confirmed by the Court of Cassation in the Al Reyami case, all of Al Reyami's defences were 'entirely incorrect'.

Yet, as in many other cases before it, BTI was forced to engage in nearly three years of litigation before all levels of the Dubai courts before it could achieve final enforcement of its arbitration award.

While it is positive that BTI was successful before the Court of First Instance and Court of Appeal, thus confirming that the lower courts in Dubai now appear to be adopting the Court of Cassation's reasoning, unfortunately lengthy, unnecessary delays in the enforcement process leave ample time for recalcitrant award-debtors to take the necessary steps to organise their assets in order to frustrate enforcement efforts.



Antonia Birt
Associate

Freshfields Bruckhaus Deringer LLP

LOOKING TO THE FUTURE

It is time courts in Dubai and the wider UAE moved to the next stage by streamlining the enforcement process and sending a clear message to arbitration users that unmeritorious challenges to foreign arbitration awards will not be without consequences.

Looking to the future, dissuading award-debtors from mounting unmeritorious challenges could be achieved in a variety of ways.

UAE Courts could create dedicated branches with specialist judges to consider enforcement applications.

STREAMLINING

This would streamline the enforcement process and help render decisions more quickly.

Although, it is not the usual practice of courts in the UAE to do this, adverse costs orders against parties who decide to mount unmeritorious challenges to arbitral enforcement could become more prevalent.

Steps of this nature might at least make recalcitrant award debtors in the UAE think more carefully before engaging in protracted and meritless challenges to the enforcement of foreign arbitral awards. and in the process cement the UAE's reputation as an increasingly arbitration-friendly jurisdiction.



Sami Tannous
Counsel

Freshfields Bruckhaus Deringer LLP

“This decision which ratified a foreign arbitral award under the 1958 New York Convention for the Recognition and Enforcement of Foreign Arbitral Awards has been widely praised by the arbitration community and it re-affirms a pro-enforcement stance.”

“The Dubai Court of Cassation confirmed that defences based on non-arbitrability of exclusive agency or distribution agreements do not in this context warrant a finding public order has been violated.”

World Class Arbitration?

Arbitration activity may be increasing in Dubai, but **Alain Farhad** of **Squire Patton Boggs**, looks at whether it can now be classed as a modern international arbitration jurisdiction.

The promise of international arbitration is to procure a reliable and efficient method for the resolution of international commercial disputes. Delivering on this promise depends on all stakeholders of the arbitration process: parties to arbitration proceedings, counsels, institutions administering arbitration proceedings, arbitrators, courts and legislators.

KEY TO SUCCESS

International arbitration has delivered on its promise for several decades in many parts of the world, particularly in developed trading states, where arbitration has become the forum of choice for the resolution of commercial disputes. Commercial parties favour arbitration because it is capable of overcoming many of the difficulties arising from litigation before national courts. Key to its success, international arbitration provides the

parties with (a) a neutral forum, in which disputes are decided by arbitrators who are not bound by the legal and cultural traditions of any national court and whose nationalities are often different from that of the parties involved (thus reducing the risk of parochial prejudice) and (b) a decision, which is final and binding on the parties, generally not subject to any appeal and which can be enforced in all the

135 countries party to the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 1958 (the New York Convention). The success of a jurisdiction for the purposes of international arbitration is best measured by the number of contracts, which include arbitration clauses referring to that jurisdiction as their legal seat. As a hub of international commerce, Dubai is well placed to become one of the world's hubs for the resolution of international commercial disputes.

In the past decade, the number of arbitration proceedings seated in or involving the economy of the Dubai has massively increased, making the need for a modern arbitration regime more pressing. Some progress has been made in the past few years to create an arbitration friendly environment but Dubai still has some way to go before it can be considered as one of the world's most attractive arbitration seats such as Paris, Geneva, London or Singapore.

In brief, a modern arbitration jurisdiction is one which has (1) acceded to international instruments enabling the recognition and enforcement of foreign arbitral awards (2) an arbitration legislation upholding the arbitral process (3) Courts which uphold such international instruments and assist arbitration proceedings without excessive interference and (4) specialised arbitration professionals. Dubai has recently experienced positive developments on all four fronts.

