SEPTEMBER 2018

CommsMEA

Critical analysis for telecommunications executives

An ITP Media Group Publication www.commsmea.com

OPPORTUNITY THROUGH CHANGE IN
SAUDI ARABIA

AVAYA'S FATEN HALABI:
REFOCUSING ON THE CUSTOMER EXPERIENCE

PREVIEW:
THE 2018 COMMSMEA AWARDS

+

THE IT SECURITY REVOLUTION

AIRBUS
AND THE EVOLUTION OF SECURE COMMS

THE FUTURE OF DATA

Data may be the "new oil." But the industry needs to talk about data security – and what it means for telcos now and in the future.


THE FUTURE
OF DATA
by Ben Mack

Data may be the "new oil." But we need to talk about data security – and what it means for businesses now and in the future.

Let's talk about data. First things first. One need only to scan the headlines to come to the following conclusion: people are more concerned about data security than ever before.

Much ink has been spilled discussing what this could mean for society going forward. Social media sites collecting information about users' habits and selling that information to third parties (and being, as Ellie Shechet of *Jezebel* reminds us, pretty shameless about the impact on democracy and basic human rights). Internet of Things (IoT) devices recording, and then sharing, our most private health data (as Sarah Burke writes in an utterly bone-chilling May piece for *Broadly*). The list goes on.

But despite the outcry, and rise of movements like #DeleteFacebook, it seems we're still more than willing to give up data in exchange for accessing technology (case in point: the recent revelations regarding data analysis firm Crimson Hexagon and misuse of Facebook user data). As Madison Sherman writes in her excellent *Teen Vogue* piece from April this year, "With every step toward progress in technology there will undoubtedly be a risk to users."

But what does all this mean for the telecommunications industry, particularly in the Middle East and Africa? Are things in Abu Dhabi, Nairobi and Riyadh different than in Auckland, New York and Reykjavik?

According to Henrique Vale, head of software for the Middle East and Africa at Nokia, the Middle East "is on a par with the rest of the

Tech advances aren't without risk, says Madison Sperman.

world, and in some cases, it is more advanced than the rest of the world" when it comes to how data is being used. He says the development of 5G services is an example of this.

Marwan Bin Dalmook, senior vice president for managed services and smart city/smart government initiatives at United Arab Emirates-based telco du, says something similar.

"Countries in the Middle East region are increasingly digitally transforming into knowledge-based economies," he says. "With increased connectivity, it is data, and specifically big data, that is enabling this change for the first time in a cost-effective manner across industry sectors. Data is very much the oil of the new era."

> "Countries in the Middle East region are increasingly digitally transforming into knowledge-based economies. With increased connectivity, it is data, and specifically big data, that is enabling this change for the first time in a cost-effective manner across industry sectors. Data is very much the oil of the new era."
> **Marwan Bin Dalmook**

He adds: "The Middle East and Africa region alone is projected to post the world's-fastest mobile data traffic growth rate from 2013-2018, and the fastest increase in business IP traffic, according to the Cisco Visual Networking Index Global Mobile Data Traffic Forecast for 2013 to 2018. Organisations that are not prepared for this data deluge risk being swept away."

Worrying stats

But just because data is being used for innovative services – like smart cities projects, personalised healthcare and more – doesn't mean there isn't a serious risk of it being misused.

"Perhaps the biggest risks are the most obvious ones – abuse and retention violation of data privacy," Bin Dalmook says. "As data becomes more 'open' and accessible, the need to have a concerted effort globally to ensure citizens' privacy is very evident."

There are some worrying stats specifically about the Middle East region.

In early July, digital security firm Gemalto released the findings of a major study into data and Middle East businesses. The fifth edition of the Data Security Confidence Index – which surveyed 1,050 IT decision-makers and 10,500 consumers worldwide – showed 56% of Middle East-based organisations cannot analyse or categorise all the consumer data they store. Even more concerning, almost one-third of Middle East companies (32%) reported they did not know where their sensitive data was being stored.

