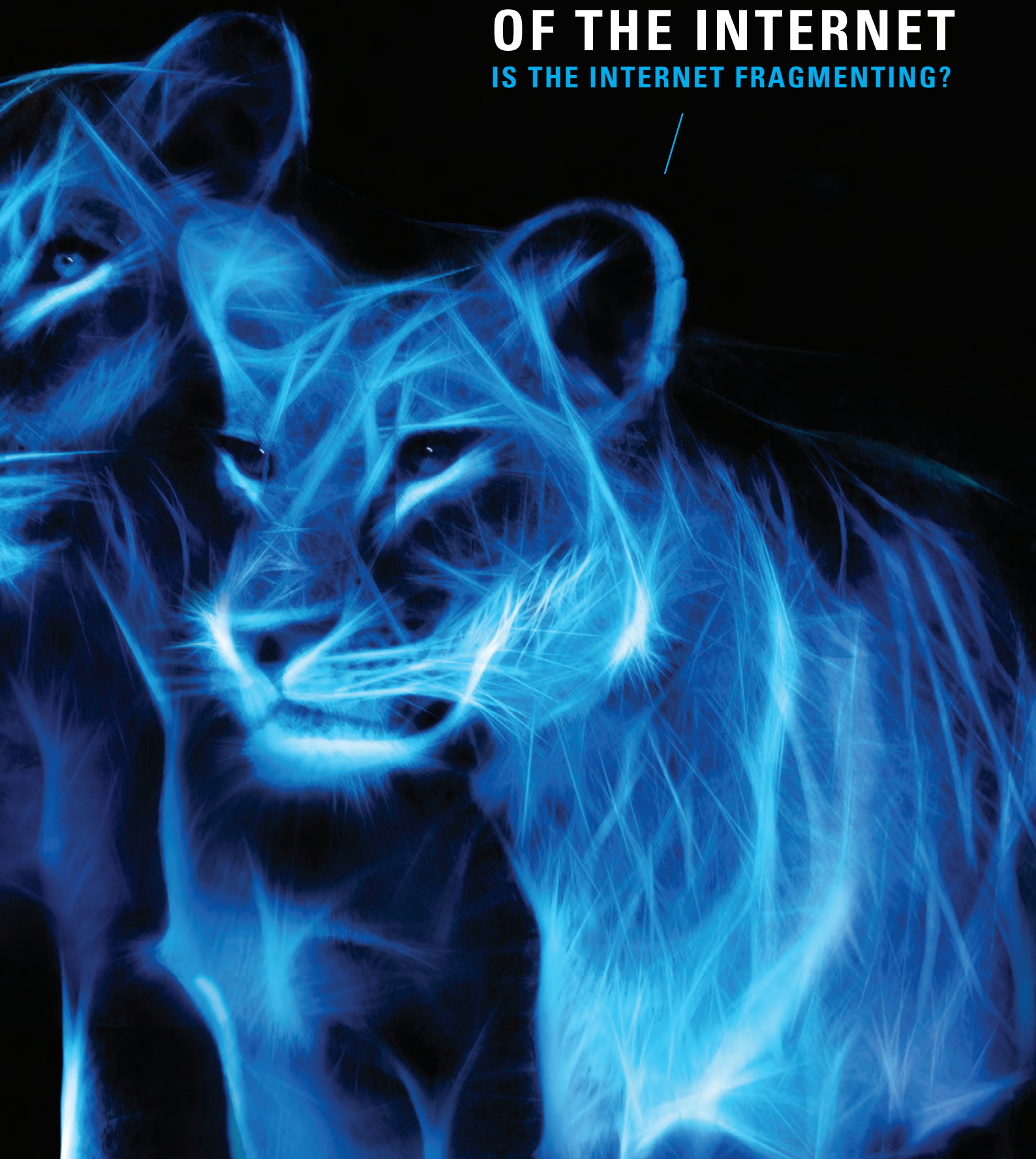
KPMG

cutting through complexity

BALKANISATION OF THE INTERNET

IS THE INTERNET FRAGMENTING?



WELCOME TO OUR CYBER INSIGHTS MAGAZINE.

In this edition 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 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 LLP.

