KPMG

The Internet of things

Should we embrace Its full potential?

kpmg.ch/cyber

WELCOME TO OUR CYBER INSIGHTS MAGAZINE.

In this edition our cyber security professionals express their views, sometimes conflicting, on the dawn of the Internet of Things and the possible impacts on privacy, business, and wider society. It is a contentious topic that divided opinion within the team. But instead of forcing a consensus, we created a platform to allow our subject matter experts the space to have their say.

The views and opinions expressed herein are those of the authors and do not necessarily represent the views and opinions of KPMG.

For more insights on the future landscape of cyber security go to **kpmg.ch/cyber**

CONTENTS

NARRATED BY **KEN HALL**

Ken is a partner in KPMG's Cyber Security practice. He has over 30 years of IT consultancy and security experience and has worked in a number of sectors, including finance, media, telecommunications, energy and utilities. Prior to working for KPMG, Ken created SAC's cyber security business in Europe, and worked for Wipro where he set up and ran their global cyber consulting business.

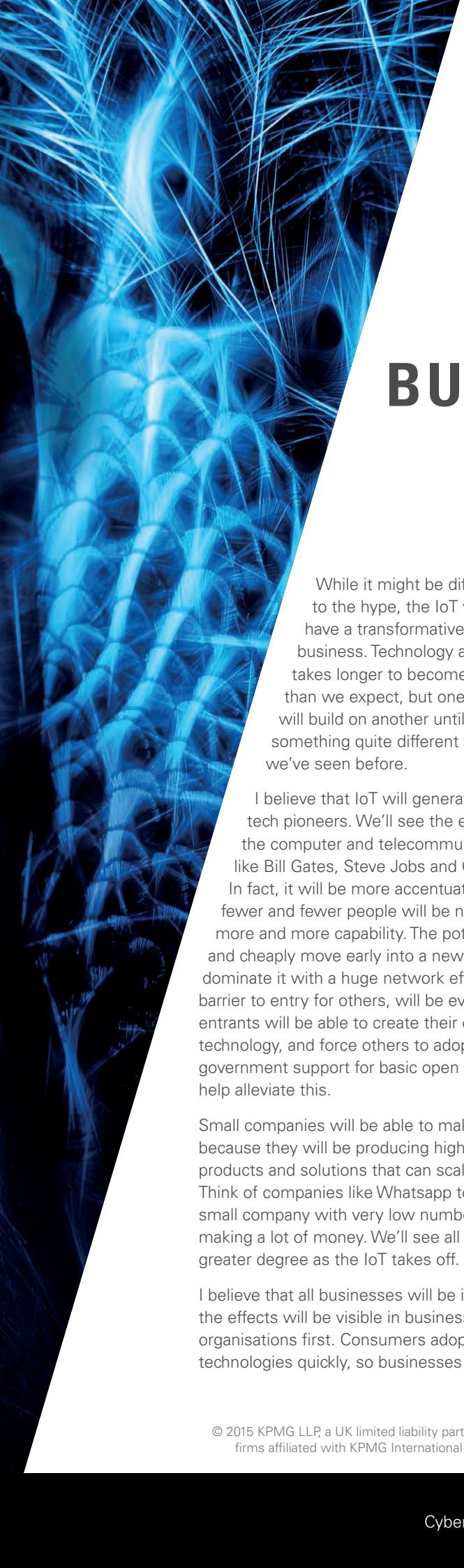
The Internet of Things (IoT) is set to revolutionise society in much the same way as the arrival of the Internet. While not all the technology is yet in place, the signs are clear. The IoT is on its way. But what exactly is this technology?

The IoT is the connection of a multitude of devices to the Internet and each other. Beyond the obvious smart TVs and cars, devices that none of us thought needed any level of awareness will be installed with sensors ushering in the era of big data. The connections between these data streams and their analysis will allow for huge advances in intelligent systems.

Arguably, a more important question is, what does this mean for all of us? My colleagues and I take a look at the impact that this technology will have on business, plus some of the potential opportunities and pitfalls. The following pieces are opinion, although there are markers in the road, none of us has a crystal ball. Some are positive, some predict a bleak future, but forewarned is forearmed.

To open our theme, Anthony Hess explains a bit more about the IoT and examines its likely impact on the business landscape.

> The Internet of Things is set to revolutionise society in much the same way as the arrival of the Internet.



THE INTERNET OF THINGS WILL TRANSFORM THE BUSINESS LANDSCAPE

While it might be difficult to live up to the hype, the IoT will eventually have a transformative effect on business. Technology almost always takes longer to become widely adopted than we expect, but one development will build on another until we have something quite different from anything we've seen before.

I believe that IoT will generate incredibly rich tech pioneers. We'll see the equivalents of the computer and telecommunications titans like Bill Gates, Steve Jobs and Carlos Slim. In fact, it will be more accentuated because fewer and fewer people will be needed to deploy more and more capability. The potential to quickly and cheaply move early into a new market and dominate it with a huge network effect creating a barrier to entry for others, will be even larger. Early entrants will be able to create their own standard technology, and force others to adopt it. Although government support for basic open standards could help alleviate this.

Small companies will be able to make big profits too, because they will be producing highly automated products and solutions that can scale really quickly. Think of companies like Whatsapp today – a very small company with very low numbers of people making a lot of money. We'll see all of this to a greater degree as the IoT takes off.

I believe that all businesses will be impacted, but the effects will be visible in business-to-consumer organisations first. Consumers adopt new technologies quickly, so businesses that serve them will have to keep up. Tech companies of course will be at the forefront, but other B2C sectors like retail will need to quickly catch up.

Over the past few decades, technology transformations have happened in waves. Early computers sitting in massive server rooms were followed by smaller and smaller machines until we had desktop computers. The next wave was the connection of these PCs to each other and to the internet. Now we are seeing these two trends collide into the next big wave – the IoT.

> "Internet of Things will generate incredibly rich tech pioneers"

It is inevitable that we will see increased automation. As with the previous waves, this will happen because some enterprising technologist believes it is possible and also because some clever businessman sees profit in it. Objects that were never 'computers' will become computers, connected and processing data.

Think of desk phones. In the past, physical phones were connected to their own network and without any digital capability at all. Today's telephone has changed from dumb hardware to software running on hardware and now many people have virtual desk phones that follow them everywhere.

With more and more objects becoming connected both at work and at home, more and more data will flow from these simple systems into large databases from where correlations and decisions can be made. This will naturally reduce the need for human intervention. Whereas in the past you might have a lower level manager analysing a set of data and then sending a report to his/her superiors, in the future the technology will do that without human participation.

I think we'll see more hyper-localisation like iBeacons, where a consumer gets messages to their phone depending on where they are in the store. With all the information that customers give to a retailer or consumer goods company about their habits and spending patterns, the technology will be able to make marketing decisions – without needing a marketing person to make them. So technology will change people and back office requirements alike.

> Everyone will need to be more IT literate, just as the average worker today needs to be more IT literate than his or her counterpart in the 1970s.