Gemalto regional director for the META (Middle East, Turkey and Africa) region, enterprise and cybersecurity Sébastien Pavie says that's concerning.

"If businesses can't analyse all of the data they collect, they can't understand the value of it – and that means they won't know how to apply the appropriate security controls to that data," he says. "Whether it's selling it on the dark web, manipulating it for financial gain or to damage reputations, unsecured data is a goldmine for hackers."

He says more: "You only need to look at the recent hacks on Facebook and, closer to home, on the riding app Careem to see the damage that can be done. What's more, data manipulation can take years to discover, and with data informing everything from business strategy to sales and product development, its value and integrity cannot be underestimated."

The Careem example is particularly relevant. Earlier this year, Careem revealed it was affected by a cyber-attack that resulted in the data of more than 14 million customers and 558,000 drivers in the Middle East, North Africa, Turkey and Pakistan being stolen. While the company claimed there was no evidence people's passwords or credit card numbers were compromised, it did reveal that names, email addresses, phone numbers and trip data of anyone who signed up for Careem prior to January 14, 2018 was swiped. Covered extensively by international media including *Forbes*, *CNBC* and *Gizmodo*, it did not escape media outlets' attention that Careem didn't admit to the breach until April 23 – more than three months after it occurred.

While such a massive breach might prove fatal to a business elsewhere, Careem's Middle East investors seem not to care – possibly because many Careem customers pay with cash when using the service, unlike companies such as Uber. Since news of the breach broke, Careem has announced plans to invest US$150 million to launch a food delivery business, and is reportedly in talks to secure another US$500 million from investors while also exploring potentially merging with Uber.

Uninformed consent

Writing for *The New Yorker*, Louis Menand

Violet Blue, author of *The Smart Girl's Guide to Privacy*, says companies are playing it to their advantage to keep people in the dark about data.

points out a bigger issue isn't necessarily data being stolen, but data being used as companies see fit without users giving informed consent. He points out that Facebook's infamous Cambridge Analytica scandal wasn't the result of hacking, but users unknowingly giving Facebook permission to sell their data.

Of course, concerns about what data might be used for aren't new. As Violet Blue, author of *The Smart Girl's Guide to Privacy*, says in an insightful 2015 interview with *Bitch Media*'s Sarah Mirk, "There's a lot of wilful misdirection going on here with companies that are playing it to their advantage to keep people in the dark."

Scholars have been sounding the alarm for more than a decade, as Alexis C. Madrigal writes in a March article for *The Atlantic*. In a piece for online cybersecurity project *Chupadados*, Tatiana Dias and Joana Varon (in collaboration with Yasodara Córdova, Raquel Rennó and Camila Agustini) describe the implications, arguing companies are "using thin arguments to gain uninformed consent in order to use the data of those who consume its services, leaving a margin for a series of abuses."

Trouble for telcos

Today, there's a growing worldwide distrust of what companies might do with data. And it's having a negative effect on telecommunications companies.

In July, *Reuters* and Australian outlets such as *The Sydney Morning Herald* reported that the Australian government was strongly considering banning Chinese telco Huawei from supplying equipment for its planned 5G broadband network. Among the reported reasons for considering a ban: fears that the Chinese government could force Huawei to hand over data about Australians.

Amit Sanyal, vice president and executive head of consumer value solutions at Indian telco Mahindra Comviva – which has operations in more than 95 countries, including throughout the Middle East – says keeping user data secure while also monetising it is an "interesting conundrum" for telcos.

"On one hand, companies the world over have rapidly jumped onto the big data bandwagon," Sanyal says. "After all, which player wouldn't want an effective medium to glean actionable insights about their customers? On the other, though, lots of companies are now looking for new ways to leverage big data to the fullest."

Requirement for responsibility

Muetassem Raslan, regional sales director for Ruckus Networks – a company which sells wired and wireless networking equipment and software – in the Middle East, says businesses and organisations have a responsibility to keep data secure, particularly if they want to retain customers in the future.