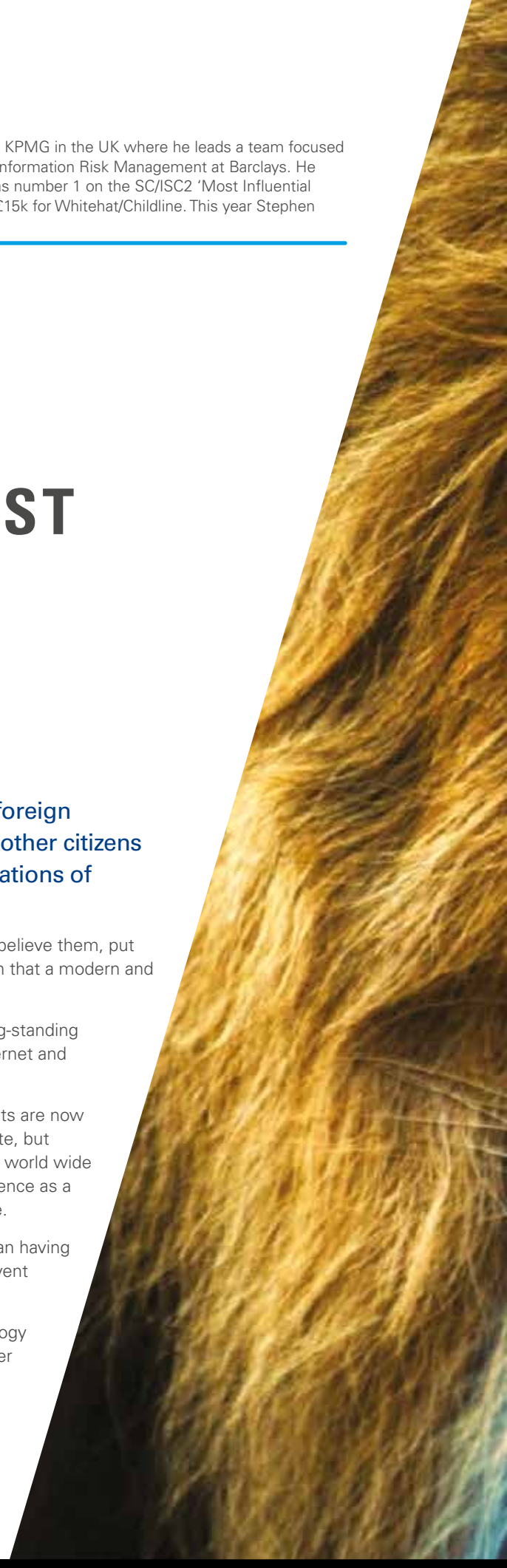
For more insights on the future landscape of cyber security and how the UK stacks up in the digital age, go to www.kpmgslant.co.uk

CONTENTS

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. This year Stephen is trekking mount Kilimanjaro in aid of Shelter.

INDUSTRY MUST PUSH BACK AGAINST BALKANISATION[1] OF THE WEB



Possibly the one thing worse than finding out that a foreign government has been spying on you and millions of other citizens over the internet just because they can, is the ramifications of those revelations.

The leaked US National Security Agency (NSA) documents, if we are to believe them, put into sharp relief the scale and sophistication of the intelligence collection that a modern and well-resourced nation can undertake on the internet.

The aftershocks have sent waves around the world and exacerbated long-standing tensions between countries and regions over the governance of the internet and how best to protect their citizens and their data.