FIRST TEST

Dubai ticked the first box of this four pronged test in 2006. Indeed, the UAE became that year a party to the New York Convention, thus enabling the enforcement of foreign arbitral awards in Dubai as well as the enforcement abroad of arbitral awards rendered in Dubai seated arbitration matters.

SECOND TEST

Dubai's onshore arbitration legislation is also expected to change. The current arbitration legislation (articles 203 to 218 of the UAE Code of civil procedure) was promulgated in 1992 and does not reflect current best practices. Since 2008, several drafts of a new UAE arbitration law have been circulated. Some have come close to what is expected of a modern arbitration legislation, others have missed the mark by a significant margin. The DIFC provides a very good example of the successful implementation of a modern arbitration legislation. The DIFC arbitration law issued in 2008 is inspired by the UNCITRAL Model law and is in line with the world's best practices.



Alain Farhad
Partner,
Squire Patton Boggs

“A jurisdiction’s success in terms of international arbitration is best measured by the number of contracts, which include arbitration clauses referring to it as their legal seat.”



THIRD TEST

The third necessary component of a successful arbitration regime rests on the local courts. The courts' more or less liberal approach to the enforcement of arbitration agreements and awards is key to the development of a viable arbitration regime. On questions not expressly resolved by the applicable legislation, the courts' interpretation has the potential of making an arbitration regime attractive or repulsive. Some concerns have been raised in the past (including among international observers) as to the Dubai courts' approach to international arbitration, in cases where arbitration awards or arbitration agreements were challenged for arguably technical (rather than substantive) reasons. Some of the Dubai Court of cassation's recent decisions however inspire optimism at least as far the en-

forcement of foreign arbitral awards and the treatment of the New York Convention are concerned. In October 2012, the Court of cassation issued a widely reported decision in the case of *Macsteel International v. Airmech (Dubai) LLC*, which upheld the enforcement under the New York Convention of two related foreign arbitration awards against a Dubai company. The court held that the New York Convention (and not the arbitration provisions of the UAE Code of civil procedure) governs the enforcement of foreign awards. The Court of cassation thus confirmed that the provisions of the UAE Code of civil procedure (and their more stringent requirements

for the enforcement of arbitration awards) only apply to the enforcement of domestic awards. This approach has since been confirmed by a ruling of the Court of cassation of 23 November 2014 and, at this juncture, confirms that the Courts of Dubai will correctly enforce foreign awards in accordance with the UAE's international treaty obligations. While there may be a long road ahead, this is the achievement of a key milestone in Dubai's development as a modern arbitration regime.

FOURTH TEST

The fourth and final requirement for a trustworthy and successful arbitration regime rests on the arbitration personnel itself: the arbitration practitioners, whether they act as counsel, case administrator at arbitral institutions, arbitrator or judge hearing arbitration related matters.

Reliable arbitration seats all have in common a sizeable pool of sophisticated arbitration professionals in all four categories. Dubai has become (and with the development of a favourable legislation will likely increasingly be) an attractive centre for arbitration professionals. For instance, DIAC has successfully developed a well-trained and multicultural staff effectively administering its caseload. Arbitral institutions such as DIAC, the ICC or the DIFC-LCIA also play a key role in ensuring that the individuals appointed to arbitrate disputes under their rules have the requisite competence and training and satisfy the requirements of impartiality and independence. Finally, judges hearing applications arising from arbitration proceedings are equally important stakeholders in the arbitration process.

The significant number of arbitration proceedings seated in Dubai justifies the development of a pool of specialised arbitration judges serving in a defined arbitration division of the Dubai Courts who are familiar not only with the legislation which they are tasked to apply, but also with the best practices of international arbitration.

BENEFITS

Dubai would draw clear economic benefits from the development of an attractive arbitration regime. The most direct such benefit would come from the growth of its arbitration legal market: more hearings would take place in Dubai and more arbitration lawyers would practice from Dubai. But more fundamentally, a favourable arbitration regime would increase the perception of Dubai as a reliable jurisdiction in which the rule of law is upheld and commercial disputes are resolved efficiently. In this context, the implementation of a modern arbitration regime would contribute to Dubai's perception as a global economic hub.