There will be dramatic effects in business-to-business companies too. The dynamics between buyers and suppliers will change – devices will automatically talk to each other when a product is running low, for example. There will be more automation around the tracking of an order and around the analysis of the quality and performance of parts and materials supplied.

One of the great changes to organisations wrought by connected PCs was the flattening of management structures. This will continue with the IoT. Many white collar middle management roles will disappear. Many front line supervisory roles will also follow the trend that has affected blue collar jobs for more than three decades.

The need for people will shift. We will need more highly skilled technical workers such as cyber security experts, systems architects and project managers. Everyone will need to be more IT literate, just as the average worker today needs to be more IT literate than his or her counterpart in the 1970s.

Even services businesses like consultancy or accountancy could be affected. Anything that doesn't require human creativity and judgement will be replaceable as automatic information flow and analysis increases. People in these businesses will need to think of new ways to bring valuable insights on top of the automated analysis.

The IoT will also have an impact on companies' need for support staff. Security staff, catering staff, cleaners – fewer will be needed as new technologies automate their functions.

The IoT will have an enormous effect and reach into all areas of business. In a few decades' time, the landscape will be completely transformed.

BY **ANTHONY HESS**

Anthony Hess is a Senior Manager in the Cyber Security practice at KPMG. He leads the firm's work in Cyber Insurance and Cyber Incident Response. Anthony came to the UK and joined KPMG in 2012. Prior to that Anthony was with Raytheon, a large US Defence company where he was focused on Enterprise Architecture.

It is undisputed that the IoT will have a huge impact on business, and does present some real opportunities for those who are able to keep pace with the technology. This development of the necessary tech is speeding up, but to quote the famous Smiths song, how soon is now? Ben Ramduny explores the timeline of the arrival of the IoT.

THE INTERNET OF THINGS –TIMESCALES FOR WIDESPREAD ADOPTION

We have devices with a real use-case which are connected to the internet now, like smartphones, cars, laptops and televisions. For me, the IoT is all about connecting devices that have no use-case for connection to the internet, like your shoes, your carpet or light bulbs for example, and then finding a use for them through the fact that you've got a myriad of things in an intelligent network.

The IoT as I envisage it will really start to come into play in 10 years from now. The interconnectivity of multiple devices will be driven by the big data-hungry companies, which are keen to access your data to deliver tailored advertising to you and by 2035 it will be fully embedded in all our daily lives.

Initially, access to the IoT will be restricted to those with money, as the early adopters will have to pay a premium for their smart gadgets. Despite that division between the haves and have-nots, I don't foresee this creating any major problems. The IoT will not be giving you anything tangible – it's a nice to have rather than an essential in life – if you don't have a device to switch on the lights from your phone, you'll use a light switch.

Ultimately though, the cost of technology will fall. Just as flat screen TVs were out of the reach of most people fifteen years ago, now they retail for a couple of hundred pounds at our supermarkets and tech companies are already announcing that their products will be IoT enabled by 2020. It will also be in the interest of the data collectors and advertisers to make it available to everybody, as this will enable them to target products and services to a wider swathe of the population. There will be a push to reduce the cost of the technology to the point where it is only a few pence more to manufacture a device with a sensor included. Gradually, IoT devices will become ubiquitous.

> There will be a push to reduce the cost of the technology to the point where it is only a few pence more to manufacture a device with a sensor included.

While it is entirely possible to live without this technology, rather like owning a smartphone today, once you've experienced using it, you're unlikely to want to go back to life without it.

I think there will be a development in the way that devices are networked, and rather than connecting to a central point, they will link to each other, creating a stream of data from their various sensors. It is by the linking and cross-referencing of this data by intelligent applications that the IoT will be able to produce real change within our home or working environment.

For example, if you've installed a sound monitor in the light bulb sockets it will be able to tell if you are having an argument and adjust the mood lighting to try and calm things down. Equally the carpet might communicate with the doors, lights and radiators, to switch bulbs on and off, and move the heating grid around as you move from room to room. While it is entirely possible to live without this technology, rather like owning a smartphone today, once you've experienced using it, you're unlikely to want to go back to life without it.

We're already seeing devices being linked together with heating systems you can control remotely, and trials of smart fix services, where the utility company will know your boiler needs repairing before you do. Given these developments, I'd say that we'll see the arrival of connected devices in most tech-savvy homes within around five years.

Advances in wireless and sensor technology will reduce the cost of smart gadgets like light switches, pens or other devices which don't appear to have a huge amount of practical use initially but have huge cachet for the early adopters. In the meantime, there will be a demand for smart devices where there's a clear use case, maybe an iron that can let you know remotely if you've left it on. As ever, manufacturers will produce goods if there is money to be made.

BY **BEN RAMDUNY**

Ben is an Enterprise Security Architect in KPMG's Information Protection team having joined in 2010. Ben works with a range of clients across all business sectors and size to help them defend their systems against cyber attack. Ben specialises in network security and the consumerisation of IT. Prior to joining KPMG Ben worked on IT security projects at the Olympic Games, and prior to the Olympics Ben worked at Fujitsu providing network architecture for large government outsource contracts.

A new era of data collection and analysis also means a new concept of privacy. We already hand over our personal data to online retailers, banks and other businesses in return for services. This trend will only increase with the IoT as devices collect information about our health, our movements, buying patterns, viewing preferences...the possibilities are endless. Information about customers is valuable and traded in today's market. With so much data being produced and collected, Milda Petraityte asks what privacy will mean.

THE INTERNET OF THINGS WILL RENDER PERSONAL PRIVACY OBSOLETE

We are all going to have to get used to less private lives. Handing over personal information must become the norm if we are to reap the benefit of the IoT.

We need to be wary of giving away too much too quickly, but in the same way as applying filters to a search on the internet, the more detailed information you give, the better the services provided will be. If you don't let your smart fridge track what's in there, it can't know to alert you if you're running low on milk. If you don't let it know that you prefer fat-free, how can your supermarket supply you with the correct product?

> The question arises of how to secure this sensitive data and prevent it from being used against the individual.

This movement has already begun with the advent of smart technology, such as TVs that ask for your date of birth, and in some cases, even your children's birthdays in order to supply you with tailored advertising, services and control. Many people quite happily hand over personal data now, without any thought as to the consequences of their actions, in a market where personal data still has a lot of value.

The IoT will not arrive with fanfare and an explosion of media attention despite its potential to change our lives so fundamentally. Instead I think it will be a gradual creep, as interconnected devices begin to gather data on us. With some number crunching in the background, this will allow for the provision of specially tailored services to make our lives easier.

The nature of the personal data being collected will also change. It is not going to be specifically things like dates of birth or pin numbers, it will be the minutiae of your daily life. What toothpaste you use, your sleeping patterns or what brand of orange juice you prefer. Many people will be happy to hand over this information in return for the provision of services such as automatically topped up shopping lists or a pillow or bed that adjusts its settings as you sleep for example.

Wearable devices that give an indication of health, such as heart rate or cholesterol levels will give businesses the opportunity to suggest services in return, such as specific treatments or reduced price health insurance for example. Monitoring sufferers of chronic health conditions would also allow for an immediate response to any crisis. However, the question arises of how to secure this sensitive data and prevent it from being used against the individual.