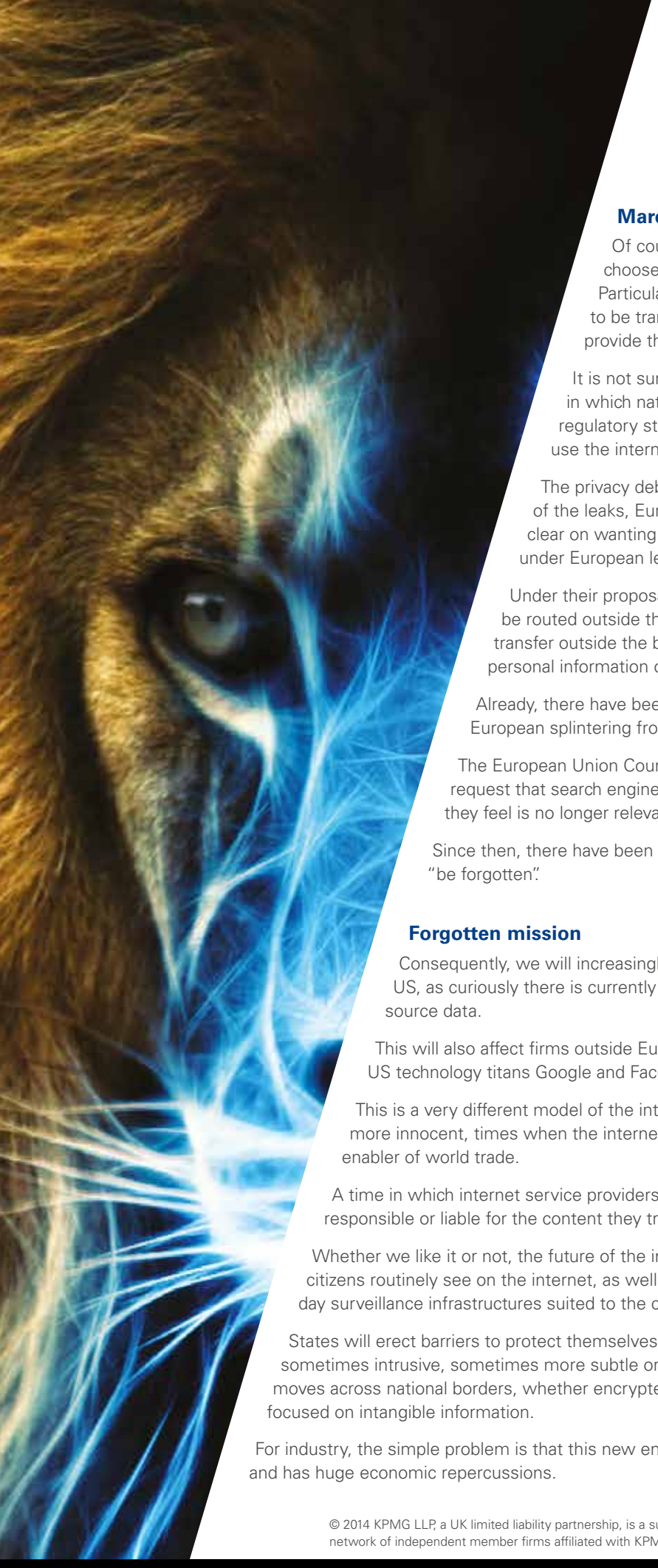
The consequences could be terrible. It is clear that incensed governments are now determined to break up the internet into smaller fragments in a desperate, but potentially ineffectual, bid to assert sovereignty. The Balkanisation of the world wide web in its most extreme manifestation would destroy the internet's essence as a global forum for the unfettered exchange of ideas, free speech and trade.

I believe this outcome would be far more unacceptable to web users than having their digital rights compromised by government agencies looking to prevent loss of life from terrorism.

To prevent nation states from the most damaging interventions, technology companies and digital rights groups must work with governments to offer better protection for web users within the global interface.

[1] Balkanize or Balkanise (ˈbɔːlkəˌnaɪz) – vb
- to divide (a territory) into small warring states
- to divide (a group or organisation) into small factions

Dictionary.com



March of Euronet

Of course it is concerning that there are countries that choose to conduct mass internet surveillance programmes. Particularly so, if such programmes lack accountability, fail to be transparent over their scale and extent, and do not provide the opportunity for judicial review.

It is not surprising that this has created a febrile environment in which nations will seek to establish their own legal and regulatory structures, and impose controls on how their citizens use the internet and interact with the international community.

The privacy debate raging in Europe is one example. In the wake of the leaks, European Commission officials have made their stance clear on wanting an internet model specific to Europe, operating under European legal principles and norms of behaviour.

Under their proposals, data to do with European subjects would not be routed outside the European Union unless specifically required to transfer outside the borders. This would create a "safe" harbour for the personal information of citizens.

Already, there have been moves which may unintentionally accelerate a European splintering from the global internet.

The European Union Court of Justice ruled in May that data subjects could request that search engines, such as Google, remove links to material that they feel is no longer relevant or outdated.

Since then, there have been tens of thousands of requests to Google to "be forgotten".

Forgotten mission

Consequently, we will increasingly see different search results in Europe than in the US, as curiously there is currently no legal requirement to remove the original source data.