"With everything comes trust," he says. "You have to make sure it's secure. You have to make sure it's used in a proper manner."

Alaa Hadi, regional director for high growth markets in Russia/CIS and the Middle East at network security software company Netscout Arbor, says something similar.

"Data is growing exponentially for all organisations. That means that as we go forward, analytics become even more important. How can you mine the data to derive valuable insights into network or application performance [and] subscriber experience? Analytics and open platforms will be the focus going forward."

Many others have also stressed the responsibility organisations have in not misusing data – and how, by being responsible, they can actually make more money, since consumers will trust them. Nokia's Vale, for one, says this increased focus on data responsibility can be a big opportunity.

"Telco service providers have access to unprecedented amounts of data, including consumer profiles, device data, network data, usage patterns, location data, apps downloads, etc. Telecom operators today are among the world's biggest aggregators of consumer data, and the volume of data will only continue to grow in the times to come."

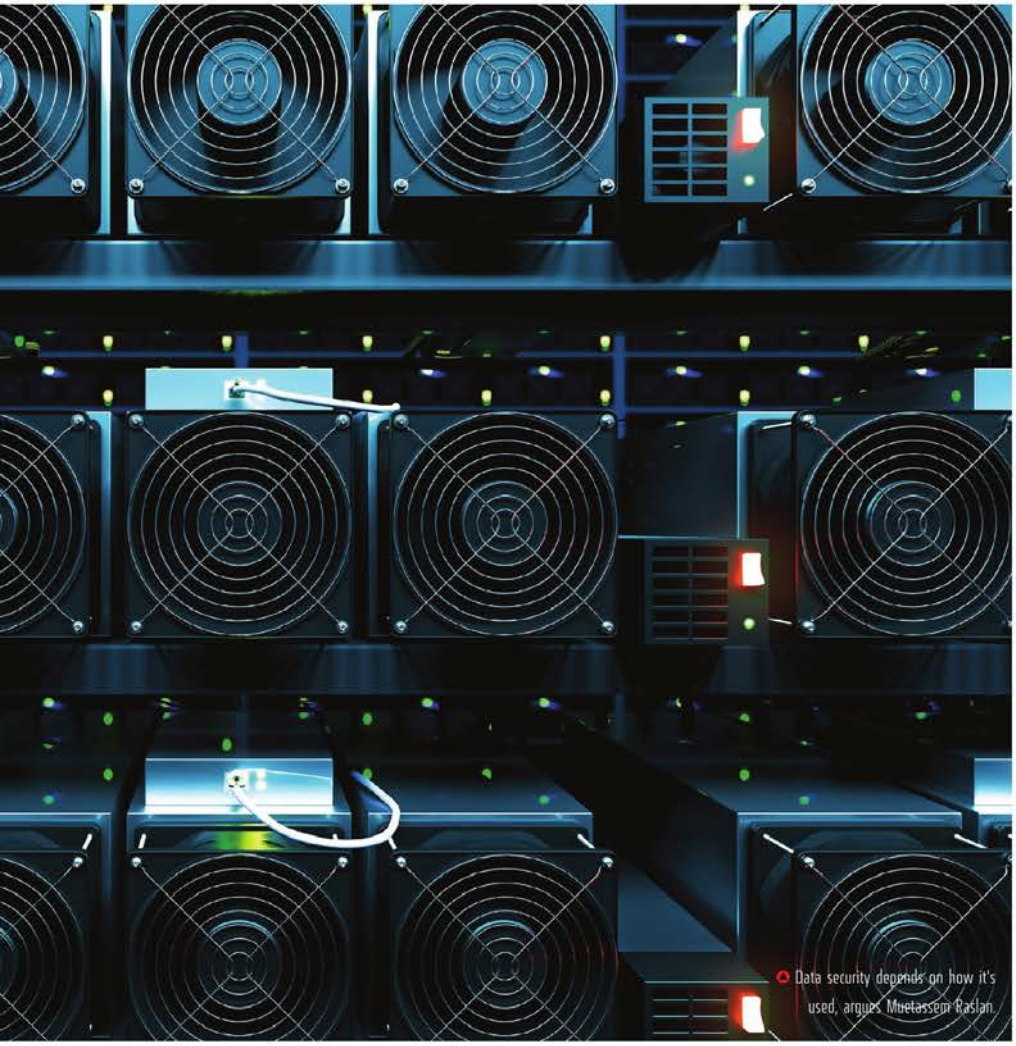
GDPR and the Middle East

Almost as many column inches have been devoted to discussing Europe's new General Data Protection Regulation (GDPR) as data security itself. Coming into force this past May, the law – among many other protections and requirements – stipulates that processors of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any

third parties or outside of the European Union. Further, people residing within the EU or European Economic Area have the right to request a copy of the data collected, and the right to have their data erased under certain circumstances. Businesses must also report any data breaches within 72 hours if they have an adverse effect on user privacy.

Mansoor Sarwar, technical director at Sage Middle East, says the GDPR doesn't just have big implications for Europe. "Even if Middle Eastern telecommunication players do not have a direct presence in Europe, they are also impacted because they handle the personal data of European residents and citizens."

Patrick Grillo, senior director for solutions



Data security depends on how it's used, argues Muetassem Raslan

marketing at cybersecurity company Fortinet, says he believes the GDPR will be the first of a wave of data protection legislation around the world – including in the Middle East.

"For many businesses, customer confidence is already being influenced by their perceived risk of conducting transactions online, or whether their personal data is at risk of being compromised or stolen. Meeting or exceeding regulatory requirements will go a long way towards assuaging those concerns."