“Dubai would draw clear economic benefits from the development of an attractive arbitration regime.”

Helping Hands

With Expo 2020 on the way, **Mahmood Hussain** of **Mahmood Hussain Advocates & Legal Consultancy** considers what changes the new Dubai Public-Private Partnership Law will make to infrastructure projects.

With Expo 2020 on the way in Dubai and the ensuing major infrastructure projects, it is good to see a new Public-Private Partnership Law (Dubai Law No. 22/2015) which was published in the Official Gazette last September, taking effect from 19 November 2015.

WHAT IS THE AIM?

This new law has been designed to revamp the private and public investment model for infrastructure projects and it is hoped it will pave the way for more collaboration between private and public players in the market. With Government entities in the region facing an increasing burden, this law will come as a welcome relief to both public entities looking to share their financial burden and private entities interested in collaborating on major infrastructure projects.

The new Public-Private Partnership Law was promulgated to help encourage the private sector to participate in development projects and enable the Government to implement strategic projects more effectively and efficiently. It also aims to increase productivity and improve the quality of public service by securing more effective management of services by the public sector. One

of its most striking developments is the aim to increase the transfer of knowledge and experience from the private sector to public sector, allowing more training of the Government sector employees in the management and operation of projects. This means, the benefits will finally trickle down, reducing the Government's financial burden, and paving the way for more competitiveness for some projects in the local, regional and international markets.

WHO DOES IT APPLY TO?

The law will apply to all Government entities which are subjected to the Government's general budget. The Supreme Financial Committee, with authorisation can extend the application of the law to entities which are not subjected to general budget (via Article 4(1)).

However, one of the important exclusions from its scope is that new law shall not apply to Public-Private Partnership projects with the Government entities except for electricity and water projects

(governed by Dubai Law No. 6/2011) and procurement which includes contract works and supply of materials and services (governed by Dubai Law No. 6/1997).

At the same time, all projects under the scope this new law's governance must be conscious of the economic, technical and social requirements prevailing in the region.

While selecting a project under the Law, certain prime factors need to be considered. These include:

- public and Government interests, economic viability and the extent of the positive influence on Dubai's development plans;
- any risk including derogative implications on the environmentalising out of execution of projects;
- the effectiveness of the capital invested; and
- the technical expertise which contributes effectively in improving public utilities' performance and ensuring quality of services.

WHICH MODEL?

Taking into consideration general Public-Private Partnership practices, the law has regulated that projects under this law will have to be implemented as either:

- a Build-own-operate-transfer (BOOT) model (where a private company finances, constructs and operates the project for the agreed period before assigning and transferring title to the project to the Government entity, and a concession is given by the Government to finance, create and operate the facility until the ownership is transferred; or
- a Build-operate-transfer (BOT) model (where a private company finances, constructs and operates the project for the agreed period before the right of utilising the project is assigned and transferred to the Government entity; or
- as a model where a private company constructs and transfers the ownership right to the Government entity, but reserves the right to commercially utilise and operate the project for the agreed period; or
- as a model where a Government entity transfers the benefits of the project to the private company for them to utilise commercially and operates it for an agreed time. As such, the Supreme Committee, the recommendation of the Government entity involved in the project and the Department of Finance (DOF) can still approve any other methods to operate such projects. The law provides certain conditions for approving projects. The Director General of the

“The law will apply to all Government entities which are subjected to the Government's general budget.”



Government agency or his nominees approve projects with a total cost of AED 200 Million to the Government agency. The DOF approve projects with a total cost to the Govern-

menting such projects without affecting the project or the assets, and requires the project company alone shall bear all consequent obligations.

“The Director General of the Government agency or his nominees approve projects with a total cost of AED 200 Million to the Government agency.”

ment agency between AED 200 Million and AED 500 Million. While, the Supreme Committee approves projects with a total cost more than AED 500 Million to the Government agency.

WHAT IS COVERED?