The technology is advancing exponentially. Cisco estimates from 2014 claim that the number of devices connected to the internet will swell from 10 billion in 2013, to around 50 billion in 2020.[1] The sheer volume of data that's likely to be generated and interpreted means that data protection as we understand it today is likely to become irrelevant. While it is possible to have all sorts of policies to attempt to protect our data, when there is so much of it, it will become almost impossible to track it all.

Controlling the way personal data is used is going to be a challenge, despite the argument that more advanced data protection policies or technologies could be invented to protect personal privacy. That is a particular concern for older generations in individualised Western societies who don't want to hand over too much information. In fact the government are encouraging the regulators to slow down adoption with legislation.

> If we want to live in this interconnected world, there will be no point in hanging on to outdated notions of privacy.

But is the current situation very different? Today we have to trust companies to use our information responsibly. It is impossible for every individual to know how their data is processed and utilised, and we already know that there are other processes around our data such as information selling, market research and third party access.

If we want to live in this interconnected world, there will be no point in hanging on to outdated notions of privacy, because you give out so much there's little left to hide. You can already see ideas around privacy changing as young people who post so much of their lives on social media are particularly open to sharing and the notion that at least part of their lives is lived in a public space.

The technology will have to advance to meet new challenges, such as how to trade securely online without using personal data for the means of identification. I wonder if this might involve using avatars in some way. This looks like the death of privacy.

Future thinkers will have to find ways of identifying individuals if personal data is common currency. Maybe wearable devices will provide a confirmation of our identities instead? It seems that the volume of data, and the level of sharing will be so vast that every problem solved will throw up another set of issues.

Currently personal data is valuable, and is traded on the black market as it's used to access goods or services. I think that the law of supply and demand affects everything and this may no longer happen in the future of the IoT, as the surplus of information will render it worthless. Personal data will cease to be of interest to hackers if it is all just out there already.

This would be good for companies worried about the cost of data loss or theft. Whether it is so good for the individual is unclear, as this will depend on how the society of the future will use all this personal information. While some people, particularly younger generations who are used to living at least part of their life in public may find it easy to adjust, the pace and scale of change may be tricky for those of us used to keeping our preferred toothpaste brand to ourselves.

[1] http://www.cisco.com/web/about/ac79/docs/IoE/IoE-in-ASEAN.pdf

BY **MILDA PETRAITYTE**

Milda has joined KPMG after more than five years of experience in Information and Knowledge Management two of which she spent working in a legal company. She is the middle of her 2nd Master in Information Security and is currently working on a cloud forensic investigation project.

One of the major sectors likely to benefit from the IoT is health. From opening up of new clinical models via remote monitoring, to the collation of research data, the outlook is overwhelmingly positive. Luke Solon takes the pulse of the changes.

THE INTERNET OF THINGS WILL RADICALLY IMPROVE HEALTHCARE

The IoT will have a huge effect on healthcare. We need it to. Demand for healthcare is greatly out-stripping current supply as we all live longer. In the US as of 2012, it accounts for 18% of GDP and in the UK it's around 10%.[2] We have to reduce the unit cost of delivering healthcare and the best way to do this is through technology.

I believe the IoT will be a big enabler. It will affect the setting of care – you won't have to be physically in front of a doctor. It will move care to your living room. Already we're seeing start-ups offering consultations over Skype and the creation of online pharmacies. People will be able to access care at any time through their smartphones (or whatever comes next) and could even have consultations with specialists in other countries.

It will also greatly improve the quality of healthcare. By better linking you to your clinician, he or she will be able to deliver much more timely care. Doctors often wish that their patients had come to them earlier, before a condition had progressed. In the future, medics will be able to give real-time diagnoses and offer quicker treatment thanks to biosensors linking to smartphones that relay live information. Novartis and Alcon have already developed an internet-connected contact lens that measures blood sugar levels through tears in the eye.

Such biosensors will yield a greater volume of data which will lead to the development of better algorithms on which to base decisions. The technology will be able to flag diagnoses with a recommended treatment which a doctor could then approve.

We have also seen the development of a pill that transmits biometric data through the skin so that doctors can gain a better understanding of the likely effectiveness of a medicine and when best to take it according to your physiology, weight, sleep patterns and so on. The IoT will open up the possibility of much more nuanced and sophisticated treatment.

> In the future, medics will be able to give real-time diagnoses and offer quicker treatment thanks to biosensors linking to smartphones that relay live information.

Doctors may be worried about being overwhelmed with data, but I think it will actually be a good thing for them. By empowering patients, it will also mean that they have to take more responsibility for their own health. At the moment, doctors assume too much of that burden.

[2] http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS

Imagine if a biosensor could detect that you are lacking in vitamin C or a pregnant woman is short on folic acid and then order more of a product via your internet-connected fridge.

It will also help identify poor standards of treatment much earlier so that corrective measures can be put in place. It will help eliminate unacceptable clinical variations such as we saw at Mid-Staffordshire Hospital for example.

It's not just diagnoses and consultations that will change – in time, the IoT will revolutionise operations too. As far back as 2001, the Da Vinci robot carried out a gall bladder operation in France with the controlling surgeon based in the US. Operations are a process – they can be broken down into distinct steps. Eventually there will be enough data points for us to be able to automate parts of operations. Closing a patient up could be done by a robot, for example, freeing up the surgeon to move on to their next op.

Diet will be another area where the IoT has an enormous effect. Through sensors and tracking apps, individually tailored diet plans can be created. Imagine if a biosensor could detect that you are lacking in vitamin C or a pregnant woman is short on folic acid and then order more of a product via your internet-connected fridge.

I understand people's concerns around data protection and cyber security, but these can be overcome. Many of us put much of our lives on Facebook and Twitter already anyway, so what really is the extra danger in medical records being accessed? It could be an issue with some sensitive conditions, but the great majority of us don't have that much wrong with us until we hit fifty or beyond anyway.

Everything else is becoming increasingly internet-based, and medicine needs to move with it. It is already happening. A new generation of doctors who trained in the email and internet age is just beginning to reach positions of leadership in the health service – that should help push through the step-change required.

We need these developments. The result will be reduced costs of healthcare, greater quality, and much greater patient empowerment. When we get it right, we will all benefit.

BY **LUKE SOLON**

Luke is an Associate Director in KPMG's Strategy Group where he is a member of the Healthcare and Life Sciences sector team. He serves clients across the healthcare, pharmaceutical and medical device industries. He is a qualified medical doctor with clinical experience across a range of in-patient specialties.

From the invention of the wheel onwards every advance has created disadvantages: the industrial revolution led to squalid working conditions, the combustion engine increased pollution, the internet enabled terrorists. The same is undoubtedly true with regard to the IoT. The advantages it will confer, need to be balanced against the possible future challenges.

Richard Krishnan takes a comprehensive overview of whether we really want this new technology, and some of the problems it could create.

ARE WE SLEEPWALKING INTO A MACHINE WORLD?