This will also affect firms outside Europe but providing services into Europe, such as the US technology titans Google and Facebook.

This is a very different model of the internet to the model we saw in earlier, and perhaps more innocent, times when the internet was seen as a forum for free speech and a key enabler of world trade.

A time in which internet service providers (ISPs) could still claim to be unbiased carriers not responsible or liable for the content they transmitted.

Whether we like it or not, the future of the internet is one with more national control of what citizens routinely see on the internet, as well as one in which the state has put in place modern day surveillance infrastructures suited to the complexity of our online world.

States will erect barriers to protect themselves against threats to their national internets, sometimes intrusive, sometimes more subtle or transient. They will be tempted to control how data moves across national borders, whether encrypted or not - a latter day export control regime perhaps focused on intangible information.

For industry, the simple problem is that this new environment gets in the way of global commerce and has huge economic repercussions.

> States will erect barriers to protect themselves against threats to their national internets, sometimes intrusive, sometimes more subtle or transient.

Economic fallout

Today, in the UK alone, the internet, if regarded as a separate economic sector, is responsible for around 8% of GDP and by 2016 it is projected to grow to 12.4%. By 2016, 23% of retail business will be transacted online.[2]

But the costs of moving away from a global platform toward a disparate hotchpotch of isolated national interests could be huge as companies operating in this environment seek to comply with an increasingly complex and diverse set of regulatory regimes in Europe and beyond.

They may be forced to replicate data centres, filter communications and change encryption architectures to meet different national standards and requirements.

That is why industry must make its voice heard in this debate on the future of governance of the internet and help shape the norms of behaviour which emerge.

Global business must contribute to the growing international debate on internet governance for the future, helping governments strike a balance between economic drivers and human rights, while avoiding a drift towards a fragmented internet where countries implement barriers that can only be financially detrimental to everyone.

This is not a technical discussion which finds a home just in the International Telecommunications Union (ITU), but an economic debate better suited for the likes of a G20 or World Trade Organisation (WTO) summit of global business leaders.

Implementation dilemma

While the economic costs are a real worry, the more pernicious danger of Balkanisation of the internet could be in the translation between the principles driving it and their implementation.

I firmly believe in the principles of increased data protection and enshrining an individual's right to privacy. They make a lot of sense.

The problem with laws, however, is that despite the best of intentions they can be complex, problematic and burdensome.

This is especially the case with regard to the internet as any new legal and regulatory structures will most likely be suited for legacy technology and could be out of date and unfit for purpose shortly after implementation.

After all, we are already staring into a future of more connected devices and more sophisticated processing of data. The search engine results of the future may be a complex fusion and analysis of base data to answer a user's query.

The judgements made by that artificial intelligence may be complex, difficult to reverse engineer and tricky to interpret. A neural network would function very differently to a modern day search engine.

Who can fathom how these new technologies will play out and the obstacles around privacy and the risks of surveillance they will generate?

> The problem with laws though is that, despite the best of intentions, they can be complex, problematic and burdensome.

Cyber insurance market

That is why industry and government must work together to put in place implementation structures. Both parties have a responsibility to think through the consequences and practicalities of complying with legal frameworks.

Otherwise governments risk not being able to enforce them and companies risk falling foul of the law despite their best efforts.

Already we are seeing a growing cyber insurance market as companies fear greater litigation by individuals affected by any data breach and increasingly large regulatory fines.

The new EU data protection regulation coming into force in 2015 is likely to penalise a business for information failures which result in subject data being compromised. Those fines are likely to be between 2% and 5% of global turnover depending on the outcome of the debate between the European Parliament and Council of Ministers.[3]

We are also seeing far greater recourse to litigation.

A recent data breach, where up to 70 million customers had payment card and personal data stolen from a US

[2] The $4.2 Trillion Opportunity: The Internet Economy in the G-20, BCG 2012
[3] European Commission memo 12 March 2013

retailer's databases in December last year has already generated more than 140 law suits, recently consolidated in a Minnesota court.

Doing things differently

I believe there are other less cumbersome ways to offer web users a secure internet which they can have confidence using, while still enabling global commerce and offering all the benefits we experienced in the early days of its evolution.

We could start with organisations empowering their customers to make choices over how their data is handled and held to account for respecting those choices.

