JANUARY 2016 | VOLUME 43 | ISSUE 4

CONTENTS

Inter MEDIA

TIME FOR IMPLEMENTATION

Our annual conference in Washington in October was the last that I will be presiding over, as we made the announcement that Chris Chapman, currently chairman of the Australian Communications and Media Authority (ACMA), will soon be taking over as IIC president. I'm pleased to say that the IIC could hardly have a better person to lead us into the next stage of our development – Chris set the goal of the ACMA to be a world-leading converged regulator, and his own and the regulator's output have been prodigious in that direction and perfectly match our overarching theme for our events and publications in recent years. Washington marked a turning point in that we are now not so much discussing why and how convergence is taking place, but more how we implement and manage it. With major communications reviews underway and certain new rules in place, our high-level networking is needed more than ever and I'll be watching with great interest. **Fabio Colasanti, president, IIC**

www.iicom.org

The International Institute of Communications is the world's leading independent, non-profit, membership forum engaged with digital media policy and regulatory affairs. IIC activities cover issues in telecommunications, broadcasting and the internet.

Intermedia editorial enquiries:
enquiries@iicom.org
Intermedia subscription and IIC membership enquiries:
Joanne Grimshaw,
J.Grimshaw@iicom.org

Follow us:
LinkedIn
@The_IIC
Watch speakers at IIC events on:
YouTube
www.youtube.com/user/TheIICom
Further content and details are available on the IIC website:
www.iicom.org

NEWS
FROM AROUND THE GLOBE

Chris Chapman, soon to leave Australia's regulator, the ACMA, has been announced as the IIC's new president. He's pictured on the left greeting current president, Fabio Colasanti, who will hand over the reins in April. Amanda Crabbe, the IIC's programmes director, enjoys the moment

EUROPEAN REVIEWS AND ACTIVITY

FRAMEWORK REVIEW UNDERWAY

Europe continues to be the main focus for global communications regulatory activity, with the review of the electronic communications framework now well underway. Various responses to the European Commission's consultation have been filed, including by the UK government's Department for Culture, Media and Sport, which notes the current framework has broadly delivered against its objectives but "the level of investment does not appear to have kept pace with the desired outcome, such as universality of services and quality of experience", and that "there are provisions in the framework that now seem outdated as technology and consumer behaviours have changed". ARCEP, the French regulator, has submitted a response that calls for national regulators to "continue to establish regulatory decisions adapted to their own national circumstances", while BEREC, the body of European regulators, has noted that strengthening the independence of regulators is needed and has urged the Commission to ensure they are adequately resourced.

Other recent European announcements include:

- The European Parliament and Council have reached agreement on the data protection reform proposed by the Commission. The reform package includes the General Data Protection Regulation (GDPR) and the Data Protection Directive for the police and criminal justice sector (see also article on page 29 for a detailed account of the GDPR).
- The Commission has opened a public consultation on how to best set up a public-private partnership (PPP) on cybersecurity, which will be launched in 2016, as part of the digital single market (DSM) strategy.
- Also as part of the DSM strategy, the Commission has published a proposal to allow Europeans to travel with their online content, and "an action plan to modernise EU copyright rules".

The European Parliament has also voted to end roaming charges in Europe by June 2017 and to set net neutrality rules for the first time in EU law, but the net neutrality regulation has come under attack for lack of clarity. Attention is now on guidelines that BEREC is drawing up this year.

- German consultant, WIK-Consult, has won a tender for three studies commissioned for the framework review, on access regimes for network investment; on market entry, management of scarce resources and consumer issues; and an impact assessment for the review.

DIGITAL ECONOMY

ICT FOR DEVELOPMENT

Some 3.2 billion people are now online, about 43% of the global population, but the goal of reaching 60% by 2020 will not be met, according to a UN report. Only 53% will be online in 2020, the ICT 2015 Development Index has found. But almost 7.1 billion people, over 95%, are now covered by a mobile signal. As a way to make connections, the UN General Assembly has adopted the outcome document of the World Summit on the Information Society (WSIS) review, which aims to bridge the digital divide, ensure freedom of speech, and address internet governance to help achieve the 2030 Agenda for Sustainable Development and the new Sustainable Development Goals (SDGs). See article on page 14.

OVER THE TOP

OTT REGULATION TEST

German regulator, Bundesnetzagentur (BNetzA), has taken a lead in discussions on a regulatory framework that includes over the top (OTT) services, asking in a recent conference it organised that the issues should be identified, such as market regulation in the traditional sense of regulating access and price, or aspects such as data protection, data security, transparency and consumer protection. "And do we mean more obligations for OTT providers or fewer obligations for classic telecoms services," said BNetzA president, Jochen Homann. "One thing must be clear: every company has a right to a reliable and consistent legal framework." One answer may have come from a German court, which has upheld a rule from BNetzA that Google must notify its Gmail email product as a telecoms service, but this is likely to be appealed. Meanwhile, the recently closed European Commission consultation on the communications framework includes possible integration of OTT into the telecoms arena.

BROADBAND

MUNICIPAL MAKES GOOD?

The OECD has published a report on the role of municipal networks in the development of high-speed broadband, finding that although private investments have been the overwhelming source of finance for networks in OECD countries, municipal networks have been used in a number of countries to fill gaps or provide substantial areas of service in a region, city or smaller town and surrounding locations. These networks have varied from being highly successful to not meeting expectations; some have provided welcome competition or enabled the use of shared infrastructure. See bit.ly/1JaIQJJ

SPECTRUM

WRC-15 BALANCES TV AND MOBILE

The dust has settled on the World Radiocommunication Conference (WRC-15), attended by about 3,300 delegates from 162 countries and 500 observers. Overall, a balance has been maintained between the mobile industry and broadcasters, which was the major area of tension.

The 700 MHz band (694 to 790 MHz) has been allocated to mobile broadband in ITU region 1 (Europe, Africa, Middle East, central Asia), which will add to global harmonisation efforts, and WRC-15 also identified 200 MHz of the C-band (3.4 to 3.6 GHz) and the L-band (1427-1518 MHz) to improve capacity and coverage. But frequencies below 700 MHz have been left in the hands of broadcasters in region 1, securing the future of digital terrestrial TV (DTT) for a decade.

The European Broadcasting Union (EBU) has of course welcomed the protection of DTT, while the mobile industry has three globally harmonised bands to work with, including in preparations for 5G, and John Giusti, chief regulatory officer of the GSMA, says this is "a major step forward in meeting the growing demand from citizens worldwide for mobile broadband".

Other decisions include allocation of spectrum for flight tracking, following the loss of Malaysian Airlines flight MH370, spectrum for amateur radio services, and the start of standards for unmanned aircraft. Frequencies above 6 GHz will be on the agenda at WRC-19.

- Meanwhile BEREC, the body of European regulators, has said that spectrum needs will vary from one country to the next and 'top-down' harmonisation could risk 'sterilising' spectrum and result in inefficient use, hampering rather than supporting innovation. Instead, it supports harmonised approaches to spectrum management from the 'bottom up'.

DATA PROTECTION

SMART CITIES POSE PRIVACY THREAT

Smart cities combine the three greatest current threats to personal privacy – and which regulation has so far failed to deal with effectively – namely the internet of things, big data and the cloud, according to a paper by Lilian Edwards at the University of Strathclyde. "While these three phenomena have been examined extensively in much privacy literature (particularly the last two), both in the US and EU, the combination is under-explored," she says. "Smart cities are a buzzword of the moment, and although legal interest is growing, most academic responses, at least in the EU, are still technological, urban studies, environmental and sociological rather than legal." The paper suggests research on privacy impact assessments for smart cities, and on how consent could be given for data collection in 'ambient' environments. See bit.ly/1mkLAcY

ADVERTISING

FTC ISSUES POLICY ON 'NATIVE' ADS

The US Federal Trade Commission (FTC) has issued an enforcement policy statement explaining how established consumer protection principles apply to different advertising formats, including 'native' ads that look like surrounding non-advertising content. "The FTC's policy applies time-tested truth-in-advertising principles to modern media," says Jessica Rich, director of the Bureau of Consumer Protection. "People browsing the web, using social media, or watching videos have a right to know if they're seeing editorial content or an ad."

The policy statement explains that an ad's format is deceptive if it materially misleads consumers about the ad's commercial nature. The FTC has published a guide to help businesses comply.

EVENTS

10-11 February, Geneva
EBU Digital Radio Summit

22–25 February, Barcelona
Mobile World Congress

16-17 March, Brussels
IIC Telecommunications and Media Forum (TMF)

2-6 May, Geneva
World Summit on the Information Society Forum 2016

8-11 May, Chicago
International Telecoms Week

29 May-10 June, Botswana
African Internet Summit

IN BRIEF

LITTLE BUT BIG

The World Bank has published the Little Data Book on Information and Communications Technology 2015, which has the most recent national data for 213 economies on key indicators of ICT including access, quality, affordability, efficiency, sustainability and applications.