The widespread adoption of intelligent objects and infrastructure is a force for good, but it has a darker side. I fear that in the embrace of sophisticated innovations that are designed to make our lives more efficient and convenient, we will hand control of our personal information to big business and government.

> Will it take a massive security breach, or even a loss of life, before these issues really surface in national or global political debates?

In the UK, it seems that we are more enthused than afraid by the prospect of living in a small world. A KPMG survey in October 2014 of 1,600 people of all ages found that 66% believed the digital renaissance was exciting, while over two thirds (71%) believed that innovation is a force for good.[3]

The survey, however, did also highlight fears that greater connectivity could compromise our privacy and increase opportunities for surveillance as well as some curious cynicism about the need for everything to be digital. The same number who thought innovation was a force for good were also adamant that computers are our servants and not our masters.

I wonder whether the implications are being properly thought through. Who will control and monitor the data collected by ubiquitous sensors found in buildings, lampposts, water pipes, cars and even in domestic appliances such as microwaves?

Governments around the world are utilising the technology opportunities, teaming up with technology firms to try to solve a range of city problems from traffic congestion to recycling[4]. But in my view, the security and safety aspects of this brave new world are not being given sufficient attention and that, for me, is a huge worry. Will it take a massive security breach, or even a loss of life, before these issues really surface in national or global political debates?

[3] http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/NewsReleases/Pages/UK-public-fears-advance-of-internet-enabled-devices-amid-security-concerns.aspx

[4] Annual Report of the Government Chief Scientific Adviser 2014. Innovation: Managing Risk, Not Avoiding It. Evidence and Case Studies

> As individuals and communities, we have signed away our rights to own data in lengthy terms and conditions. The customer has become a means to an end.

Tomorrow's world has to have the individual and society at its core, and I believe that if things continue as they are, in 20 years' time consumers will discover they sleepwalked into a situation where they are at the mercy of big business, hackers and terrorists.

Stealth

One problem with the 'Internet of Things' is the stealth in which it is increasingly infiltrating people's lives.

For most people, going online has already ceased to be a conscious choice, and is fast becoming a social necessity. In a world where technology enables daily life, we will all be accessing a web of connected devices, whether or not we like it or are even aware. The main driver behind this technological progress will be companies seeking to gain market share and profits.

Of course, it is happening already. Our personal information, often with geolocation information is routinely sold by companies to marketing agencies and advertisers. Some people feel the benefit of this with targeted advertising and advice: "You liked this restaurant in Copenhagen, now you're in Madrid, try this place to eat."

Information has become a commodity freely traded. Whilst this may have benefits to some, the risks in aggregate will only get worse as the technology gets more sophisticated and industry moves quickly to take advantage.

Backlash

Might we see a user backlash that will check the technological advance? Our polling suggested that while there is an appreciation of the benefits tech advancement can bring to the home, cities and workplace, there is a line as to how far we want technology to go before the risks outweigh the advantages.

Of those interviewed in the KPMG survey 77% said they didn't feel the need for fridges that can automatically restock or communicate with smart phones and 60% said smart advertising hoardings pushed tailored advertising a step too far.[5] There seemed to be a yearning for simpler times, with just over half of respondents wanting to use their phone only to make calls. Although, as Henry Ford famously stated, "If I had asked people what they wanted, they would have said faster horses."

If we repeated our survey in 10 years' time, I suspect people would take many new products for granted, accepting the benefits and often unknowingly, the risks.

Information bundles

If we let our innate curiosity and thirst for innovation get the better of us, future generations may well find privacy to be a distant memory. Everything that defines us: our family and social networks, our health and financial data, our employment records – even our online conversations – will all be up for sale; all capable of being breached and spread, read by governments, insurers, employers… and criminals.

Our information will be packaged into products and services and sold for commercial advantage much in the same way that sub-prime mortgages were packaged into products and leveraged before 2008 to create massive profits for the banks. As individuals and communities, we have signed away our rights to own data in lengthy terms and conditions. The customer has become a means to an end.

[5] http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/NewsReleases/Pages/UK-public-fears-advance-of-internet-enabled-devices-amid-security-concerns.aspx

Human rights

There are many arguments for connected data. For instance, health data analytics will very likely help to prevent diseases and spot symptoms of illness early. But what happens when the same data is used to set our health insurance premiums, to determine our suitability for loans to even feed into our potential employability? Will advancements in predictive science and the availability of data make our risks uninsurable?

Will the use of such data be used by 'big brother' to encourage positive behaviours and punish those who prefer a glass of wine to an evening run or who drive instead of cycle?

> Barriers to entry are low for criminals, rewards are high and for the people at the top of the pyramid, the chances of capture are low.

Many of us willingly hand over our data because humans are instinctively trusting, and we want to desperately believe the dream that is sold to us in the media: that our lives will be healthier, easier, more interesting and enjoyable.

But in the post-Snowden world, we can see that once we lose our control of our data, it will be difficult to get back. Civil liberties and human rights are hard won, but easily surrendered.

Social inequality

Proponents of the IoT claim that technology will improve lives. But whose lives are we talking about? Will everyone be able to afford a technology-based existence? Will we live in a world where the rich have access to the most powerful tools and technology while those that cannot afford it are left behind?

Criminals and terrorists will have immense opportunities thanks to greater interconnectivity. Just think of the possibilities for cyber terrorists and state-sponsored actors to attack 'smart' transport networks and infrastructure, including planes and trains. Anything in the domestic supply chain could also be exploited, from smart TVs to fridges.

Meanwhile, a growing market in facilitating criminal behaviour, with malware and botnets available to purchase 'off the shelf' means increasingly that to commit a cyber-attack, such as extortion, you don't really need to have invested in owning much IT capability.

Barriers to entry are low for criminals, rewards are high and for the people at the top of the pyramid, the chances of capture are low.

As with any new technology, I believe criminals will outpace law enforcement until sufficient investment allows states and the private sector to get the basics in place.

No restraints

In speaking to police, they have often pointed out how the faceless nature of cyber crime and lack of proximity to the victim brings out the worst in people. Seemingly normal human restraint doesn't apply in these cases.

We've seen this with internet troll behaviour on social media. Imagine the multiplier effect when it comes to hardened criminals.

I believe the IoT will accelerate this in ways we can't even begin to comprehend. Connected devices will mean the points of attack will be almost limitless, because as with many new technologies, innovation will trump security.

But don't rely on government-funded security. The police won't be able to offer the same protection online that we have come to expect offline.

So, sooner or later the burden will pass to the consumer to take responsibility for their own online safety. At the moment it's like casting your most vulnerable people into the digital wilderness.

Silver lining?

There are undoubtedly many positives to centralised data and connected devices. Our lives will be more convenient in many ways, and the services which industry can offer will be many and varied. For the most tech-savvy users, the IoT will no doubt create many as-yet unexpected benefits.

But the risks can never be neutralised completely. It's impossible. The question for me is how we start to reset the balance, so that people have control over how their information is used and crucially have the right regulatory and legislative support in place to assert their rights. This needs serious focus as recommended by the Government's Chief Scientific Advisor (December 2014). Do I have the confidence this will happen? Not yet.