Perhaps, in time, users would even get real financial benefit from the commercial use of their information, not just tailored services and direct marketing, but micropayments by firms who use their data.

In addition, with networks and routing infrastructures becoming more sophisticated, I believe we are almost at a point where companies can respect a user's views on how their data is routed and protected.

I'd also like to see more use of encryption of data being transferred across the borders raising the bar on intelligence collection, along with greater transparency by countries on the scale and extent of their surveillance efforts.

My view is that the internet is at a crossroads right now with the challenge for nations to put in place sensible legal and regulatory structures working in partnership with business.

If we get this wrong, we end up with a fragmented and economically inefficient internet with a bureaucracy of enforcement which would do more harm than good and have an economic cost for everybody.

A EUROPEAN INTERNET IS SIMPLY THE MANIFESTATION OF POST-MODERN SECURITY

The Treaty of Paris (1951) laid the foundations for renewed diplomatic and economic stability in Western Europe following two world wars.

It was believed that economically linking the previously feuding European powerhouses (France and Germany) would significantly mitigate against the chances of future European-instigated world war[1]. Thus far, this premise holds true.

So, if Europe were to run and secure its own information super highway, this, in my view, would simply be a natural information-age evolution of the 1950s security-inspired principle.

I believe there is growing appetite from senior European political leaders to create such a regional telecommunications network and we should positively embrace it.

Appetite for change

Without doubt, a Euronet with the ability to protect its own infoscape, operating as an alternative to the current US-led global hegemony, is on the cards.

Sufficient European technology infrastructure is already in place to host the estimated 10 Exabytes (1 Billion Gigabytes) of data currently held by Google[2].

The German Chancellor Angela Merkel put the political wheels in motion for a regional network set apart from the US and other potential "prying eyes" earlier this year by publicly raising the concept of a Euronet.

This followed revelations of mass US information-gathering efforts including allegations that the National Security Agency (NSA) tapped the Chancellor's own phone and an apparent failure to obtain a no-spy agreement from the White House.

Within a week, France signalled public support for Chancellor Merkel's proposals.

These are strong messages, which I believe, are reinforced by the sense that a fragmentation of the global structure of the internet could be the catalyst to re-assert Europe's place on the world stage.

Sick man of the world

Europe was a global powerhouse in the last century. But now, some would say, the region is struggling to grow economically and with rapidly aging populations.

The creation of a Euronet, its advocates believe, will showcase Europe as an intellectual and political information-age force, giving the region a much-needed boost to be able to compete against other regional economies that boast younger populations and greater resources.

This will create a platform for Europe to become the centre of the growing global e-commerce market, built on trust and reliability. In so doing, Europe will also position itself as a sophisticated technology hub and attractive to young international intellectuals.

However, the tipping point for a self-sustaining Euronet is still some way off. Some political will and the promise of increased security is a good start but it's not enough.

[1] Schuman declaration 9 May 1950 http://europa.eu/about-eu/basic-information/symbols/europe-day/schuman-declaration/index_en.htm

[2] 2014: Randell Munroe TED Talk Mar http://www.ted.com/talks/randall_munroe_comics_that_ask_what_if

The initiative will need tangible buy-in from eurozone countries to be both economically and structurally feasible with these countries prepared to commit some resources, whether that comes from the state or the private sector.

Other hurdles will be financial investment and the costs and hassle related to the adoption of common standards to ensure network homogeneity.

There will also undoubtedly be fierce opposition from the existing global internet providers who will fight back against such an initiative before it can assume a competing size.

> I foresee the digital equivalents of the Schengen Agreement being used as mechanisms to enforce the appropriate controls on the European infoscape.

It's all about networks

A common European data network will certainly not be the first time in history where standardisation and control have lead to improved efficiency and effectiveness. The rail system and electricity supply are two famous examples. There are parts of the world where 110V is the norm (that is in the US) and others where 220V prevails (Europe).

Nonetheless, it is possible to "tap into" either network through a simple adaptor. In a similar vein, regional internets will interact through appropriate adaptors.

Not an iron curtain

Euronet, however, will not stand apart like some Cold War relic. It will exist alongside and be joined to other regional "nets" around the globe.

The biggest difference will be that Europe will have control of its own information in Euronet as well as what comes in and leaves the network.