This law also ensures a fair way for governing tender processes and appointing partners. It requires in all cases the principles of publicity, transparency, free competitiveness and equal opportunity must be followed. It allows companies to form a consortium to submit a bid in its name (unless otherwise specified in the tender document). However, the applicable partnership contract (or the PPP project contract) must be executed by a project company licensed to operate in Dubai.

In many scenarios including consortium bids, this effectively requires a project company in the form of a Special Purpose Vehicle to be incorporated in Dubai.

Another key development is that this law requires standards or provisions to be included in partnership contract on the scope of work, asset ownership, intellectual property rights, responsibility to obtain licences, permits and approvals, financial and technical obligations, termination of the partnership contract, penalties for breach of contractual obligations, and environment safeguarding measures. In a step forward, the law also envisages that project companies may obtain funding for im-

As well as encouraging private sector participation in projects, this law also promises the state's support in all mega structured infrastructure projects. It appears the new Public-Private Partnership model will allow the Government to benefit from private players offering their expertise while still easing its financial burdens and other capital risks to their budget.

POINTS TO CONSIDER

Having said that, clarification is still required on some grey areas which have not been addressed in this Law.

Firstly, it is not clear whether the project company must be established as a local entity under UAE Commercial Companies Law or if it can be formed as a freezone entity. Secondly, the law requires the local ownership of business, which is established as LLC (Limited Liability Companies). However, it does not mention if the 51/49 rule (restriction of 49% on foreign shareholding) is applicable or not.

Thirdly, the law does not specify whether the Dubai Government will issue sovereign payment guarantees for assuring payment obligations of Government entities for a given project. Finally, it is silent on the issue of capital offerings from an interested SPV or whether such an SPV is to be incorporated in a freezone or in the mainland. Going forward, it looks as if this legislation will assist development of economic and social growth but it will be interesting to see which Government entities come forward to collaborate in such initiatives with private players.

Lessons for Lawyers...

What cyber security means for you

It's not just clients that need to think about cyber security. It can also cost law firms their business and reputation. Arif Barber of Barber & Co looks at lessons from the UK on the subject.

With new innovations in technology it is more important than ever that businesses remain vigilant against unwarranted cyber threats and take all action necessary to protect themselves and minimise the risks associated from such online activity.

The UK Government has realised the impact this could have on UK businesses and has provided training, arranged by the Department for Business, Innovation and Skills for individuals and businesses against cyber-attacks.

To understand the implications of this, we need to understand what is meant by the term cyber attack. Basically, it is when an attempt is made by hackers to damage or destroy a computer network or system.

Many lawyers brush aside this topic believing it will not affect their day-to-day work. However, this is a dangerous approach and one which could have deadly consequences.

POTENTIAL IMPACT

What if due to a cyber attack on your company, your case management system was affected? Then this in turn affected your accounting, time-recording and bill generating systems. What would happen if these systems were turned off for a week while you investigated the cyber attack? Although the adage 'old is gold' is relatively true, these days like most sectors the legal profession is dependent on technology. Lawyers in this day and age cannot survive without information technology.

The reality is that cyber attacks represent a growing and potentially damaging threat to a law firm's business.

With an attack like this, highly confidential information about clients can be compromised to their

detriment. Personal information like addresses and bank details, or commercially-sensitive information such as proposed business deals, intellectual property information and possible legal actions are all held by law firms for their clients.

If this sort of information is passed to a third party by an employee or contractor, or obtained by criminals via a phishing email opened up by unwitting lawyers or support staff, the consequences for both the client and the law firm can be devastating.

In the end, if a firm is known to have allowed such a data breach or has fallen prey to a cyber attack, it will inevitably harm their business' reputation.

LAW FIRM SPECIFICS

At a basic level, privacy and data protection issues have always been relevant to law firms who tend to hold vast amounts of client information. Historically these risks tended to be principally loss or theft of data from hard copy documents or files. However due to technological advances, data is now stored in so many different electronic formats and ways, that it makes things more difficult. This increases the risks of an attack, so it is in a law firm's best interests to keep this data as secure as possible wherever it is held.