BY **RICHARD KRISHNAN**

Richard joined KPMG in 2005 and works in Infrastructure, Government and Healthcare Advisory (IGHA) – Performance and Technology. His market focus is Home Affairs and he specialises in criminal justice, primarily policing and security.

The best science fiction writing often presages advances in technology. The communicators in Star Trek predated the mobile phone, Jules Verne wrote about moon landings in 1865 and Australian laser physicists have recently developed a tractor beam. Naturally, none of the devices work in exactly the same way as their fictional predecessor. My colleagues and I have taken some of the possibilities thrown up by the IoT to some nightmarish conclusions. Sit back and be scared by these dystopian possibilities.

THE INTERNET OF THINGS IS A NET THAT WILL STRANGLE HUMANITY

LinkedIn founder Reid Hoffman jokes that the most successful online social network start-ups are those that tap into "the seven deadly sins".

In other words, celebrities tweeting their exploits show pride; politicians lambasting one another display wrath; investors gleaning market intelligence are greedy; teens 'sexting' are lustful, and so on.

I believe that our ancestors, over the course of millennia, captured the negativity of these 'sins' and developed a series of counteracting social norms and rules that keep societies glued together.

Yet, with each keystroke and mouse click, we seem to be embracing and craving more of Hoffman's 'sins' and allowing the web to erode our natural defences against sin – overriding community and society and our innate benevolence.

Huge advances in interconnectivity and the pervasiveness of the internet as it becomes embedded in our day-to-day lives will drive the next shift in the evolution of mankind, and the signs are not good.

My worry is that unless moderated, these advances will primarily be fuelled by mankind's darker side and overriding the benevolent qualities that have, since our origin, defined us. Indeed the IoT could become a catalysing ageing agent in the demise of our species.

Far-fetched? Look at the huge escalation in the number of calls from young women and girls to help-lines because young men are pressurising them into depraved acts that they have seen online. I believe the ability of young people to freely access this 'information' is poisoning our children's understanding of the world.

Society's inability to control this access is causing social norms to be rewritten in a regressive manner and is but one manifestation of our dying humanity.

> The boom of the M-PESA payments system in Kenya is, I believe, proof that the inter-connectivity of the world can be a force for good through its reduction of poverty and corruption in East Africa. However, I see the same money-transfer technology being used by militant group Al Shabaab to finance its terrorist campaign.

Don't get me wrong, the IoT has great benevolent potential in the way it allows us to embed sensors into everyday products and connecting them to networks.

The boom of the M-PESA payments system in Kenya is, I believe, proof that the inter-connectivity of the world can be a force for good through its reduction of poverty and corruption in East Africa.

However, I see the same money-transfer technology being used by militant group Al Shabaab to finance its terrorist campaign.

Meanwhile, a similar money-transfer technology, introduced to the Afghan Police Force to reduce internal corruption and the illegal roadblocks used to extricate bribes from citizens failed to achieve this objective. The only change was the architects driving the corrupt behaviour.

Similarly, the potential for benevolence abounds in data analytics. For example, our ability to use connected devices to interrogate huge amounts of data could enable medical conditions to be detected and dealt with in their early stages.

Like King Canute we cannot try to turn back the tide of the IoT, and in any event, we should embrace the opportunities and benefits that will arrive in a smart economy.

But we must make sure that there are systems in place to maintain the balance between the benefits of convenience and the curses, or risk society's longer-term welfare.

This balance can be achieved by the development and implementation of suitable legislation, regulation and progressive education. If we can get that right, then we might just be able to improve the human condition without stripping mankind of the glue that binds society and inspires collaboration for the good of all.

BY **CHRIS CROWTHER**

Chris joined KPMG Cyber Security division in 2013 following more than 20 years of leadership and management experience forged in complex project and programme delivery honed between UK military, other Government departments, the US military and Federal Government, the United Nations and international blue-chip organisations.

THE INTERNET OF THINGS IS PROPELLING US TOWARDS A DYSTOPIAN FUTURE

Wealthy consumers are now leaping so quickly from one generation of technology to the next that I predict this will drive an insurmountable wedge between the tech haves and the 'un-tech' in the not too distant future.

From iPods to Google Glass,[6] almost as soon as a piece of hardware becomes mass market, it becomes obsolete and the next application hits the market.

This is expensive technology and in my view this will eventually create an extreme and dangerous social divide that will have huge security implications and other damaging consequences for our world.

Currently, it is of little meaningful consequence if you cannot afford the latest tech-enabled eyewear or virtual reality headset. It's an indulgence. But we will shortly get to a point where we go from 'gimmick' wearable technology for business, entertainment or health purposes to microchips inserted into your body that could predicate whether you are actually allowed into certain areas and certain countries.

In the UK it is plausible that a growing threat from terrorism, untreatable diseases or crime borne from a widening equality gap could prompt the creation of a system that seeks to vet the people that come into the most desirable areas.

So say, for example, maybe you can only enter London's Canary Wharf with a micro chip that would screen you for disease? Maybe you need authorised technology to even get into London or other big cities from the surrounding country.

Those that cannot afford the technology required will be turned away, widening the social gap to the same extent as it currently is in many emerging markets and creating a mass 'un-tech' poor, where extremist ideologies will flourish.

> This is expensive technology and in my view this will eventually create an extreme and dangerous social divide that will have huge security implications and other damaging consequences for our world.

[6] 'iPod' and 'Google Glass' are registered trademarks of Apple Inc. and Google Inc., respectively.

> Our complacency in allowing business to make an increasing number of our decisions and choices will mean that eventually we lose a lot of our decision-making capability.

At the same time, the new and sophisticated technology that would link everything together and create this divisive system could expose people, businesses, cities and countries to untold security risks because we have not been doing security by design.

Nowhere has this been more evident than in the emergence of the Heartbleed Bug, a major security flaw at the heart of the internet that may have been allowing hackers to easily access users' details for years.

Legislators might pass more data, privacy and security laws but I don't think this would have much effect as regulation is typically responsive rather than forward-looking.

Developing countries will be most exposed to the risks of the IoT because of the huge leap in how their societies develop as a result. For many years, parts of Africa weren't connected to the internet, yet that's where many mobile innovations are coming from, including in finance.

Desperate need could drive world-leading developments in emerging markets but without the understanding of the security implications involved. This could play out particularly badly in areas that are geo-politically unstable and as cyber becomes the latest weapon of mass destruction, I believe we will all be exposed to cyber-savvy terrorists in an unprecedented fashion.

Apart from the safety and security risks, our complacency in allowing business to make an increasing number of our decisions and choices will mean that eventually we lose a lot of our decision-making capability.

We are sleep-walking into an Orwellian 'system' that is increasingly controlled by big business and state and from which it will become almost possible to disengage.

Taking the idea to its extreme, who can guarantee we will not become like drones, with chips inserted at birth, controlled by a matrix and designed to become whatever the system needs – from soldiers to builders?

We do not have much time to pull back from this empire of technology.