With this control comes improved recognition of the interests of member states and individuals, convenience, economic prosperity and, most importantly, reliable collective security helping to protect Europe from cyber crime and cyber war.

In terms of security, I can see organisations such as the European Internet Foundation playing a key role in the protection of European interests in the digital environment, possibly even taking on a security role.

Who knows, perhaps we will even see a Euronet border force.

With this, I foresee the digital equivalents of the Schengen Agreement being used as mechanisms to enforce the appropriate controls on the European infoscape.

There may be some trade-offs of personal liberties but I believe they will be made willingly in pursuit of unrivalled convenience and security: a new and improved European information highway, facilitating the pursuit of happiness, prosperity and normality within our own control.

BY **CHRIS CROWTHER**

Chris joined KPMG in the UK 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 PUSH FOR EURONET IS A LOSING BATTLE

The exposure of mass online US surveillance programmes monitoring citizens outside the country last year blew the lid on tensions that have been simmering for a while about whether governments should intervene to safeguard their citizens' data and security online and to what extent.

A law has already been passed in the EU that entitles individuals to apply to search engines, like Google, to remove links to suspect material from their past, and more data protection laws will be passed in the region in 2015.

There is also talk about other moves to cut off the internet in Europe from its global interface, like moving data centres into member states so that no data leaves the EU in transit.

But I believe that this protectionist stance is unhelpful as individuals and businesses will not want to be annexed from the wider interface despite the risks to security and privacy involved.

People and businesses value open communication and a free market first and they will look for ways to circumnavigate national firewalls in a similar way to Turkey's web users getting round the Twitter ban and even in China, committed internet users find ways to beat the Great Firewall even at the risk to their personal safety.

The cyber war between Russian and Ukrainian supporters, with hackers from both sides disabling their rivals' sites with distributed denial of service (DDoS) attacks is another example of how nothing will stand in the way of savvy web users.

> There is [also] talk about other moves to cut off the internet in Europe from its global interface.

Open communication

The internet was founded as a forum for open communication and quickly developed as a facilitator for world trade.

I don't believe individuals or businesses want to see it fragmented and lose all the benefits it offers.

The leaks from the US government contractor Edward Snowdon seemed to take everyone by surprise, but I'm not sure why.

We know that all our data is out there in the public domain. We get random calls from car insurance companies, accident "helplines" and PPI compensation companies. So why would we be so naive as to think that governments wouldn't use it for their own purpose?

I think I'd prefer to know that the Government was on top of any terror threats and therefore protecting my life rather than my online privacy.

We are all being watched, but the good thing about that is that wrongdoing in cyber space will also not go unnoticed.

Pan-European law enforcement

As I said, I don't think regional or national ringfencing of the internet is the answer as imposing national or regional sovereignty on a global forum will only create additional costs and process for business and individuals and cannot be effectively enforced.

But I believe what we could see over the next 10 years is a European policing body of sorts, like Interpol, that can crack down on international crime conducted or orchestrated over the internet.

This would also help to manage and control cyber bullying, stalking and harassment over social media.

> ...but the good thing about that is that wrongdoing in cyber space will also not go unnoticed.

BY **MICHAEL EVANS**

Mike is a Resilience and Security Advisor in KPMG in the UK's Global Centre of Excellence for Information Protection & Business Resilience. With a background in private consultancy and the Armed Forces, Mike has experience and expertise in all areas of business continuity and resilience, crisis management, incident response, and disaster recovery.

USERS MUST NOT RELY ON GOVERNMENTS TO PROTECT US ONLINE

Throughout history, power - the ability to force one's will onto another - has always been fought over between competing actors. For a long time, the church was arguably the most important actor in the international system, usurped by nation states following the signing of the Peace of Westphalia treaties in 1648.

Over the past few decades, the order of power has been upset again with the emergence of powerful non-state actors: huge global corporations, which have at their disposal more money, flexibility and influence than many individual countries.

Nowhere is this more evident than online, where the growth of large communication platforms has transformed how we interact with each other.

Without really noticing, the world's internet users are sleepwalking into ceding control of a large chunk of our lives to a handful of organisations.

New hegemonic order

Think of the services that we interact with on a daily basis: Google, Facebook, and Twitter to name a few. While the internet is commonly characterised as a level playing field for free expression, this is in fact inaccurate. In reality, most of the internet is a battleground with hegemonic corporations and governments fighting to wield control.