ACMA REPORTS

The Australian Communications and Media Authority has released the latest iteration of 'The ACMA – meeting our standard', in which it reports on its mission to be a 'world-leading, best-practice converged communications regulator'. See bit.ly/1MC6vNW

FCC RELAXES RULES

The US FCC has relaxed rules on local phone companies that required they support long distance services, provided that alternatives are offered and rural and business customers are protected.

BEREC CHAIRS

Sébastien Soriano, chair of France's regulator, ARCEP, will be chair of the Body of European Regulators for Electronic Communications (BEREC) for 2017, and is vice-chair this year to Wilhelm Eschweiler, vice-president at German regulator, BNetzA.

MOBILE TARIFFS

The ITU has issued a technical guide that will help regulators to set fair and affordable tariffs for international mobile roaming voice services. The guide is accompanied by an online tool.

CONVERGING ON WASHINGTON DC

The IIC's annual conference in Washington in the autumn brought together many of the world's top industry figures and regulators. Convergence is still the main game in town – but the focus is shifting to its management. Report by Intermedia editor, **MARC BEISHON**

The IIC's 2013 Communications and Regulation Week in London – the major annual event for the institute – was held in Washington DC in two main locations. First the International Regulators Forum (IRF) was hosted by the Federal Communications Commission (FCC) at its headquarters – this, like all IRFs, is a 'closed doors' meeting for regulators only. After this two-day forum, the annual conference took place, also over two days, at the Ronald Reagan Building and International Trade Center – the first federal building in Washington designed for both governmental and private sector purposes.

A workshop meeting, hosted by the IIC and Microsoft, also took place at the end of the week on the role that ICT can play in the new Sustainable Development Goals and the contribution of the WSIS review (the World Summit on the Information Society and its vision beyond 2015). See also article on page 14 for a briefing on the issues.

The main theme of the conference – trends in converged communication, and fostering innovation, growth and societal benefit – marked a change in emphasis in the overarching topic of convergence. Debates have moved on from mainly how convergence is taking place, to an acceptance that indeed it is happening at a rapid pace – and how best all players – policymakers, regulators and industry – can adapt rules and strategies to maximise the potential of digital communications and the digital economy.

> **Human capital – capacity building and technical assistance – are probably more important than the 'transfer of cash' for emerging countries.**

One important announcement was made at the conference – that the current president of the IIC, Fabio Colasanti, will be succeeded in the presidency by Chris Chapman, who in turn is nearing the end of his spell as head of the ACMA, Australia's communications regulator. And the 2016 IIC Communications and Regulation Week will take place in Bangkok, Thailand.

FCC'S CHAIR GIVES KEYNOTE

The opening keynote address was by Tom Wheeler, the FCC's chairman, leading off a session on 'connected the unconnected'. He started by picking up a theme he spoke about at the IRF the day before – "We all have the privilege of standing astride a development that has created the most powerful and pervasive platform in the history of the planet," he said. "There's never been a technology like the internet and high-speed broadband to reach so many people so fast." He echoed points made by Colasanti that there are urgent problems facing the planet and technology can tackle the challenges. But 4 billion people are still not connected to the internet and in 49 least-developed countries, over 90% of the population is not online.

Wheeler highlighted the infrastructure goal in new Sustainable Development Goals, now ratified by the UN, which aims to provide universal and affordable access to the internet in least-developed countries by 2020, and to make ICT a development priority similar to more traditional types of national infrastructure. Human capital – capacity building, technical assistance and the exchange of experience – are probably more important than the "transfer of cold hard cash", he said, adding that the FCC's international bureau is active in this sphere.

He noted that the FCC's activities coincide closely with the four subthemes of the IIC's conference, and outlined how this is so, starting with competition, which is "the central tenet of the FCC's policy agenda – I believe that competition is the most effective tool for advancing the public interest and promoting innovation and investment across the ICT sector," he said. "Where competition exists, we must work to protect it and where greater competition can exist we will encourage it and where it cannot be expected to exist we will not hesitate to act to protect consumers," he added. It's what he describes as a 'regulatory see-saw' – as competition goes up regulation can go down and vice versa. As the best example, he cited the FCC's much publicised open internet order, as it "empowers the market to pick winners and losers, not network gatekeepers". The FCC believes that the internet's open design is essential to its success, he said – preserving competition at the network's edge is linked directly to competition between network operators. The simple truth is that fixed broadband competition is limited in most US markets and given their strategic importance to the economy should be "subject to fully effective oversight... No one, neither government nor private sector, should intervene with public access to lawful content, applications and services."

He added that the open internet order is a new regulatory model for modern times, and is like a referee on the field of play, and if the rules are broken, "We will blow the whistle." But there will be no micro-management – no rate regulation, network unbundling, and no tariffs. "No utility style regulation," Wheeler said, and he believes the rules will both protect openness and foster massive private investment in broadband networks.

Turning again to the unconnected, he commented on the investment and take-up in the US, but local demand in some rural locations won't support investment. Ten million Americans can't get wired broadband at all, and there are still six million who can't get 3G mobile. He described how the Connect America fund is giving $9 billion to private operators to help plug these gaps, but he also said there are further challenges on the demand side, as only 48% of low-income Americans have broadband (those earning less than $25,000 a year), and he stressed how technology must meet the needs of people with disabilities.

On the internet of things (IoT), he cited Cisco's projection of 50 billion such devices by 2020, and a huge $8 trillion in economic value over the next decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this value will need tackling a new set of challenges. Cybersecurity is one, given that there are potentially billions of 'attack vectors', and Wheeler mentioned a framework developed by the US National Institute of Standards and Technology (NIST) for cyber-risk management, and the FCC has been meeting with companies to assess how effectively such risk is being managed according to the framework. "The key question is, are the cybersecurity protocols that we're all agreed on working," he said.

Right: Tom Wheeler, FCC chairman, in full flow in the opening keynote Left: a panel convenes in the conference room

On spectrum, Wheeler said new approaches are needed for ubiquitous connectivity, and the FCC has been working on expanding unlicensed spectrum, flexible use policies, sharing, new bands for mobile, and the upcoming incentive auction. The FCC has also embarked on a 5G strategy, and he said: "Global harmonisation is critical."

Finally, Wheeler touched on over the top (OTT), where 40% of US consumers already subscribe to services such as Netflix. And it's about spectrum and mobile too – a wireless operator has said 60% of its traffic is now video, he noted. The OTT movement is also a major factor in merger review. Competition between OTT and traditional video distribution models is central to any merger analysis, and access to programming on competitive terms is crucial for OTT entrance to be successful. "There's a line of new OTT providers queuing up to expand video choice and demand for broadband," Wheeler said, adding that supporting the growth of local content is also important.

> **The open internet order is a new regulatory model for modern times, and is like a referee on the field of play.**

TARGETING THE UNCONNECTED

Mauricio Ramos, CEO of Millicom, kicked off a detailed session on connecting the unconnected in both mature and emerging markets. Millicom is an operator in Latin America and Africa, and Ramos described how the supply and demand side can be approached in his markets (see Q&A, page 12). Kemal Huseinović, head of the ITU's infrastructure department, said regulators have a crucial role in bridging the digital divide, although there is no 'silver bullet' in boosting the ICT sector. He put up a slide that showed how different regulatory priorities have shaped the ICT sector over time, with clear moves towards more infrastructure

sharing, broadband plans, allowing people to use voice over the internet, and adoption of class/general licensing. He highlighted the gender gap as a big issue in tackling digital divides. Infrastructure alone is not sufficient – new services and local content are vital, he added.

Huseinović outlined four generations of regulation – regulated monopolies, opening up competition, an enabling environment to boost investment, and finally what he terms integrated regulation, where regulators and policymakers are now under pressure to ensure they stay relevant in the digital world to meet social goals. The fourth generation involves integration with other sectors such as financial regulation for social inclusion. Europe is ahead in '4G' regulation he noted.

Google's Ross LaJeunesse, head of international relations, spoke first about the demand side of the search giant's activities, noting that it caters for 180 languages, and its translate tool is also growing in scope. The supply side though is a new part of Google's business and is looking at electricity supplies, reducing the cost of accessing the internet, and also at backbone infrastructure. LaJeunesse highlighted a solar energy project in South Africa, the continent where Google is focusing much of its efforts, he said, and kites that generate electricity from the wind (a project called Makani) that cuts a lot of the cost of using wind turbines.

"A lot of people laughed at our Loon balloon internet project that can provide internet access in remote areas," he added, "but they're not laughing now." A stationary internet drone project called Titan is also underway, and Google is pushing to lay fibre, and a ring is now in place around Kampala, Uganda. In South Africa, LaJeunesse says the company has worked with the regulator to release unused spectrum for wireless, and he noted investments in undersea cables and data centres.

Carlos López Blanco, Telefónica's global policy and regulatory affairs head, first described the way telecoms is now competing with internet players as part of a 'single universe', but the internet is also changing, from north to south, fixed to mobile, and open to closed, the latter meaning the rise of Facebook, Google and others. It means too a new agenda for telcos, including net neutrality, a level playing field, 'digital confidence' in privacy, and access. The key challenge in developing countries is internet access, not quality, reliability and speed.