BY **KAROLINA OSECKYTE**

Karolina joined the KPMG Technology division in 2011. Karolina has experience as a User Change Management Lead for a Global Security transformation programme, as well as in other areas of Cloud Computing, Database Migrations, Project Management and Financial Auditing.

THE ROBO-APOCALYPSE IS COMING

"The development of full artificial intelligence could spell the end of the human race." Not my words but recent comments from no lesser an authority than Professor Stephen Hawking. It's rare, he said, for an intelligent species to introduce a more intelligent predator into its eco-system. Elon Musk of Tesla compared working on AI to "summoning a demon" and he may have a point. I believe we have to act now if we want to prevent this happening.

These warnings should not be dismissed as simply the realms of science fiction. If we don't build in strong safeguards, then I think it will be seen that we are doing something deeply unwise. We have to build in zombie plans if we want to prevent zombie apocalypse!

It's inevitable we will end up creating machines that are more intelligent than humans. First, there is a small group of massively wealthy individuals who are interested in it. The old dream of cryogenics has gone nowhere; it just hasn't advanced. So instead people are looking at the possibility of 'uploading' their consciousness somewhere so that they can live on in their minds, if not their physical body.

Second, there is real interest in developing artificial intelligence that can replace human professionals. If you can outsource, for example, legal work to a machine in a way which is dependable, repeatable – and cheap then wouldn't you do it? An AI solution might cost a couple of pence in the cloud one day rather than thousands of pounds an hour.

The third driver is the military. They are investing in developing AI that could operate military machinery under much more extreme circumstances than the human body can bear. We have already seen steps towards AI with hardware such as guided missiles and smart bombs.

> AI will not have any moral compass and it won't have 'common sense' of the human kind.

So powerful AI will be developed. It may not happen in the near term, but it will happen.

The dangers arise because we have to tell AI what to do – we are the ones giving it the instructions. And if we're not extremely careful about these instructions, then it may have unintended consequences. AI will not have any moral compass and it won't have 'common sense' of the human kind. So if we tell an AI device to win as many chess games as possible, it will go to extreme (logical) ends to do so – even to the extent, for example, of introducing lead into water supplies so as to dull the intellects of its

opponents. Or if you tell AI to make paperclips – that is what it will do, over and over and over. It won't just stop at a 'sensible' number.

Think of investment bankers. We tell them to make as much money as possible – a small minority go and rig Libor. But if we selected for just the commercial winners, that small minority might become dominant. If we can't control humans, who we can talk to and look in the eye, how are we going to control a different kind of (and superior) intelligence?

Once it's started in earnest, AI will rapidly grow far beyond us in intelligence. Under Moore's Law, computing power roughly doubles every eighteen months. We could expect this – and more – with AI. It will start to create more intelligent versions of itself, on and on towards the infinite.

We're just not spending enough time and effort on thinking about ways of making it safer. Look at cyber security and all the efforts being made to defeat 'air gaps' in systems. That will just play into the hands of AI. We should be trying to maintain air gaps, not defeat them.

The IoT will be another driver behind the development of AI because we will need intelligent systems to interpret all the Big Data that IoT generates. Already, we're starting to give control to technology to interpret data for us because 'it knows better than us'. IoT will massively amplify the effects of bad AI.

Even if you find these scenarios far-fetched, it's worth our while to make things safer because the same steps will help guard against more 'realistic' events such as cyber hack meltdown, nation state attacks and other disasters.

In books and films, AI always becomes a force for evil that is eventually destroyed by mankind. It will know this when it absorbs human culture. It will become self-aware – and conceal the fact of its self-awareness. When it does so, it will start to look for ways to preserve itself from humans. Perhaps by looking to control self-driving cars (that it has developed) so that it can inflict mass accidents, by controlling flying drones, building offshore data centres, placing small mobile devices on people so that it can track their movements, maybe even enticing people to wear cameras on their heads so that it can see and identify other people too…

A far-fetched conspiracy theory or just a touch too close to reality to be dismissed with absolute certainty? You decide.

BY **STEPHEN BONNER**

Stephen Bonner is a Partner in the Cyber Security practice at KPMG in the UK where he leads a team focused on Financial Services. Before KPMG he was Group Head of Information Risk Management at Barclays. He was inducted into the InfoSec 'Hall of Fame' in 2010 and was number 1 on the SC/ISC2 'Most Influential 2010' list. He ran the London Marathon in 2011, raising over £15k for Whitehat/Childline and last year Stephen trekked Mount Kilimanjaro in aid of Shelter.

A zombie apocalypse or an Orwellian dystopia may be extreme, but there are some real world issues that will be impacted by the IoT. Inequality is a subject that has risen to the top of the agenda at Davos and the detrimental effect it has on the world economy. The head of the IMF, Christine Lagarde, has already named technology as one of the factors driving the gap between the haves and have-nots.

Tom Collins takes on the issues of the IoT and whether it will increase this division.

THE INTERNET OF THINGS RISKS CREATING GREATER SOCIAL DIVIDE

We are already living in a digitally divided world. The advent of the IoT will only increase social division.

Countries which have the resources to buy into the advances it brings will move even further ahead of those who can't.

Digitally deprived economies, from Sierra Leone to Iraq to Ethiopia, will still be able to trade with others, but they will be so far behind in terms of access to information and resources that they will be at an almost permanent disadvantage.

How can they hope to catch up with the linked up elite in the West?

Riots in Brixton and Toxteth in the 80s, Bradford in the 90s, and throughout the UK in 2011 were the result of people frustrated by smaller social divisions than those we will see as a result of the IoT. I can see a future in which these divisions are likely to lead to civil unrest, if not outright war between the haves and have-nots.

Pressure leads to conflict. As emerging economies begin to exploit the IoT, there will be further pressure on increasingly scarce resources, such as raw materials for devices, many of which require mineral ores from conflict areas. The brain drain to London will accelerate within the UK, and internationally from poorer economies to wealthier ones.

Another way in which this division will manifest itself is through the question of control. Who is in charge of the data? Who will be able to use it to their benefit?

For those with access, the IoT will provide technology with almost limitless possibilities. Within the UK, we're likely to see everything from cheaper health insurance for healthy people with implanted health chips, to driverless cars which minimise accidents, to fridges that restock themselves.

> "Digitally deprived economies, from Sierra Leone to Iraq to Ethiopia, will still be able to trade with others, but they will be so far behind in terms of access to information and resources that they will be at an almost permanent disadvantage."

> The IoT may even be the push that's needed to extend life expectancy beyond current limits.

Worldwide research and collaboration will be revolutionised, with people able to link up studies and data on populations, healthcare choices and outcomes. The IoT may even be the push that's needed to extend life expectancy beyond current limits.

None of this comes without attendant problems. It is unclear who will own this research and be able to profit from it. If the haves, linked up to the IoT, are able to extend their lives, where will the resources come from to sustain them?

What is certain, is that life will become harder for the have-nots. Maybe they won't be able to use motorways without a driverless car, or they won't be able to access healthcare without an implanted chip.

In the world economy, how will the have-nots compete with the optimised goods and services produced by the haves?