Sure, it's great that in theory we can publish content and communicate online using whatever service we wish, but increasingly, if we don't use the big players, our voices and messages will go unheard.

For much of the younger generation in the West, if their friends aren't on Facebook or the latest social network, then they may as well not exist given how much of our social lives take place there.

So in a sense, these global corporations have become the new hegemonic order and the new custodians of freedom of speech. They have privatised the public square, so to speak, with corporate decisions on what content is allowed on these platforms having conceivably huge implications on our ability to speak freely that goes well beyond legal policy.

Stark implications

After all, Facebook and Twitter aren't just a "broadcast" medium, like a TV company. Facebook choosing to delete certain posts for breaking its rules is analogous to BT interrupting your phone call to a friend to explain why you can't talk about a particular topic.

The implication in terms of power is stark and it can work in the public's favour if we engage with these companies effectively.

This was the case when some of the biggest websites in the world went "dark" in 2012 in protest against the US Stop Online Piracy Act (SOPA) and other planned anti-piracy laws that threatened to destroy the internet as an open and free platform for all to use.

The exposure resulted in a massive public backlash and the bill was dropped almost immediately.

> Nowhere is this more evident than online, where the growth of large communication platforms has transformed how we interact with each other.

The internet is fast becoming a space where there is a rock/paper/scissors power play going on between governments, corporations and users.

I would suggest that tipping the balance of power away from governments is actually not such a bad thing as, primarily, governments are self-interested, looking first and foremost to protect state rather than individual interests.

Government reliance

Unlike the state, interacting with companies is at the individual's discretion and therefore web users must take more responsibility by directly engaging with those whose online services they rely on to protect their data and privacy in a way that is acceptable to them.

We must wean ourselves off a reliance on government to step in where there is a problem.

If the big technology companies fail to help users make the internet a safer and happier place for the people that use them, then these firms will be challenged by others who are prepared to make those promises – and people will vote with their clicks.

The internet is young and we are still exploring the boundaries of how we all use it.

During this learning stage it is up to us, the web users, to hold the powers that control the internet to account and it is up to companies and governments to listen to their customers and citizens.

BY **MORGAN PHILLIPS**

Morgan is a chartered accountant by training and joined KPMG in the UK information protection advisory practice from a background in controls audit. His career has seen him working with owner managed businesses and global FS clients. He says a career highlight has included a project rescuing a struggling football club.

UK MUST NOT FALL OUT WITH US OVER DATA BREACH

In light of recent revelations about nations spying on other nations (and individuals), some are questioning the validity of using the US as a safe harbour for our data.

But I believe that the US is our most important ally in the world today and withdrawing our data from its borders would be a huge mistake on a number of levels.

We would not only be limiting ourselves from arguably the hub of the global data market and a massive user base, but, more seriously, such a move could have repercussions for the special Anglo-US relationship.

If this was to fall apart, it could affect our relations with other members of the "five eyes" intelligence club: Australia, New Zealand and Canada and this could leave us vulnerable to opportunist nation states.

No safe haven for data

Similarly, if we also do not trust China and Russia with our data, (particularly after recent geo-political events), we could be soon asking ourselves the question: "Who's left to turn to?"

Sure, there are other European or ASEAN countries to form alliances with, but they do not have the buying, selling or developing capability of the global super powers.

Moreover, I think it is important to question whether data is safe anywhere? I think the honest answer to that is no. If a determined hacker wants access to your data, he or she will get to it one way or another.

> I think it is important to question whether data is safe anywhere? I think the honest answer to that is no.

Take the computer worm Stuxnext for example. A 'party' gained access to Iran's nuclear programme and in doing so was able to sabotage progress. Nothing should be as protected as a nuclear facility yet even this was compromised.

With that in mind, securing data, as all of us in the information security industry know, is striking that finite balance between availability and usability.

For example, do you lock your data away in a vault so you can never sell or use it, or do you put in on the shop floor, so everyone knows you have it (and make yourself more susceptible to risk)?

Right level of security

I believe that balance can be achieved by not only looking closely at your data assets and understanding its value, but by also looking at the impacts of a potential exposure. This will allow the owners of that data to ensure the right level of security.

> I believe the emphasis should be on strengthening existing relationships (and fostering new ones) across the globe.