Taking Brazil as an example, López Blanco showed how strong investment in telecoms infrastructure can lead the way in emerging economies, as the country now ranks much higher in mobile and fixed infrastructure compared with other countries than it does in sectors such as roads and railways. Stable and equal regulation that promotes investment is critical, with private-public partnerships where private only is not feasible. He also highlighted spectrum policies that are not just revenue raisers, and government broadband plans that are non-discriminatory. "Universal service is a common challenge for governments and companies," he said. Finally, innovative commercial services are needed to reach more people.

From top: the panel on connecting the unconnected, with Telefónica's Carlos López Blanco speaking; Pranesh Prakesh, policy director, Centre for Internet and Society in India, asks a question; an earnest exchange of views and cards; delegates from South East Asia during a coffee break

CONTENT – FROM THE US TO INDIA

The conference moved on to content and applications and the tension between OTT and legacy players. Consumers can now 'gorge' on video content, said Rebecca Arbogast, VP of global public policy at cable firm Comcast, and she quoted a media commentator, David Carr, who had said that the excellence of new TV shows threatens to consume people's waking moments. In 2015, there were 400 original series shown in the US, double from a few years ago. "And we are only beginning to scratch the surface of user-generated content."

It still feels radical, she noted, that users are in control of where and when media are consumed. This is changing the shape of bundles, with smaller 'skinny' offerings now on the market. Makers of devices, such as Tivo and Apple, are going head to head in media delivery and lines are blurring between networks, programmers, distributors and equipment providers, "which is exciting but calls into question existing regulatory structures".

The further tension between global, regional and local content impacts trade, jobs and cultural values, said Arbogast. "At Comcast we create both global and hyper-local programming", such as in Hispanic areas, she added, mentioning the debate in Europe about territorial licensing and protecting local cultural and language content.

In the US, much of what the FCC wants to achieve in video is happening, such as rapid growth in choice, and there is no need to intervene. When cable TV was first regulated in 1992, it owned 98% of pay TV – now that's 53% – "Don't regulate for regulation's sake but recognise the market is in extreme flux... focus on modernising the regulatory approach," she concluded.

Pulak Bagchi, VP legal and regulatory at Star India, the country's largest TV company, painted a contrasting picture about his country where, despite being number one or two in the world TV market and the world's largest film producer, economic value is small. He said media sectors with the most regulation are doing worse than those with lighter regulation, such as film and print. The rise of millennials in India is driving smartphone and mobile internet adoption, and new edge providers are dominated by Indian music-based players, although YouTube is doing well, and Star's own Hotstar video service achieved 10 million users in just 40 days.

The ambitious Digital India plan for a national broadband network is running well behind schedule and it is a challenge for operators to monetise data traffic, and the rise of OTT players such as Facebook is under close scrutiny by the Indian regulator and government, said Bagchi, who asked whether the internet will tread the same path as traditional media in huge numbers but poor monetisation. There is no shortage of new content offers, and there is much business activity, he added, but a danger of legacy linear TV regulation being carried over into the new converged world.

Concluding, he said that the internet in India can break the monetisation 'jinx' if OTT is allowed to have full market dynamics in play.

FRESH THINKING ON SPECTRUM

In a keynote, Craig Silliman, Verizon's general counsel, said his company will keep on delivering the promises of the digital future but policymakers need to also deliver the right environment in three main areas, spectrum, access to backhaul and global coordination. On spectrum, he said a pipeline of new capacity is needed but in the US it takes on average ten years to redeploy spectrum and the 'low hanging fruit' is already picked – after the incentive auction, no more is planned, he said. "Human factors in getting folks to relinquish spectrum may be as significant as the technical ones," he added.

Sharing is a key approach and may be more important when moving to higher frequency bands, but it can lock in inefficient use of federal spectrum. Flexible use terms, such as in the AWS bands now used for 4G, have also proved important, as is a thriving secondary market governed by rules. Silliman also highlighted improving utilisation through WiFi and unlicensed LTE, which he says "interacts with WiFi better than WiFi does with itself". As for 5G, there are new challenges for policymakers as it may need higher frequencies, so they need to work early with industry – "We can't afford to wait ten years," he said.

Silliman then made the point that wireless also needs wired backhaul, which in the future may be from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum is also key for many reasons.

Julius Fritz, from One Media, a new TV broadcast platform, asked how you would judge what has more value – a one to many broadcast service or a one to one mobile experience. He showed how if the US incentive auction succeeds, a remarkable 65% of broadcasting channels will have been reallocated, but from his perspective the future of free to air TV could not be brighter thanks to a new IP standard that will support high definition and mobile screens, and 'deep building penetration', and will also allow innovation without ongoing regulation.

> **"Sharing is a key approach and may be more important when moving to higher frequency bands, but it can lock in inefficient use of federal spectrum."**

AT&T's Carl Povelites said that the mobile industry needs new licensed and unlicensed spectrum. On the licensed front he said there needs to be a large band size to accommodate multiple competitors, large block sizes for broadband, adjacency to existing bands, international harmonisation for economies of scale, and auctions without restrictions on who can bid. On unlicensed, there's activity in the 5 GHz band in the US. He added that temporal sharing is not well understood, unlike geographic models.

In discussion, it was said that spectrum reallocations are very hard policy decisions to make, and if governments could 'internalise' the value of spectrum it could make such decisions easier.

INTERNET OF THINGS

Panelists on the IoT session chipped in with a number of introductory thoughts. Ericsson's Bruce Gustafson noted there are two camps – a communications mindset that focuses on interconnection of billions of devices, and an IT bias that sees IoT as an expansion of the internet and is more interested in data flows. His view though is that IoT is a more complex issue, and he used the example of the Sim City game to show that it is analogous to having a software simulation of a virtual city to control a real city. "IoT is Sim City applied to real cities using real data in real time – a much bigger challenge than just connecting billions of devices."

> **An important issue is automation – as connected devices become more prevalent, people may lose essential skills.**

There are three steps to IoT, he said: mobile phones, apps and sensors are first; shared economy assets are in step two; and in step three everything talks to everything else.

The discussion moved quickly to possible regulatory issues, as Gustafson said lack of trust and privacy are the biggest threats to IoT. Matthew Jennings from Bosch said his company makes several million sensors a day and there is already a lot of data being generated so there is a need for policy, standards and security, but issues vary according to industries, such as in healthcare.

There was debate too on how the value of connectivity can be measured as data flows across various networks, and the way forward is likely to be experimentation with business and socially beneficial applications such as in farming. For manufacturers, IoT can change business models from a business to a service mentality, said Jennings, as they can be in touch with products in the field.

The role of telecoms and network providers becomes more important in adding value to companies that conduct much of their business by exchanging data, such as with Uber, he said. "There's a new generation looking at sharing rather than owning assets." For IoT, there will be questions about whether cellular networks can accommodate traffic, and perhaps private networks will spring up to fill gaps for certain applications in cities. An important issue is deskilling and automation – as connected devices become more prevalent, people may lose skills.

Aaron Burstein, an advisor at the US Federal Trade Commission, said the FTC has looked broadly at IoT and taken the view that basic consumer protection principles apply to the new technologies involved. As examples, he said consumers should still know about what sorts of data are being collected and should give consent, and under the agency's unfairness authority if a company fails to take reasonable data protection steps, it can still be acted against even if it hasn't published protection provisions. There was discussion about whether privacy rules could be too restrictive for IoT and Burstein said the FTC's view is that companies should think about what is meaningful and the context in which consumers use devices.

RS Sharma, chairman of India's regulator, TRAI, gave a detailed account of initiatives such as smart cities and public-private industrial policy that will affect the development of IoT in his country.

DIGITAL TRENDS

This session was about how regulators and policymakers can respond to changes in use of digital media. Robert Pepper, Cisco's technology policy expert, spoke on video usage, noting that his company's visual network index, which now goes back ten years, and projects traffic growth, was within 10% of its 2010 projection for 2014. Looking ahead, internet traffic will be growing at a 23% compound annual growth rate until 2019, driven by more users and devices, faster broadband speeds and of course, more video, which will be about 80% of traffic by 2019, and over 70% of traffic on mobile operators' networks will be video, Pepper added. As an aside he said: "There's no such thing as a mobile network – the network doesn't move, I do," noting that wireless traffic has to go to base stations and to a core network, and that TRAI's chairman, RS Sharma, had earlier spoken of the need for fibre backhaul as a vital plank of the Digital India initiative. "India gets it," Pepper said.

Further, even if people don't spend more time with video, the step up to high definition and ultra high definition will drive more data traffic. As for devices, by 2019 43% of connections will be machine to machine (M2M) but will be only 3% of traffic, with a wide range of requirements in terms of factors such as latency. And Pepper added that countries such as Korea and Japan will have a much higher percentage of devices that are M2M than those at the other end of the scale, mainly emerging countries. "This is a third wave of the digital divide that I think is unacceptable," he said (the first wave was phone, the second connecting to the internet).