He adds new data rules can be an opportunity for businesses. "It is better to view them as an opportunity to achieve competitive differentiation, as well as a way to drive greater customer confidence and trust."

Alain Penel, Fortinet's regional vice president for the Middle East, says the GDPR needn't be a headache – and many issues can be mitigated with good organisational systems.

"Organisations need to be able to demonstrate compliance through appropriate governance measures, including detailed documentation, logging, and continuous risk assessment. There is an added expectation that security should, as far as possible, be an integral part of all systems from the outset, rather than something applied in retrospect."

The future

Naturally, discussions about data inevitably lead to that "F" word: the future.

Mahindra Comviva's Sanyal points out the importance of organisations listening to their customers when it comes to data security – and letting people know what's happening with their data. He adds this will become even more important with the introduction of 5G services for consumers.

"The age of data will, clearly, continue, spurred on by the rollout of 5G networks and the proliferation of smartphones," he says. "What's important to remember is that it isn't enough to be at the forefront of big data deployments amongst one's peers. Security counts too. After all, customers trust you with their data."

The du smart city/smart government initiatives and managed services senior vice president Bin Dalmook also says telcos have a key role to play in future developments.

"The future in unseen, but we believe the move towards a more virtualised world is certain," he says. "We expect most regular day-to-day transactions and interactions will be supported by data insights as a default feature for most businesses once the technology is made more accessible to the masses. This means further reduction in investments in physical assets by organisations, and more traction in 'on-demand' services that can handle the vast amounts of data.

"This is likely to accelerate the need for a new breed of data scientists, who can work on more creative varieties of use cases, and the emergence and normalisation of data science everywhere is another expected outcome as well."

Ruckus' Raslan stresses the need to "go back to basics," despite changing technology and new ways of generating revenue.

"The UAE in particular, and the Middle East in general, are leading with smart cities and big data," he says. "You just have to visit GITEX. This is only the beginning with the new technology that's coming.

"Information is everywhere now. Data analytics is playing a big part in shaping our future. We're going to depend more and more on it. It's going to enhance every part of our living."

He offers more advice for telcos – and really any organisation – that may just be at the heart of the debate about data.

"Data security really depends on how you use data. The best way you can keep data safe is to use it in the right way."