UK LESSONS

Guidance from the UK Government on minimising data protection issues and cyber attacks suggests managing risk. This can be done by improving staff awareness and providing specific training.

It also involves creating an incident plan, increasing network security and malware protection and outsourcing information technology services. This is a useful introduction to what firms need to do to prepare. However, while it recommends putting an incident plan in place it does not specify what sort of things that plan should include. Although, one useful recommendation would be to put in place an

"If a firm is known to have fallen prey to a cyber attack, it will inevitably harm their reputation."



Arif Barber
Barber & Co



“Recent developments such as the UK phone-hacking scandal have made us all acutely aware that private information can be obtained.”

incident plan which includes reference to forensic specialists. It is also helpful to identify which specialist you would turn to in the event of an incident.

INSURANCE POLICIES

All law firms can benefit from a cyber or data breach insurance policy which can also provide access to the insurers' specialist vendors in the fields of forensic IT, PR and where applicable also legal advice. A major part of dealing with cyber attacks is the first party costs, as no third party profes-

sional indemnity policy will cover these expenses. Therefore it is helpful to look into cover provided by bespoke cyber insurance policies.

REPORTING BREACHES

Although reporting data breaches to the Information Commissioners Office (ICO) is not mandatory under UK or European Law, it is highly recommended to immediately report breaches. Taking this action will reduce a potential fine due to the early notification. Admittedly, there is also a risk the data breach could be publicised by the ICO if they decide to investigate it. However, the adverse publicity would far greater if no reference to the ICO is made. It is also worth noting that ICO fines can be covered by insurance.

OBTAINING CONFIDENTIAL INFORMATION

Confidential and private information in a law firm's possession can be wrongly obtained in a number of ways by third parties. These include:

- hacking phones and devices;
- malware which can capture and send private data; or
- phishing emails which ask for information like IDs and passwords, or contain attachments which, if opened, allow data to be captured.

To address this range of threats firms need to consider issues ranging from IT security, through to staff training, but also establish a firm policy to

ensure safe online practices are operated by staff and there is a procedure to report and deal with breaches.

STORING DATA

A further technological advancement which can have an impact is the ability to store data in an online cloud. This allows firms to free up storage on their servers and also their IT resources. It also means the data can be accessed from literally anywhere in the world.

This online backup is a good alternative for firms to minimise costs. However if the cloud is not secure it can be prone to a cyber-attack. Therefore, data stored in a cloud should be encrypted and a further back up made available in the case of a breach.

Recent developments such as the UK phone-hacking scandal have made us all acutely aware that private information can be obtained by third parties. Technology continues to evolve at a rapid pace allowing opportunities for those wishing to unlawfully obtain confidential information for financial or other benefit but, at the same time, data protection, privacy and confidentiality laws are necessarily flexible and continue to develop to keep up with new threats and issues. For example, the European Court of Human Rights has shown a willingness to grasp developments in online personal information.

There are other developments in the UK too, Lexcel (an accreditation for law firms) have made further amendments to their policies, providing the Lexcel mark to firms who have complied with their new information technology policy.

The Solicitors Regulation Authority (SRA) in the UK have made it mandatory that there are specific posts in law firms for legal practices compliance officers and finance and administration compliance officers. These individuals must report breaches and ensure firms are fully compliant with the new rules that come into force as technology evolves. Data protection has been a cause for concern in the past and will continue to be. Sadly all lawyers can do is keep systems in place to minimise potential risks and pray their firm do not fall prey to attacks.

Law Graduate Profile

Dina Al Dulaimi

University of Groningen

Iraqi born, Dina Al Dulaimi talks about her experience of studying law in the Netherlands and her hopes of working one day in Dubai.

Born in Bagdad in 1990, Dina Al Dulaimi has lived in the Netherlands since she was nine and her parents decided to move there. Arabic is her mother tongue, but she speaks and writes Dutch and English fluently. Dina has just completed a Masters at the University of Groningen, in Northern Holland, one of the most popular student cities in the Netherlands (in 2014 it had over 30,000 students) because its campus is in the heart of the city.