"I really hope our forecast is wrong on this as it is avoidable," he added. Countries could miss out on the economic benefits of IoT in sectors such as manufacturing, energy, healthcare and more. "It's a tale of two networks – capacity driven by video and number of devices by IoT/M2M," said Pepper, "and it's leading to incredible complexity that we will need to manage," such as with different types of spectrum. He mentioned the Industrial Internet Consortium, which now has more than 200 members, as one of bodies addressing the questions.

Nuala O'Connor, president of the Center for Democracy and Technology, spoke about the attacks on free speech, such as by the hackers who broke into Sony in response to the film about North Korea, and of course the attack on Charlie Hebdo in Paris. "But the response from governments around the world is to clamp down further," she said, noting that 20,000 Twitter accounts were taken down. "The internet is not the cause of terrorism – I come from Belfast in the 1960s and there were terrorists before the internet," she said. Further, there are individuals, especially men, who misuse the internet and reinforce existing power structures, she added, asking delegates to think about how 'digital dignity' can be maintained.

Sky's David Wheeldon described how empowering users with linear TV tools such as watershed protection can be applied to OTT products and broadband, and Facebook's Kevin Martin showed how users in emerging markets can be brought into the digital age through the Free Basics app.

COMPETITION CONUNDRUM

IIC president, Fabio Colasanti, introduced the closing plenary, on competition, which he said is proving to be one of the most intractable issues, in particular whether European approaches to opening up networks are sufficient. Mirko Bibic, chief legal and regulatory officer at Canada's Bell, showed how services such as broadband have grown from 56% to 81% of revenues in ten years at Bell, and legacy phone is now only 9%, and echoed earlier points about the benefits of broadband. He noted that regulators – in the US, Canada and Europe – are stating publicly that competition is an underlying theme. "But how do we get there? Too often, policymakers and regulators can lean towards the short-term, with an emphasis on lowering price, but that invariably comes at the expense of durable, long-term facilities-based competition." Creating incentives for companies to lay next generation technology and using ex-post competition policy is the way forward, Bibic said, referencing points made by FCC chairman Tom Wheeler in the opening address.

Sizing up an issue during a tea break

> **Countries could miss out on the economic benefits of IoT in sectors such as manufacturing, energy and healthcare.**

Steve Unger, from Ofcom in the UK, described the regulator's strategic review, which is taking place ten years after network unbundling was undertaken. He highlighted availability of fibre networks, noting that the regulator's main job is to ensure people don't get left behind, and not to rule on technology or price. "At present about 8% of UK homes don't have 10 Mbps broadband – for me that's one of the biggest issues in the review." On competition, Unger said Ofcom is as concerned about mobile as fixed, and is keen to focus on end to end competition, rather than remedies that promote virtual operators.

In fixed networks, he said the question again is whether access-based competition is still the best model, rather than end to end. There is also debate on access to passive infrastructure. Unger set out options for changes to the Openreach wholesale operation, noting that separation from BT is the most controversial.

In discussion, Unger said he doesn't see major tension between competition and investment for network availability – but service innovation to drive social and economic benefits is key.

WHAT ELSE HAPPENED DURING THE IIC'S WEEK?

The International Regulators Forum (IRF), which took place at the FCC, focused on the following themes:

- Regulatory innovation – this session asked the question, 'What do citizens want from their regulator?' There was comment that telecoms is looking more like other markets such as energy in terms of regulation.
- Competition market failure – wide-ranging discussion covered topics such as tackling bottlenecks, licensing and consolidation.
- Consumer protection – this session looked at the rapid multiplication of content, protection vs free speech, 'must carry' rules , cultural identity, and linear vs non-linear.
- Digital divide – regulators shared plans that address supply and demand, ideas such as a digital inclusion fund to help access public services, and an overall point was made that technology alone can't solve all problems.
- The unregulated – here the regulators focused on OTT and VoIP, raising issues such as licensing, plurality, advertising and convergence.
- Spectrum – the US incentive auction was described, and general subjects included the challenges of refarming, new uses of spectrum and higher frequencies for 5G. Sharing is seen as 'key to the future'.

Breakout groups

In the annual conference there were also a set of lively breakout groups on topics such as the sharing economy, next-generation networks, net neutrality (in the light of the FCC's open internet order), internet governance, and 'digital kids' – how to protect children, where the point was made that there needs to be more interaction between parties such as search engines, payment processors, domain name registrars etc. to raise the protection bar.

SDGs and the WSIS Review

A workshop hosted by the IIC and Microsoft (see page 14).

Q&A

With **ADRIANA LABARDINI**
commissioner at Mexico's IFT

Q WHAT IS YOUR POSITION?
A I am a commissioner at the Federal Institute of Telecommunications (IFT), Mexico's independent regulator and competition authority for the telecoms and broadcasting industries, created by constitutional decree in June 2013. The board consists of seven commissioners who, after a very competitive examination process, were nominated by the president of Mexico and appointed by the senate for a fixed term tenure.

Q AND YOUR BACKGROUND?
A I am a lawyer, specialised in telecoms regulation and public policy. I earned a masters from Columbia University, where Eli Noam lectured on telecoms courses at the business school and worked as his assistant at the Columbia Institute for Tele-Information at a time when market liberalisation and privatisation of telephone operators were taking place in many countries, and the impact of the AT&T divestiture was being studied by scholars, policymakers and investors. On my return to Mexico City in 1991, the incumbent, Telmex, was being privatised and a new legal framework was being discussed and I was fortunate to be able to participate in the national debate on fostering competition in a traditionally monopolistic sector. I worked as an advisor to the ministry of communications as an outside counsel but eventually joined the then regulatory agency, Cofetel, for four years but went back to the US on a Humphrey fellowship. I came back in 2004 determined to start an independent organisation to promote consumer rights for telecoms and other utilities, some of which were badly abusive without consumer advocates.

> **"There is still much to do in Mexico to raise awareness of consumer rights as corporations have not had a culture of customer satisfaction."**

Q THAT SOUNDS INTERESTING...
A I wanted to help consumers have a voice, especially in telecoms which of course I was familiar with. But I found a lot of problems and complaints about other services such as financial and transportation services, and other public services as well. There was only expensive and complex access to justice, no class actions for consumer claims, inefficient consumer protection procedures, and poor education of consumer rights. I realised that we really needed more effective collective actions to access justice, so we fought for Congress to introduce class action legislation so that entities could represent consumers before the courts. After a four year effort, we succeeded in getting an amendment to introduce class actions procedures for consumer and environmental claims, and also antitrust cases. I worked on this independently through Alconsumidor, a non-profit organisation I founded with a partner, which became a member of Consumers International. There is still much to do in Mexico to raise awareness of consumer rights issues as corporations have not had a culture of customer satisfaction and social responsibility, because competition had not been all that strong and consumers were held captive by rent-seeking corporations.

Q WHAT ARE EXAMPLES IN COMMUNICATIONS?
A There are lots of examples, some of which we have addressed at IFT, because we have broad powers and autonomous status. Using both regulatory and competition mandates, we have been able to remove some barriers to foster competition in both the fixed and mobile markets, which are highly concentrated, with high prices, still low penetration and not the best quality. The incumbent would charge domestic roaming even though it had a national network, high interconnection rates, and impose abusive contracts on users. Through asymmetric regulation we have ended domestic roaming charges, lowered termination rates, mandated infrastructure sharing and unbundling, and the incumbent has to go to public tender for all its wholesale services. There are also problems and abuse in pay TV, with long-term contracts, high penalties if you want to terminate contracts earlier, high priced premium packages, and a vertically integrated broadcaster, content producer and cable and satellite distributor. A combination of competition and regulation is our strategy to enable a more efficient market.

Q IT SOUNDS LIKE THE INDUSTRY WOULD OBJECT TO A CONSUMER CHAMPION AT THE IFT...
A Well yes, but the industry knows I am truly independent, without any business or political agendas, and my concern for consumers has been honest and legitimate. I understand that our industry needs incentives to invest and grow, but it has to understand the benefits of more competition and the need to gain their customers through good service and prices, and fair practices and contracts – or lose clients. President Peña Nieto looked closely into the commissioners' exam results, credentials and personal history, I assume, and he and the senate appointed three lawyers, me included, two economists and two engineers. We all bring value to the table, and we have all become engineers, economists and lawyers in a way. About 800 people applied as there was a lot of interest in becoming part of the founding board of IFT. The president was given 35 names out of which he picked seven, then confirmed by the senate. I was talking to regulators from other countries at the IIC's International Regulators Forum in Washington and they were very impressed with this selection process.