But in order to mitigate data threats, I believe the emphasis should be on strengthening existing relationships (and fostering new ones) across the globe.

Some may say that we are putting ourselves at risk by using the US as a data safe harbour and vice versa, but lessons from history indicate that good relations with superpowers are a worthwhile trade off.

BY **MICHAEL EVANS**

Mike is a Resilience and Security Advisor in KPMG in the UK's Global Centre of Excellence for Information Protection & Business Resilience. With a background in private consultancy and the Armed Forces, Mike has experience and expertise in all areas of business continuity and resilience, crisis management, incident response, and disaster recovery.

WHEN ONLINE GOES OFFLINE – TOTAL INTERNET FAILURE

The subject of internet blackout risk receives relatively little attention. It is often drowned out by tales of the risks associated with state sponsored cyber crime and sophisticated malware. As a consequence companies could be in for a shock, at any point in the near future.

I think that we have experienced an extremely unlikely and unusual period of stability of core internet services like routing tables and name lookups. This good luck has meant most organisations don't take the threat of long-term internet outage seriously enough. I think one of the biggest IT risks that we face is the combination of capacity and complexity issues causing internet failures.

Who pays for the internet's utility bill?

Organisations should be surprised that the internet works so well, rather than be surprised when it fails – given that no one body is responsible for making it work. This is only an issue because it has become normal to think of the internet as a utility such as power, telecommunications or water, where a service is paid for with contractually agreed service levels.

Organisations do protect their connection to the internet, for example by using 'dual pipes' from two providers, but out of sight, the internet is cobbled together in a whole series of insecure, outdated technologies which are lashed together with the sweat and tears of network engineers.

Spiralling out of control

The internet is also dependent on numerous other factors which cannot be controlled by end users. For example, reliable power and access to cooling is needed and a global network of cables needs to be protected from being cut by construction machinery or damaged by fishing trawler nets. Then of course, there are risks caused by those acting maliciously – which has happened in the past. 'Worms' for example have spread rapidly across the internet, causing significant disruption.

It represents a giant leap of faith for so many organisations to bet their business model on the internet, which is managed with so few formal controls. Ironically, it is also an endorsement for this 'unregulated' approach, as it appears to be more robust than highly regulated systems such as power or financial networks which have rare, but very significant outages.

Exponential growth versus linear growth

The loads and complexity of internet usage is growing exponentially while the skills and capability to manage the systems is growing (at best) in a linear fashion. Last year, we passed the point where more than half of all internet traffic was created by machine-to-machine communication – the number and criticality of connections facilitated by the internet is far outpacing the resources dedicated to maintaining it. More and more data is being transferred by an ever more exotic collection of devices, from fridges to pacemakers.

I believe that we will see substantial disruption to organisations and entire businesses failing through not appreciating that relying on the internet means relying on third party services for which there are no contracts and not even a clear owner.

> ...that the internet is cobbled together in a whole series of insecure, outdated technologies lashed together with sweat and tears of network engineers.

Quantifying the impacts

I take no pleasure in suggesting that another item be added to the already daunting list of IT risks which need to be considered. However, heavily internet-dependent businesses which have processes and procedures in place to respond to the internet failing for a number of days are currently likely to be in the minority. Have you taken the time to consider the impact on your business of an extended internet outage beyond your (or your ISP's) control?

It could be argued that organisations should celebrate the miracle that is the internet proving to be so robust for so long and press ahead with business as usual. But having contingency plans in place to survive a sustained loss of internet access is probably wise, from maintaining access to business critical information to interacting with customers and having appropriate insurance to cover losses. The internet is incredible, but this shouldn't blind us to the fact that it isn't a traditional utility and its prolonged failure is an IT risk.

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. This year Stephen is trekking mount Kilimanjaro in aid of Shelter.

WE ARE...

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.

INDEPENDENT

We are not tied to any technology or software vendor. All of our recommendations and technical strategies are based solely on what is fit and appropriate for your business.

GLOBAL, LOCAL

We have over 2,000 security practitioners working in KPMG's network of firms, giving us 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

We 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

We have a long list of certifications and permits to work on engagements for 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 constatntly 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 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.

CONTACT US

Stephen Bonner

Partner

Information Protection & Business Resilience

T: 020 7694 1644
E: Stephen.bonner@kpmg.co.uk

www.kpmg.com/uk/cyber