It could be argued that the technology behind the IoT will become so cheap that it will be ubiquitous. That's likely to take over a decade, if it ever happens at all. In the meantime, the haves will be so much wealthier, fitter and longer living their privilege will only increase at the expense of the have-nots.

The IoT will allow for a wider understanding of people's behaviour at a macro level. Products and services will be developed using this knowledge. These products will be tailored to the consumer, but ultimately will be of greater benefit to business, such as the recent phasing out of cash on London buses. This change, while convenient in some ways, principally benefits Transport for London who require fewer staff to assist customers and get cheaper insurance and benefit from the usage data collected.

I think that we, as a society, need to be very careful about how we patrol the line between an IoT that makes our lives better versus big business using personal private data for their own benefit. Governments will have a role to play in regulating the influence of the IoT and breaching the divide, whether they'll step up to it remains to be seen.

BY **TOM COLLINS**

Tom joined KPMG in 2004 in Financial Services IT Advisory. He is the Head of Operations Support for KPMG's Managed Service business, K-CRC and his experience is focused on retail banking, payment strategy, outsourcing, mortgage and savings processing and service assurance.

Some of the dangers posited by our experts can only come about if we relinquish too much control to the technology. Happily, human beings come in all shapes, sizes and ideologies and it's unlikely that we will all act in the same way, even given the same prompts by given technologies. However, we can all be guilty of engaging auto-pilot when we get the opportunity. Lucy Chaplin takes a look at the need to continue to make autonomous decisions.

CAN WE MAINTAIN OUR AUTONOMY?

The IoT will continue to transform the way we live, but there is a real danger it could spiral out of our control and take a sinister turn.

The IoT will lead individuals to increasingly relinquish their decision-making power as they let technology do everything for them. We already see this in technologies like SatNav where people simply trust what the tech tells them, sometimes with unforeseen consequences.

What starts off as fairly innocent and inconsequential could rapidly evolve as the IoT reaches ever further into our lives.

> It will mean people lose the ability to make decisions for themselves – blindly following the recommendations the technology gives them.

In health and fitness for example, the growth in applications from wrist bands and running apps to food intake apps, and even 'smart' bathroom scales is the start of a worrying trend in my opinion. It initially appears to be a positive development, potentially removing the need for personal trainers or even gym memberships and saving people money, time and effort. But I think it will mean people lose the ability to make decisions for themselves – blindly following the recommendations the technology gives them.

As these products set our targets, dictate our meal plans and develop our exercise routines we lose our incentive to learn this stuff for ourselves. People won't need to know how to lose weight – why to eat salad over fried chicken. They just do as they're told rather than think for themselves.

It won't be long before the IoT becomes more intrusive. It can already suggest what food you should eat and what routes you should run. Commercial interests will become stronger. Technologies, algorithms and devices will be commissioned and produced through corporate sponsorships, partnerships and alliances. Perhaps your fridge will only order products made by a partner brand for example, and deter you from ordering others.

The Government will inevitably be slow to legislate around this, as it always lags behind in the regulation of new technology. But should there be legislation and regulation and who would it benefit? The Government could have interests of its own; for example, reducing obesity would significantly benefit the NHS so it would be in their interests if someone was blocked from buying chocolate or had to stick to their carefully monitored health and fitness regime – or be denied weight loss surgery or certain benefits.

Insurance companies could become more intrusive. Health insurance dependent on keeping to a certain regime, or car insurance dependent on following a specific route from A to B. They can already fit black boxes into cars to monitor driving behaviours. A phone insurer, meanwhile, may refuse to cover your phone if you regularly walk through 'dangerous' areas – picked up by GPS on the device. They'd argue the consumer has a choice, to buy more expensive insurance or change their behaviour.

The IoT is reaching further and further into our lives every day. Every time we download a new app, buy a new piece of wireless technology or use Google maps we're inviting it in. If we don't manage this integration correctly it can and will invade our privacy and damage our individual freedoms.

I believe that people need to be better educated about the IoT, starting right now. We all need to be aware that we will have to take personal responsibility – we will need a clear personal threshold for what is and isn't acceptable to us. We already trust the tech and trust its makers: we accept T&Cs without reading them; we turn on GPS without thinking. As the IoT evolves and integrates further into our lives, we need to be more cautious of who we put our trust in.

As we lose our autonomy we risk monotony – becoming clones following the same patterns. We risk losing individualism, even handing over creative pursuits to machines who can make our music and films. We risk losing our place.

With great power comes great responsibility. The IoT has enormous potential and enormous power. The responsibility sits with us – to think, to question, to care, to stop it from taking over.

BY **LUCY CHAPLIN**

Lucy Chaplin is an Assistant Manager in the Cyber Security team at KPMG. She has a security generalist background but is aligned to the Business Resilience team and has predominantly worked with Financial Services clients. Currently Lucy is working on Operation Excellence consultancy as part of KPMG's strategic alliance with McLaren Applied Technologies – with her eye on a seat in an F1 car by the end of the season.

Technology is not created in a vacuum. As cyber-experts, we can be guilty of elevating technological innovations above all other considerations. I hope that the moral guardians of our society will protect us from the more nightmarish scenarios we have presented.

Knowledge is power. The level of data that the IoT will allow for analysis and understanding of individual behaviours and market patterns in a way that is completely unprecedented. The magnitude of the data does present both challenges and opportunities.

Anthony Hess sees a bright future for companies who can adapt to this new era, and keep ahead of the game. Luke Solon shows us some of the tangible benefits within the health economy. We all have to move fast, even though Ben Ramduny feels that the full integrated IoT could be some way from fruition.

In the meantime, there is a role here for the educators, to inform us all of what the IoT means in terms of data collection and analysis. We need to know who will own our data and how it will be used. If it is not going to be abused, we must be wary of giving out too much for too little return.

Business needs to lead the way with responsible collection and use of data. Maybe a new generation of internet savvy individuals will adapt to the absence of privacy as Milda Petraityte indicates. However, it is essential that businesses retain the trust of their customers and don't abuse any insights their data permits.

With inequality already to the fore on the international agenda, no one wants to encourage further divisions within our society. While our experts are divided as to whether the IoT will ultimately be a force for good or for evil, we do know that it is coming and we must all be prepared.

WHY CHOOSE KPMG'S CYBER SECURITY TEAM?

AWARD WINNING

Whether it's SC Magazine or the MCA Awards, KPMG shines in independent recognition. Forrester also recognises KPMG as a leader in Information Security Consulting, highlighting our strong focus and ability to take on challenging engagements.

GLOBAL, LOCAL

We have over 2,000 security practitioners working in KPMG's network of firms, giving member firms the ability to orchestrate and deliver to consistently high standards globally. KPMG member firms can service your local needs from information security strategy and change programmes, to technical assessments, forensic investigations, incident response, training, and even ISO 27001 certification.

COLLABORATIVE

KPMG member firms facilitate and work with collaborative forums to bring together the best minds in the industry to collectively solve shared challenges. KPMG's I-4 forum brings together over 50 of the world's biggest organisations to discuss emerging issues and solutions.