Adriana Labardini, commissioner at Mexico's IFT

Q HOW ARE THE IFT COMMISSIONERS ORGANISED?
A As commissioners we all have to vote on the proposals the different units submit to us, including antitrust procedures, rulemaking, licence applications, spectrum auctions, sanctions for illegal practices, technical standards, mergers, content related issues, interconnection, complaints and more. The IFT has a staff of more than 1,200, and the commissioners each have eight or nine advisors. I also chair the transparency council, in charge of reviewing cases of denial of access to information, and sit on the ethics and civil careers committees.

Q THE WHOLESALE MOBILE NETWORK IS A BIG MOVE...
A This is a disruptive model mandated by constitutional amendment to use the 700 MHz band, which will be freed after our analogue TV switch-off is concluded, for an open access, wholesale 4G network, from which current operators and MVNOs will be able to buy capacity across the nation to accelerate mobile broadband services. It will be for the internet of things, multicasting, telemedicine, national security services and much more that requires mobile connectivity not available in Mexico, where 4G is only starting to take off. The wholesale shared network is meant to be a public private partnership (PPP) to be adjudicated through a bidding process that will take place this year. The government will contribute 90 MHz of spectrum in the 700 MHz band, using the APT 700 standard, and the winning developer will start operating the network in two years. The IFT's role is to issue terms and conditions of licence and bidding rules to make sure the PPP acts on the basis of competition neutrality, offers capacity on a non-discriminatory basis and makes the most efficient use of spectrum to meet its goals.

Q THERE'S A LOT HAPPENING...
A Yes, we are also auctioning 80 MHz in the AWS band in February, which we hope will enable more competition among the three existing carriers and better quality of service. On TV, after having only two commercial networks for decades, we auctioned a third national network in 2014 and we will auction a fourth this year. There's an urgent need for competition and plurality in Mexican media that requires more spectrum, public and community broadcasting including radio and TV for indigenous groups across the country, and 'must carry' rules for cable and satellite TV licencees that have access to the over the air channels in their coverage areas. We have also been very successful in lowering interconnection rates, and our new telecoms act also eliminated domestic long distance charges, and the incumbent's ability to charge termination rates. Only the other mobile and fixed carriers may charge LRIC-based termination rates. And we have set up a new consumer affairs division at IFT to provide information tools for consumers so they can easily compare rates, quality of service and packages.

Q DO YOU REGULATE CONTENT?
A At present, IFT has some powers of surveillance of children's rights and media, caps for advertising time and other guidelines dealing with audience rights. We are working on guidelines for broadcasters, which must hire an ombudsman to take care of complaints from their audiences. I am interested in comparing methodologies to measure plurality in media, and I am also following the debate about over the top (OTT) players and whether they should be licensed or otherwise regulated. So far, we have not opted for licensing, but that doesn't mean that they are exempt from competition, privacy or consumer and protection rules for minors. We have some brief net neutrality principles in our new telecoms act.

Q FINALLY, WHAT ARE YOU KEY AIMS?
A In the two remaining years of my tenure, I will keep working to make sure consumers have competitive options nationwide, contribute to bridging the digital divide, and work very hard to strengthen our organisation to make sure we are efficient, transparent, inclusive, and highly professional and expert in our field, and the best regulator and competition authority in our region.

Q&A

With **MAURICIO RAMOS**, CEO of telecoms and media firm, Millicom

Q WHAT IS YOUR BACKGROUND?

A I'm from Colombia, where I obtained degrees in economic and law. I've worked in the office of the president of Colombia, taught economics and worked in investment banking before joining the cable firm, Liberty Global, in Latin American roles. After 15 great years at Liberty, it was time for a change and I saw that Millicom has a platform for fixed-mobile convergence, of which I am a strong advocate. It made sense to bring in a 'cable guy' who believes in mobile and I joined as CEO in 2015.

Q MILLICOM IS PRIMARILY IN EMERGING MARKETS...

A Yes, we operate mainly in Latin America and Africa, under the Tigo brand name – in frontier as well as emerging markets – and 70% of our business is mobile. We like to say that Millicom is the little known $6.5 billion telecoms provider – but we have been around for 25 years and have 60 million customers. Historically the company focused on 2G mobile and then made the transition to 3G, but Millicom came on my radar because it was also one of the companies that started buying and investing in cable networks, with the goal of being a convergent provider of services in the markets where it operates. So, being very familiar with the Latin American landscape, this caught my attention. We want to build cable in our markets and provide consumers with seamless connectivity between fixed and mobile. We have also launched 4G where licences have been granted, with a few exceptions at present. So we have made a leap into a data proposition for our consumers, both in mobile and increasingly on fixed.

> **"The only way to limit the digital divide is to embrace the ubiquity that mobile provides, with the capacity that only fixed can provide."**

Q SOME DEVELOPING COUNTRIES HAVE DIFFICULTIES EXPANDING FIXED BROADBAND THOUGH...

A My personal view, and the company's view, is that the only way to limit the digital divide between developed and developing and emerging countries, is to fully embrace the ubiquity that mobile provides, with the capacity that only fixed can provide. That is the only alternative that most of these markets really have to provide a robust internet experience, with lots of bandwidth. The cost of providing a bit over a fixed network is a fraction of the cost of providing a bit over a mobile network. The spectrum on mobile is by definition limited, whereas the spectrum for fixed services can be created on a modular basis. So as consumers demand more data, wherever it is possible, fixed and wireless need to be provided and converged as otherwise they will have limited experience. Now, this will not be true everywhere, because the economics of providing broadband are largely dependent on density. In areas of low density, fixed won't work and spectrum becomes increasingly important to get coverage. So it really is a combination of all the tools that are available.

Q WHAT ARE EXAMPLES FROM YOUR MARKETS?

A Take a relatively small country such as Bolivia, where mobile network coverage is significant, and 4G services have been launched, but fixed networks have not yet been truly built. It's a country where I can envision that 50% to 70% of homes could be serviced economically with cable because the density is there and networks can be built in an economically viable way. Colombia is another important example. It has a population of about 45 million and about 10 to 12 million homes, depending on what census you take. You would think that in a growing economy you can easily reach 60% to 70% of those homes, about 6 to 7 million. Our network currently covers about 4 million, so there is an opportunity to launch more fixed networks there.

Q DO YOU MEAN CABLE OR BROADBAND?

A Cable is broadband but it's a hybrid technology. For some reason, cable has allowed itself to be labelled as not fibre, and that's not true. Hybrid fibre coaxial (HFC) is mainly fibre, and only in the last small part to the home does it become coaxial. That gives us the ability to take fibre closer to the home to the point where it could eventually be taken all the way, but it's just not economical to do so at present. In developed markets, average speeds are 40 Mbps on fixed networks, but in emerging economies they are 2 Mbps, at best. We need to take it step by step and HFC cable is the most modular of those technologies and of course can be seen as creating our own 'spectrum' – a mobile operator typically has about 60 MHz available, whereas the type of HFC cable network we are currently building in Bolivia, El Salvador and Guatemala is 1 GHz, a gig of 'spectrum'. It really is a matter of being smart about what network delivers what bit, to what subscriber, at any point in time.

Mauricio Ramos, CEO of Millicom

Q YOU MAKE IT SOUND STRAIGHTFORWARD...

A Well it's a huge challenge to get the right ecosystem that combines fixed with mobile to reach the most people, with all that entails in investment and allocation of spectrum, including low frequency spectrum for rural areas. It's also the case that existing asymmetric technologies won't be adequate for consumers and for machine to machine communications, apart from in broadcasting, where cable, digital terrestrial and satellite TV are fine, and in fact we are also in the direct-to-home satellite market. But on the internet the future will increasingly be unicast and symmetrical as users will want to upload things like video chats, and it's more than just a technical challenge.

Q IT WILL REQUIRE YET MORE INVESTMENT...

A Yes – over the past ten years, when commodity prices were high, most emerging economies were being buoyed in their purchasing capability, because their exchange rates were relatively strong. Looking forward, that's not going to be the case. So that's one of the biggest challenges I think we have in connecting the unconnected in emerging markets – players in these countries need hard currency to make investments in new network technology.

Q WHAT IS YOUR READING OF HOW QUICKLY WE ARE CURRENTLY ADDRESSING CONNECTIVITY GLOBALLY?

A Overall about 65% of people not using the internet are in emerging markets and the connectivity challenge has of course been met much more quickly in mature markets. But connectivity growth has actually been slowing down in both mature and emerging markets – in the latter it's actually gone down from about 24% between 2001 and 2005, to an estimated 12% between 2010 and 2015. So in total there are still about 4 billion unconnected people on the planet – more than those connected – and assuming a rate of 12% stays steady, it will take decades to connect them, although we will see a billion new users by 2020 or so. We have to realise that connectivity can be life-changing for emerging market consumers, with applications such as mobile financial services.

Q WHAT ARE THE BEST MARKET APPROACHES?

A We have to be very consumer focused to address both the supply and demand problems. In fact, many of the supply problems are being addressed – up to 80% are on their way to being covered by mobile networks, and mobile devices are getting cheaper, but operators need to be very careful in not complicating a product offer. Most of the work needs to be done on the demand side in emerging markets, as when you take that 80% or so coverage, only about half actually take up a service, despite the fact that 3G phones are now less than $40 and there is little complexity in prepaid models. The number one issue is for people to actually value using the internet, and number two is digital literacy and local language content.