"Students are everywhere here, living in what we call 'rooms'", says Dina. "Once you step out of your dorm, you immediately feel the student life. Students here benefit from special discounts and offers."

Dina's passion for the law started at 19. "I have always been a seeker for solutions, always striving for justice. I like to analyse, and distinguish relevant factors to understand the underlying problem. This is a challenge, because it's not an easy task. I wanted to know more about the law and understand how it acts as a regulating instrument in society."

"I have learned so much during these four years in law school. I have also gained life experience."

Dina's friends describe her as really positive, determined, patient and a good listener. "I am straight to the point, if there is a problem I immediately take action. I am determined to progress and get results that are important to me. I take criticism as a learning tool in order to develop. Constructive

criticism only challenges me to accomplish more. The key to success is preparation. When I am working on something I am passionate about, I put my whole heart in it. If I really want something, then I will just go for it because I am very determined."

HER STUDIES

Dina decided to study at the University of Groningen because it had a good reputation in the Netherlands. It is believed to have the highest level of education, and is famous for both its Academy building and huge library. The Faculty of Law provides one



of the best law schools in the Netherlands. Most of the professors are legal practitioners, judges and lawyers who are experts in their field. They are always ready to answer student questions and are helpful. Each semester is five months long and covers five subjects.

"I loved the Academy Building, so many important things happen there. Students graduate in that building." She also has fond memories of her hours of studying in the University Library, an enormous building with four floors, a view across the city and a big canteen at the top. "The library was so crowded, they eventually placed an electric



university of
groningen

Open days

29 January 2016

9 April 2016

11 November 2016

> 24 English-taught Bachelor Degrees

> Over 100 English-taught Master Degrees



Top 100 University

www.rug.nl



board at the entrance to show us how many seats and computers were available."

Studying at Groningen taught Dina how to be more independent and strengthened her time management. "The pressure is high and the quality of work you have to deliver needs to be outstanding. There is a lot of freedom, the studying requires you to be self sufficient. This doesn't work for everyone. You have to be a good planner and work in a structured way. I set my own deadlines while preparing for my presentations. This worked well for me as I am at my best working under pressure."

Having completed a Bachelor's Degree in Dutch law, Dina passed her Masters in private law last

year, having written her thesis on family law, in particular divorce law. "The Netherlands recently passed a law allowing couples to divorce without having to appear in front of a judge and without the need for a power of attorney. The aim of this law is to make divorce easier. Although in my opinion," Dina says "this law will not help with this and in fact getting a divorce will be more difficult. In complicated situations partners will definitely need advice from an expert such as a lawyer or a mediator." Studying law at the University of Groningen wasn't just something she got to pick out of a hat. In

order to apply for International and European Law the student has to meet the required GPA. "Exams and lectures are difficult and the professors consider you a lawyer at law school. You have to be a scientist, think like a lawyer, and actually be a lawyer. They constantly challenge you by expanding on the effect of the law. Courses aren't just theoretic. The compulsory pleading courses prepare students for moot court. This style of education has prepared me well for my career." Dina expects the pressure for high performance to continue after law school, as doing the Bar takes three more years. This means three years of post-doctoral education, examinations and taking practical courses to acquire your points. "I have learned so much during these four years in law school. Not just by being shaped into a young law professional, but I have also gained so much by way of life experience. I have always felt the need to help others. But I learned too that before you help others, you should help yourself. It's

the key to finding balance in your life." The Faculty of Law encourages its students to be active. Competition between students is high. They accelerate by doing exchange programmes and running plea contests. Various student organisations connected to the Faculty of Law also encourage students to compete. There is even a plea society law students can join to plea against each other. "This is one of the reasons I would recommend the University of Groningen to others. You can get the best out of yourself." Students also get the opportunity to practice during their studies by consulting clients. Dina acted as a legal consultant for student organisation SOG, advising them on housing law.