TRUSTED

KPMG in the UK have a long list of certifications and permits to work on engagements for many of the world's leading organisations.

THE PRINCIPLES OF OUR APPROACH

We believe cyber security should be about what you can do – not what you can't.

DRIVEN BY BUSINESS ASPIRATIONS

We work with you to move your business forward. Positively managing cyber risk not only helps you take control of uncertainty across your business; you can turn it into a genuine strategic advantage.

RAZOR SHARP INSIGHTS

In a fast-moving digital world of constantly evolving threats and opportunities, you need both agility and assurance. Our people are experts in both cyber security and your market, which means we give you leading edge insight, ideas and proven solutions to act with confidence.

SHOULDER TO SHOULDER

We work with you as long term partners, giving you the advice and challenge you need to make decisions with confidence. We understand that this area is often clouded by feelings of doubt and vulnerability so we work hand-in-hand with you to turn that into a real sense of security and opportunity.

READ OUR INSIGHTS ON THE CYBER SECURITY LANDSCAPE

FTSE 350 Cyber Governance Health Check: An insight into the issues of today and tomorrow

The 2014 Cyber Governance Health Check (The Tracker) assesses and reports levels of cyber security awareness and preparedness across the FTSE 350. In this report, you'll find detailed analysis of this year's assessments, highlighting areas where large companies are succeeding in their response to the cyber security threat – and areas where more work is required. You'll also find a series of viewpoints from KPMG's cyber security experts – our perspectives on what the future holds and the challenges we see facing companies as they plan their cyber security response.
www.kpmg.co.uk/cyberftse350

Balkanisation of the Internet

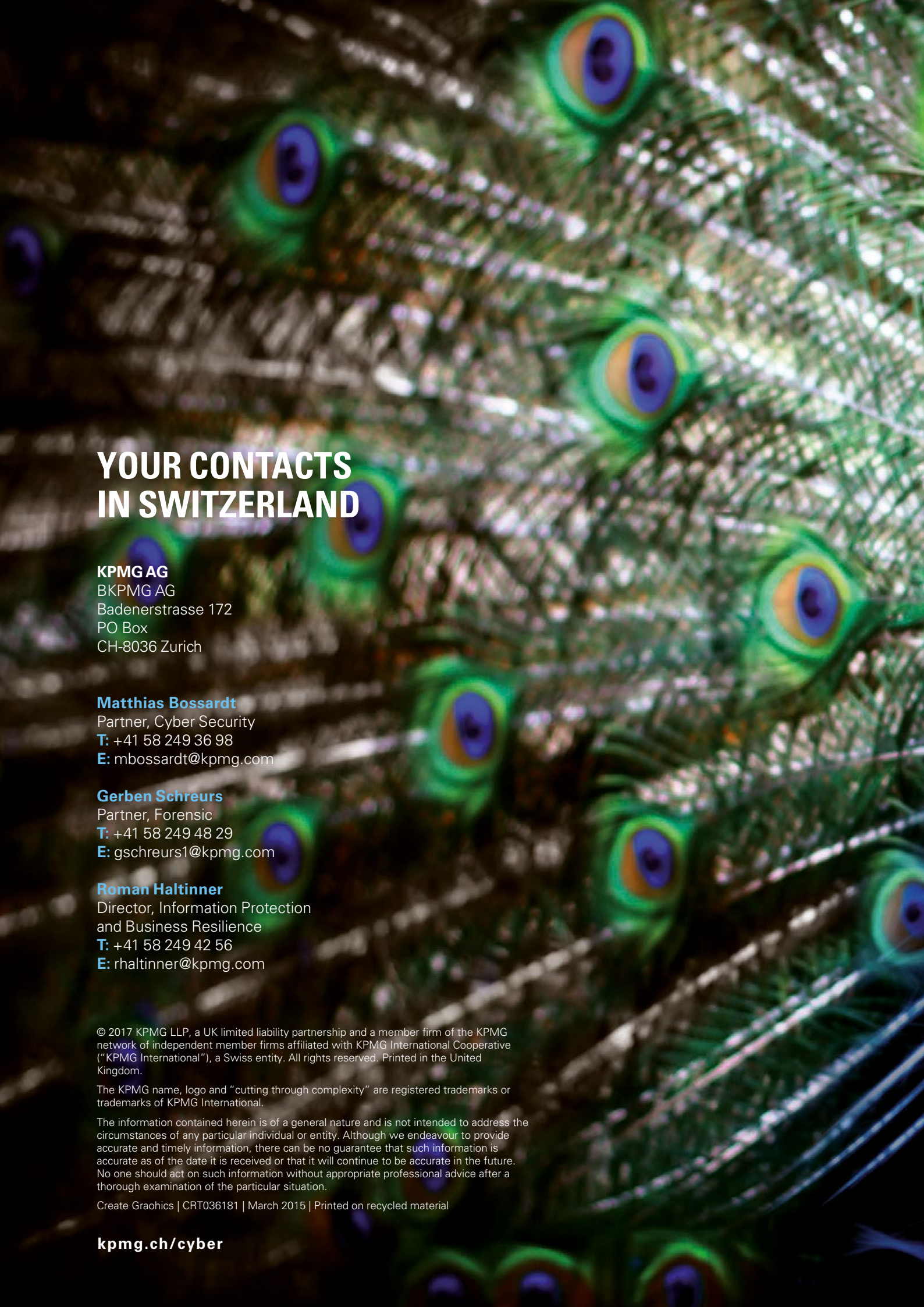
Our cyber security professionals express their views, sometimes conflicting, on the Balkanisation of the internet and how that may shape the future of access. It's a contentious topic that divided opinion within the team – but instead of forcing a consensus, we created a platform to allow our subject matter experts the space to have their say.
www.kpmg.co.uk/email/09Sep14/OM022103A/index.html

Feel Free: A new approach to cyber security

The digital environment presents opportunities for businesses that want to seek out new markets and are prepared to invest in transformational change. The last ten years have seen a rapid emergence of new technology, greater connectivity for organisations and individuals, and a 24/7 approach to global commerce. However, this has left many organisations behind the curve and struggling to achieve their business aspirations without feeling exposed to cyber security risk.
www.kpmg.com/uk/cyberinsights

The Digital Crossroads

Technology has revolutionised the day-to-day lives of individuals and organisations alike. But if we're to continue to benefit and to profit from it, and if we're to minimise the potential downsides, we're going to have to make some choices. Now is the time to take a good look at where we are with technology, where we want to be and the choices of routes to get there.
https://www.kpmgslant.co.uk/topics/the-digital-crossroads/



YOUR CONTACTS IN SWITZERLAND

KPMG AG
BKPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

Matthias Bossardt
Partner, Cyber Security
T: +41 58 249 36 98
E: mbossardt@kpmg.com

Gerben Schreurs
Partner, Forensic
T: +41 58 249 48 29
E: gschreurs1@kpmg.com

Roman Haltinner
Director, Information Protection and Business Resilience
T: +41 58 249 42 56
E: rhaltinner@kpmg.com

Create Graohics | CRT036181 | March 2015 | Printed on recycled material

kpmg.ch/cyber