Q HOW ARE YOU ADDRESSING BOTH SUPPLY AND DEMAND AT MILLICOM?

A As I said, this is a business where money gets poured into the ground first, which we've done, but reducing the cost can be done with sharing – in Colombia we've built a 4G network with Telefónica with the blessing of the government. And about 60% of the 3G handsets we sell are entry level models but it's also important to provide financing, which we do for example in Paraguay. On the demand side, we have found that the best way to educate users is to first educate our salesforce. So far we have trained 8,000 door to door salespeople in our Tigo sales school on what the internet means on a mobile phone and what apps can be put on, so they have a selling proposition that explains the advantages. In our markets, mobile is sold through thousands of points of sale – it's not a few outlets in a shopping mall but many individuals who are the catalyst to explaining the internet. Using mobile financial services, used say for top-ups, is key to showing what connectivity means – and today about 4.5% of Paraguay's GDP is done this way. And local content is also vital for our value proposition.

Q HOW CAN POLICYMAKERS SUPPORT YOU?

A Competition is important and there is an issue we need to address in emerging markets, which is that network operators book revenue locally but the over the top (OTT) players book globally. I've mentioned spectrum, and would add that emerging markets currently have half that of mature markets and a huge amount of work is needed to refarm and release it for use in our fixed-mobile convergence models. There is a balancing act – we know that competition can fragment spectrum holdings and high auction prices can result in successful bidders lacking capital resources. And the strongest policy initiatives we've found are those that promote demand, such as e-government initiatives. As for the investment challenge, governments that abolish say VAT on handsets can help greatly in the connectivity drive.

FOCUSING ICT ON THE NEW UN DEVELOPMENT GOALS

How can ICT best be deployed to advance the new Sustainable Development Goals? **M-H CAROLYN NGUYEN** and **PAUL MITCHELL** review the history and current position

Self-contained: a solar-powered internet cafe in Kenya built from a container and connected by white spaces spectrum (Microsoft)

The internet and advances in information and communication technologies (ICT) have revolutionised our lives – the way we find information, the way we communicate, how we run our businesses, how we entertain ourselves, how we share knowledge – the list is endless. They have also transformed global economies. It is estimated that the internet accounted for 21% of GDP growth in mature economies from 2004 to 2009 and is worth 3.4% of GDP across the large economies that make up 70% of global output.[1] There is clear evidence of a correlation between the maturity of the internet ecosystem and several other measures, including increased innovation, entrepreneurship, creation of new business models, and a general rise in standards of living.

Technologically, the internet is a network of networks that serve as a platform for other technological innovations. Cloud computing builds on the internet to make available services and applications globally, democratising access to information, knowledge, and computing resources around the world. This has the potential to transform the 95% of businesses in the world which are small and medium enterprises (SMEs), and which are responsible for about 60% of private sector employment.[2]

Healthy local SME ecosystems directly impact sustainable economic development as they can develop locally relevant content and services more quickly, provide faster responses to local market demands, and have more immediate impact on local job growth. For entrepreneurs and SMEs, the cloud lowered the cost of capital investments and IT skills required, enabling them to compete on an equal footing with larger and much better resourced entities – IT-enabled SMEs increase revenues 15% faster and create jobs almost twice as fast as other SMEs.[3]

Availability of cloud resources in turn drives a number of other opportunities. Data analytics and machine learning bring the promise of an intelligent cloud that enables more effective and efficient solutions in a wide range of sectors, including healthcare, disaster response, agriculture, sustainability, and transportation. The internet of things (IoT) can help the farming industry meet the demand to increase food production by 70% by 2050 to feed an estimated population of 9.6 billion people, while also addressing the anticipated challenge of climate change and potential impact of intensive farming practices.[4] For crop farmers, for example, the IoT will mean being able to prepare the soil, plant, and harvest at precisely the optimal time given predicted weather.

It was in recognition of the fast pace of the ICT evolution and potential impact on development that in 2001 the United Nations (UN) General Assembly (GA) agreed to convene the World Summit on the Information Society (WSIS) to define and realise a vision of what should be achieved in two phases: the Geneva Summit in 2003, and the Tunis Summit in 2005.

The Geneva Principles declared the common vision of the information society as *"a people-centred, inclusive and development-oriented information society, where everyone can create, access, utilise and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purpose and principles of the Charter of the United Nations and respecting fully and upholding the Declaration of Human Rights."*[5]

It recognised that ICT and the internet must be integrated into national and regional strategies to advance sustainable development. The principles also raised the need for internet governance, and called for a working group that would make appropriate proposals for actions in the 2005 summit.

ADDRESSING THE WORLD'S CHALLENGES

In the late 1990s, at the same time that tremendous progress was being made on ICT, and the potential of ICT for sustainable development was being considered, there was a concerted global effort to address global challenges such as poverty, nutrition, human rights, and lack of participation by women. This culminated in the Millennium Summit in September 2000, where 189 world leaders met and adopted the UN Millennium Declaration, committing their respective countries to a new global partnership to reduce extreme poverty and setting a series of time-bound targets to be achieved by September 2015.[6]

There were eight Millennium Development Goals (MDGs), aimed at eradicating poverty and hunger; achieving universal primary education; promoting gender equality; reducing child mortality; improving maternal health; combating HIV/AIDS, malaria, and other diseases; ensuring environmental sustainability; and developing a global partnership for development. The last goal on partnership emphasised the need for developed countries to aid developing countries with development assistance and other policies including market access, debt relief, and increased access to ICT.

Although the MDGs have succeeded in focusing attention on addressing extreme global poverty, progress has been uneven. Some of the achievements include decreasing the number of people living in extreme poverty by more than half, from 1.9 billion in 1990 to 836 million in 2015; increasing the literacy rate among youths globally from 83% to 91% between 1990 and 2015, and narrowing the literacy gap between women and men; and improving internet penetration from just over 6% of the world's population in 2000 to 43% in 2015.[7]

However, there remain large gaps affecting the most vulnerable populations in equality between genders, between developed and developing countries, and between rural and urban areas; progress in climate change; ongoing threats of conflicts and their impacts; and the more than 800 million people still in extreme poverty.

In 2012, the UN Secretary General launched a consultation on a post-2015 development agenda that would incorporate learnings from the MDGs and define a broader framework to advance the initial objectives. In September 2015, the 2030 Agenda for Sustainable Development was adopted by 193 countries with 17 Sustainable Development Goals (SDGs) to be achieved by 2030.[8] The SDGs reinforce the MDG goals of *"eradicating poverty in all its forms and dimensions"*, linking this to sustainable development, and emphasising that this is necessary to *"realise the human rights of all and to achieve gender equality and the empowerment of all women and girls"*. The goals balance the three dimensions of sustainable development: economic, social, and environmental.

ROLE OF ICT IN SUSTAINABLE DEVELOPMENT

The Geneva Principles from 2003 specifically made reference to harnessing the potential of the ICT and the internet *"to promote the development goals of the Millennium Declaration"*, but also to achieve sustainable development and other development goals in building out an inclusive information society. The second phase of WSIS in 2005 produced the Tunis Agenda, intended as a plan to turn the Geneva Principles into actions. This was a seminal document that reconfirmed the central role of the internet and ICT in enabling the information society, laid the foundation for many of the issues in globalising internet governance, created the Internet Governance Forum (IGF) as a global multistakeholder forum to facilitate dialogues on related public policy issues, set up 11 action lines as part of an implementation plan for progress towards the information society, and requested a review of the implementation of the WSIS outcomes in 2015, including the IGF mandate (this is commonly referred to as the WSIS+10 review). In December 2015, the UN General Assembly convened a high-level meeting to review progress over the past ten years, identify gaps and challenges, and consider any future actions.

> **Internet penetration has gone from 6% of the world population in 2000 to 43% in 2015.**

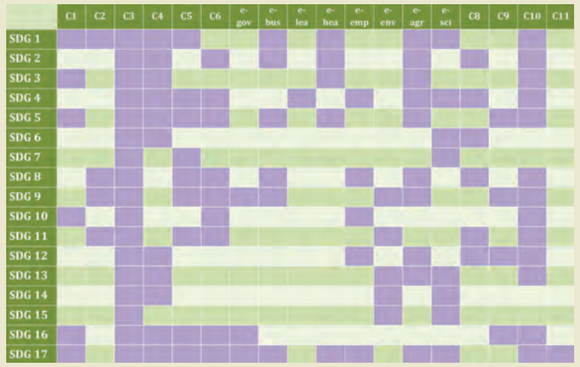
The review process officially began in June 2015, when ambassadors Janis Mazeiks, permanent representative of the Republic of Latvia to the UN, and Lana Nusseibeh, permanent representative of the United Arab Emirates to the UN, were named by the president of the UN General Assembly as the co-facilitators to lead the intergovernmental negotiation and create a preparatory process to produce the final outcome document. The co-facilitators created a process[9] to integrate input from all stakeholders within the constraints of the UN model. In addition to including informal stakeholder consultations into the process, they also personally participated in non-UN events to engage in dialogues with stakeholders, including a workshop hosted by the International Institute of Communications (IIC) and Microsoft, and the tenth Internet Governance Forum.