WORK EXPERIENCE

Dina recently interned with VerdonkAdvocaten, a law firm in Heerenveen in the Netherlands. "I was a paralegal to lawyers in the family and criminal law department. Being a trainee in a law firm was one of my best learning experiences. Although it was for a short time it definitely opened my eyes to so many aspects of life and gave me a clear confirmation that I really wanted to become a lawyer." She has also worked at a tax office providing information on surcharges and did charity work for UNICEF. "The only way to understand the problems of society is by participating in society." Currently, she is working as a tutor at Capita Selecta, a student organisation which provides homework guidance to law students. There she provides several law courses on areas including civil procedure, contract and family law. "I am very busy but doing all this makes me truly happy. If you have the right attitude and mindset, you can have it all. Like they say, a positive mind gives a positive life. Try to surround yourself with positive people and they will lift you higher. And most importantly, stay true to yourself."

AMBITIONS


Dina's ambitions are clear. She is interested in practising international private law and business law. It is her dream to work in Dubai and she wants to become a lawyer. "It would be amazing if I could get a job in Dubai and start my career in the UAE. I can see myself working there as a lawyer or a legal consultant. If I get the chance I would definitely immigrate to Dubai immediately. I'm open to new challenges and a future in Dubai."

Being a trainee in a law firm opened my eyes to so many aspects of life and gave me a clear confirmation that I really wanted to become a lawyer."

Heading into unexplored territory? **We're there.**

Our far-reaching global footprint brings with it far-reaching knowledge. This allows us to deliver bold new ideas in established markets and react first in emerging markets all around the world. From complex regulation to local laws and customs, our experience allows us to tackle the terrain with certainty. So whether your next step represents geographical or intellectual progress, you can feel confident taking it with us.

Law around the world
nortonrosefulbright.com



Financial institutions | Energy | Infrastructure, mining and commodities
Transport | Technology and innovation | Life sciences and healthcare

Did you know... where all the wigs and gowns come from?

“Robes and gowns had traditionally been worn since medieval times to display educational attainment and social status.”

Wigs were first seen in court in the 1660s in England during Charles II's reign. At this time it was common to wear a wig in polite society. However, it took some time for the practice of judges wearing wigs to be accepted as a standard norm for all the judiciary. Although, the late 1700s saw a decline in the popularity of wigs in England, bishops, coachmen, lawyers and judges still wore them. However, there were changes. The full-bottomed wigs judges had worn in the past continued to be worn in criminal trials up until the mid 1800s, but judges started wearing shorter wigs for civil trials in the 1780s. Today, judges tend to wear the smaller wigs for court hearings, and save the full-bottomed ones for ceremonial occasions. Sadly, the wigs were not the most convenient thing to wear. Initially, a huge amount of effort was required to maintain them. As a result many ended up giving off a heavy odor and there were even cases of them impairing judges' hearing.

In fact, these problems remained until Humphrey Ravenscroft patented his wig in 1822 and it is this type of wig which is still worn by legal professionals today.

As to robes and gowns, these had traditionally been worn by people since medieval times to display their level of educational attainment and social status. It was not until the 1600s, when rulers began to standardise their organisational structure and procedures of governance that specific robe styles began to be required of various legal professionals. Ruling families would decide the colour, fabric, and length of the robe to be worn depending on the stature of the profession in courts. The most commonly worn, black robe comes from England. Legal professionals in England wore a black robe in mourning for King Charles II who died in 1685. Due to British colonial influence this legal traditional



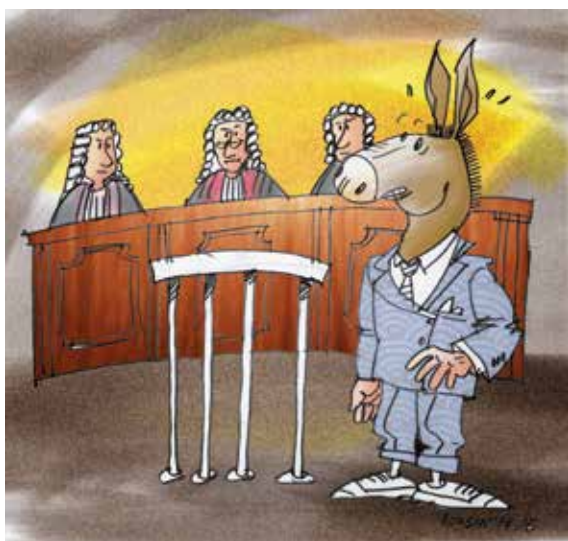
dress, variations of this black robe, commonly with red and white linings or trimmings, was exported and continues to be the most commonly worn attire for judges and some barristers in the world.