With both the 2030 Agenda and the WSIS+10 review occurring in the same year, there is growing consensus that the two discussions should be better aligned, due to heightened awareness of the role of ICT in both, and that the SDGs provide an important socioeconomic context for the development of the information society. While the 2030 Agenda does not focus on ICT, the role of

SDGS AND WSIS ACTION LINES

WSIS ACTION LINES

C1 The role of public governance authorities and all stakeholders in the promotion of ICTs for development
C2 Information and communication infrastructure: an essential foundation for the information society
C3 Access to information and knowledge
C4 Capacity building
C5 Building confidence and security in the use of ICTs
C6 Enabling environment
C7 ICT applications:
E-government
E-business
E-learning
E-health
E-employment
E-environment
E-agriculture
E-science
C8 Cultural diversity and identity, linguistic diversity and local content
C9 Media
C10 Ethical dimensions of the information society
C11 International and regional cooperation



How the SDGs map against the WSIS action lines

ICT in advancing the SDGs is recognised through mentions that technology and innovation are key in enabling a number of targets. The role of ICT in advancing all the goals is made more explicit by a mapping between the WSIS action lines and the SDGs presented at the WSIS Forum in May 2015.[10]

In October 2015, just after the SDGs were finalised and just as a preliminary draft of the outcome document became available from the co-facilitators, the IIC and Microsoft workshop took place, titled 'Dialogue on the Sustainable Development Goals and the WSIS Review', in Washington, DC.[11] Our objectives were to enable a dialogue on practical examples of multistakeholder initiatives in enabling the SDGs and the WSIS action lines, give examples of and challenges in sustainable economic development, and address cybersecurity capacity building as part of bridging the digital divide. Highlights from this dialogue are included below – these are intended to capture some of the topics mentioned throughout the day, and not to imply any consensus or policy recommendation among the participants on these issues.

In the opening session, Janis Mazeiks noted that the WSIS+10 review is an opportunity to take stock of the progress that has been made in enabling an inclusive information society, bridging digital divides, and be forward-looking in how the WSIS action lines can help to realise the SDGs. While participants acknowledged the tremendous progress that has been made in enabling more than 3 billion people to connect to the internet, much more needs to be done to create an enabling environment necessary to connect the remaining 4.1 billion. The challenges are not limited to building out adequate infrastructure with technologies that can provide universal and affordable access, but also include a broader discussion with economic, social, and political dimensions to create opportunities for 'meaningful inclusion'. Some of the main challenges discussed are as follows.

ADEQUATE INVESTMENT AND FUNDING – this was a recurring theme during discussion. There needs to be greater focus on financing challenges, and that top-down and bottom-up approaches need to be combined and tailored to address and prioritise local/regional investment needs. International organisations, private entities, local organisations and others all have a role to play. An enabling policy environment is also needed to incentivise continued private-sector investments – business models that are viable, replicable and scalable are essential to sustainable development.

LINKAGE BETWEEN LOCAL/REGIONAL DEVELOPMENT PLANS AND BROADER UN GOALS, AND PARTICIPATION OF LOCAL ORGANISATIONS – several participants emphasised the need for local/regional SDGs that would prioritise investment and flexible funding approaches tailored to regional needs, along with local/regional sharing of information on best practices and resources. Participation of local/regional organisations also enables development initiatives that are more sustainable as they address real needs, increasing the long-term viability of each project.

MULTISTAKEHOLDER PARTICIPATION – an "ecosystem of multistakeholders" was cited by some participants in a number of implementation examples, and that "it is essential for stakeholders to work together to address the challenges identified and to produce concrete results – it is not sufficient to issue a statement". However, it was noted that public-private partnerships often do not work due to lack of consideration of each other's perspectives and expectations, and that more efforts should be made to develop shared goals. The value of discussion across diverse sectors and inclusion of international organisations such as the OECD was also highlighted.

PROTECTING FREEDOM OF EXPRESSION AND HUMAN RIGHTS ONLINE – although ICT democratises access to information and fosters global exchanges of ideas, there are also increased opportunities for government control and repression of speech, leading to challenges in enabling an inclusive information society.

CLOSING THE GENDER GAP – gender inequality was emphasised as an issue that must be addressed by the WSIS review to achieve the SDGs. The need for more girls and women to participate in global and technical discussions, and "equal opportunities for leadership positions in technology" was also raised.

PARTICIPATION FROM DEVELOPING COUNTRIES – the lack of participation from developing countries in global discussions and technical discussions was noted by a number of participants.

BUILDING CAPACITY TO ENABLE QUALITY, LOCALISED CONTENT AND SERVICES – some participants noted the importance of addressing both the supply and demand side of connectivity, and that policy frameworks needed to address these together, not as distinct issues. Others noted the need for better information sharing, especially locally and regionally, on solutions implemented, success stories, and resources. Sustainable 'human trust networks', grassroots initiatives where citizens train and empower each other on infrastructure building and maintenance were suggested. The need for technology transfer to developing countries was also raised.

ADDRESSING CYBERSECURITY AND TRUST – some participants raised these as issues that would need to be addressed through multistakeholder partnerships, and that cybersecurity capacity training is essential to enable successful realisation of the SDGs.

GOVERNMENT COLLABORATION BEYOND 'SILOS' – this was raised several times during the workshop. Diverse government agencies, eg. finance, economics, health, education and security must be active participants in the national and global debates on sustainable development.

The discussion also noted the essential role of ICT, not just in realising the SDGs but also in measuring their progress – an element that was an acknowledged shortfall with the MDGs.

Participants also recognised that the IGF is a valuable platform for engagement on these and other issues, as exemplified by the growth of local, national, and regional IGFs. Even without negotiated outcomes, some participants noted concrete results that had been achieved from discussions that originated at the IGF.

Microsoft's Project Mawingu, which delivers low-cost broadband access to previously unserved locations near Nanyuki, Kenya, evolved from discussions at the 2011 IGF in Nairobi.[12] The project uses TV white spaces technology that enables low-cost yet long-range broadband connectivity, and solar panels to provide power for the base stations and for charging the devices that are used. By working together with national governments, local communities and other stakeholders, we were able to deploy a solution that addresses real needs, reinforcing the value of the multistakeholder approach, leading to long term sustainability of the initiative. This single trial has led to over 15 projects around the world, connecting 70 primary and secondary schools with a total of 36,000 students, and eight universities serving 176,000 students.

> **Gender inequality was emphasised as an issue that must be addressed by the WSIS review.**

A summary of the dialogue was submitted as an input to the WSIS +10 review process.[13] In December, negotiation concluded on the outcome document of the high-level meeting of the General Assembly on the review of the implementation of WSIS outcomes.[14] The document calls for *"close alignment between the WSIS process and the 2030 Agenda for Sustainable Development, highlighting ICT's crosscutting contribution to the SDGs and poverty eradication, and noting that access to ICTs has also become a development indicator and aspiration in and of itself"*. This sets a broader context for the development of the information society, and brings to the forefront additional social, economic, and cultural considerations.

Although the document recognises the tremendous progress that has been made in the past ten years, and the impact of ICT on economic, social and environmental betterment, many of the challenges brought up above were also acknowledged. These include the need to connect remaining people; bridging significant digital divides between and within countries, and between women and men; increasing participation from developing countries; developing financial mechanisms; protecting human rights online; and strengthening confidence and security in the use of ICTs with a renewed focus on capacity building.

Significant is the recognition of the value of multistakeholder cooperation in the WSIS process, and the value of the IGF was recognised through an extension of its mandate for another ten years.

The next overall review of the WSIS outcomes will be in 2025, which will be used as an input into the review process of the 2030 Agenda for Sustainable Development, encouraging further coordination between the two processes.