WHY ARE THEY STILL WORN?

But why do lawyers and judges still wear these gowns and in some cases wigs? Some say it is simply because no one has stopped them. Others believe the traditional wardrobe has more than a cultural purpose. The simple attire makes all practitioners look equal before the law and connects them with a shared duty to uphold it. There is one final view, however, and that is that it serves a purpose of presenting court professionals with a public display of authority.

Remarkable!

Donkey's Day in Court



Buddy is 300 pounds and about three and a half feet tall.

He is furry and well groomed. Buddy was no average witness, he was a donkey. In 2007, Buddy quietly came into the courtroom in Fort Worth, Texas, with his owner, Gregory Shamoun, to persuade the court that he was not guilty of the charges brought against him. Shamoun, a lawyer himself, had been sued by his neighbour, John Cantrell, who had accused Buddy of being 'a nuisance in the neighbourhood' and of 'causing Cantrell to not be able to use his luscious estate'. Cantrell claimed poor Buddy was being too loud and had left several manure piles. In fact, Mr Cantrell told the court, 'They bray

a lot. Any time day or night. You never know when they're going to cut loose.'

Originally, it seemed this particular conflict had stemmed from a land dispute. Cantrell was upset about a shed Shamoun was building in his backyard. Cantrell then said that Shamoun was simply using Buddy to get back at him for having com-

plained about Shamoun's shed. Mr Cantrell stated that one particularly convincing point was that Buddy usually stayed at Shamoun's ranch in Midlothian, and was only brought to the backyard during the dispute regarding the shed. However, Shamoun claimed he had brought Buddy over as a surrogate mother for a calf that needed to be fed in Dallas.

As Shamoun explained in his interview with CBC

Radio: "Instead of introducing pictures of Buddy, I thought maybe the best evidence would be Buddy showing up in front of the jury so they can judge him face-to-face".

Buddy, the donkey behaved perfectly in court. He maintained silence and was very calm. In fact, the jury did see that Buddy maintained his composure and did not lose control of his bladder in Court, during the jury deliberations. However, Shamoun and Cantrell decided to settle the case out of Court. In the end, Shamoun agreed to buy portions of Cantrell's land and Cantrell agreed to withdraw the complaint, so it appears that this strange tactic did actually work.

By Definition...

De jure (latin: de iure)

Legitimate, lawful, a matter of law, according to the law.

De jure means 'from law' having complied with all the requirements imposed by law. De jure is commonly paired with de facto, which means 'in reality', 'in practice' or 'in fact'. When de jure and de facto are contrasted in a legal context, they are put to use instead of 'by law' or 'by practice'.

De jure expresses actions regulated by law, however the law may not be used as general practice or may not be practically in force. In such cases, the terms are merely used to describe a political or legal situation.

Where you have a de jure government it means the legal, legitimate government of a state and a government which is so recognised by other states.

In contrast, a de facto government would be in actual possession of authority and control of the state. For example, a government that has been overthrown and has relocated to another state would have de jure status if other nations refuse to accept the legitimacy of the new revolutionary government.

Another legal example can also be found in elections of supervisory boards. For example, if person A is appointed as the chairman of a supervisory board by law, but another person, B, is chairman in practice, this would be the case as A would be the figurehead covering up B's position.

"Cantrell claimed poor Buddy was being too loud and had left several manure piles."



Doing Business in the Middle East? So are we...

As the largest law firm in the Middle East, Al Tamimi & Company knows more than just the law. We pride ourselves on understanding the business environment in which we operate, benefiting the clients we work with.

We have the knowledge, expertise and cultural awareness to ensure that our clients are at the forefront of doing business in the Middle East.

16 Offices | 9 Countries | 330 Lawyers

www.tamimi.com



THE DUBAI MALL

THEDUBAIMALL.COM