M-H CAROLYN NGUYEN *is director of technology policy at Microsoft and works to influence global policymaking on internet governance issues.* ***PAUL MITCHELL*** *is general manager, technology policy, at Microsoft.*

REFERENCES **1** McKinsey Global Institute (2011). The great transformer: The impact of the internet on economic growth and prosperity. **2** Edinburgh Group (2013). Growing the global economy through SMEs. **3** Boston Consulting Group (2013). Ahead of the curve: Lessons on technology and growth from small business leaders. **4** Beecham Research (2014). Towards smart farming: Agriculture embracing the IoT vision. **5** ITU (2003). Declaration of principles, building the information society: A global challenge in the new millennium, World Summit on the Information Society. **6** UN General Assembly (2000). United Nations Millennium Declaration. Resolution adopted by the General Assembly. 55/2. **7** UN (2015). The Millennium Development Goals Report. **8** UN General Assembly (2015). Transforming our world: the 2030 Agenda for Sustainable Development. Resolution adopted by the General Assembly on 25 September 2015. **9** WSIS+10 United Nations General Assembly high-level meeting, unpan3.un.org/wsis10 and also Preparatory Process Roadmap, unpan3.un.org/wsis10/roadmap **10** WSIS Forum (2015). WSIS-SDG Matrix: Linking WSIS Action Lines with Sustainable Development Goals. **11** IIC (2015). A dialogue on Sustainable Development Goals and the WSIS Review. bit.ly/1PvHgEt **12** Microsoft 4Afrika. White spaces project. bit.ly/1OG6D3i **13** IIC/Microsoft (2015). A dialogue on Sustainable Development Goals and the WSIS Review. Summary report. bit.ly/1Y1OZSK **14** UN General Assembly (2015). Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of WSIS outcomes. bit.ly/1NjXFbw

SEARCHING FOR THE CREATIVE ECONOMY

IAN HARGREAVES pieces together projects and evidence that are defining a crucial, technology driven sector of the economy

This article draws on my work as professor of digital economy at Cardiff University, especially with regard to four intersecting projects, some research-based, others policy-focused. The common thread in this work is the 'creative economy': its definition, scale, composition and potential, which readers may be surprised to learn is highly significant and a key consideration for technology and communications regulation and policy.

The argument can be summarised in this way: collaborative creativity, massively extended in scope by the availability of rich global, online media and data, increasingly supports two very desirable possibilities: added competitive edge based on more innovation in a substantially post-industrial world, and a simultaneous route to enhanced civic capacity, agile problem-solving and consequent social wellbeing.

These are compelling qualities in a world where 'big politics' increasingly struggles to persuade and 'big business' struggles to sustain trust. The success of the creative economy, however, does also rest on the avoidance or successful management of reputational issues on the part of governments and business if we are to avoid undermining trust in the internet.

A library and how books and print could be reimagined for the future. An exhibit at The Rooms showcase of REACT projects

PROJECT PORTFOLIO

Three of the projects in my portfolio occurred almost simultaneously. The first was a review of intellectual property and economic growth, initiated by the UK coalition government in the autumn of 2010, which I was asked to lead. At more or less the same time, I took leadership of a multi-centred, research council funded project in the large 'connected communities' workstream. This project bears the title: Media, Community and the Creative Citizen.[1]

Shortly afterwards, I signed up as co-director for a second, larger project funded by the Arts and Humanities Research Council. This involves the creation and running of four UK creative economy knowledge exchange hubs, in our case centred in Bristol. Its shortform name is REACT (Research and Enterprise in Arts and Creative Technologies).[2]

The fourth project arose indirectly from the first three and represented a year's collaboration with Nesta, a UK innovation charity, which led in 2013 to the publication of a manifesto for the creative economy.[3] It is also worth mentioning that the creative economy theme has been internationally extended through a close working relationship with the Brussels-based think tank, the Lisbon Council, where I have been involved in a number of Europe-focused projects and publications.

Let me step through each of these projects and publications in the order in which they have emerged or are emerging, before turning to a converged narrative arising from them.

The first in time sequence and the best known is the review of intellectual property (IP) issues, which turned out to focus chiefly on the highly contested subject of copyright, with some side-lights directed towards patent proliferation and the struggle to establish a unitary EU regime. The UK Prime Minister's exam question was to ask whether the UK's existing IP laws are inhibiting innovation and growth. My reply was that, unintentionally, they are and that, especially in copyright, they have failed to adapt to the reasonable expectations of consumers in a digital world.

The report, 'Digital Opportunity',[4] set out these arguments in detail in May 2013, and in August that year the government indicated its support for my conclusions, along with its intention to legislate in favour of a more extensive range of exceptions and limitations to copyright, along with some other reforms, with a view to pursuing these arguments in the context of a then promised review of the EU copyright framework.

The goal, as I see it, has been to ensure that IP law does not get in the way of the efficient development of markets and that the internet is broadly allowed to continue to evolve as a primary route to innovation, made possible by enhanced collaboration among creators of all kinds, from software engineers to musicians, via geographically expansive digital platforms, and often involving a pervasive blurring of boundaries between amateur and professional, audience and performer, user and maker.

The review involved intense political arguments and opposition in some cases from major international businesses. The process culminated in a three-year process of parliamentary scrutiny and broad approval.

Media, Community and the Creative Citizen, by contrast, had us working with tiny community groups: a husband and wife team who generate a brilliant 'hyperlocal' social media service in a Birmingham suburb; a network of young Bristol music makers and video artists; a community of London residents wishing to collaborate in resistance to a local development plan; a knot of entrepreneurs sharing office space wanting to connect better to their creative neighbourhood.

The academic team was drawn from five universities across a range of disciplines which included media, economics, performance, design, architecture, film, technology and cultural studies. Our strategic partners were also eclectic, including Ofcom and Nesta, on the one hand, and the South Blessed media network and a London community centre on the other. We started work early in 2011 and wound up in 2015. Our book, *The Creative Citizen Unbound: How social media and DIY culture contribute to democracy, communities and the creative economy;*[5] catches the flavour of our work. The book is due out in April this year.

REACT,[4] the third big project, was launched in 2012 and runs until early 2016. Its goal has been to generate surprising and promising partnerships between creative businesses and academics (chiefly from the five partner universities) to create brilliant ideas, products and services: a way of filling the R&D gap which limits the scope of many small companies.

> **"In five months Sandbox delivered as much as some publishers have done in five years."**

The 53 projects initiated have built on open innovation methodologies such as 'Ideas Labs' and 'Sandbox', developed in recent years at Bristol's Watershed digital media centre, which has been a pivotal player in the emergence of the city's creative and tech economy – home to major players such as Aardman Animation and Hewlett Packard. In four years, REACT has brokered and nurtured a network of over 800 individuals and organisations, working across themes including the internet of things, documentary, publishing, journalism, heritage, games, play and music.

George Walkley of publisher Hachette, asked to advise REACT, commented: "It is no exaggeration to say that in five months Sandbox has delivered as much as some mainstream publishers have done in five years." An end of programme REACT festival in November, called The Rooms (theroomsfestival.com) attracted over 5,500 visitors in two and a half days and a full assessment of its work will be available in the summer of 2016.

At Cardiff University, we are applying the lessons of REACT in the development of Creative Cardiff, a one-year-old research and engagement project which aims to connect and strengthen otherwise fragmented creative economy networks in the city region and thereby add momentum to the creative economy of South East Wales.

MANIFESTO FOR THE CREATIVE ECONOMY

The fourth project in my creative economy arsenal is Nesta's manifesto for the creative economy (2013), which arose directly from conversations with Nesta following the 'Digital Opportunity' report. I was drawn to working with Nesta when I became aware of Hasan Bakhshi's collaboration with scholars in Australia, which aimed to provide a method to

Contemplating a 'volume of circumstance' at The Rooms library exhibit

measure the creative economy, defined as comprising the economic outputs of everyone who does a creative job, whether in the specialised creative industries like music and publishing or beyond that, for example in the marketing and design operations of banks, manufacturers and retailers. For the UK, Nesta's analysis suggested the creative economy defined in this way accounted for 2.5 million jobs, amounting to 8% of the workforce. Expressed in terms of economic gross value added, this took the creative economy to almost 10% of the whole, making it larger than financial services: an eye-catching claim.

Our manifesto worked from this foundation of measurement to ask questions about the policy and operating landscape of the creative economy, pointing to the need to re-think approaches not only on measurement and intellectual property, but also on education, competition policy, R&D tax credits, regulation of the internet, investment in bodies like the BBC, local and regional industrial policy and digital infrastructures. This work builds on debates animated by the likes of Charles Landry ('creative cities') John Howkins ('creative economy') and Richard Florida ('creative class') and also connects strongly to the work of John Hartley, a leading UK cultural studies scholar now based in Australia, who collaborated with us on the creative citizenship project and is co-editor of our forthcoming book.

Hartley's own recent work has applied theories of evolution and complexity to the creative or DIY economy and society. With creativity defined as the production of newness in complex, adaptive systems Hartley reasons that change can come from anywhere in the system. It is not confined to what economics recognises as innovation because anyone can make a contribution, whether acting in the role of employee, entrepreneur or citizen.

Evolutionary approaches require attention to the potential creative and productive energy of everyone, not just professionally trained elites or commercially contracted experts. They involve, in principle, harnessing the productive power of everyone: a conclusion with potentially radical implications for the way we think about economic and social progress.

Taken together, these four pieces of work and their surrounding literature and practice, point us towards a powerful creative economy story which has, unsurprisingly, gathered ever greater political salience. UK Prime Minister David Cameron mentioned 'creativeness' as a key UK asset in the climax to his short victory speech on the steps of Downing Street in May. President Xi's recent state visit to London was accompanied by strong messages about China's recognition of the UK's admired strengths in finance, universities and creative businesses, as China continues its long march from a 'made in China' economy to a 'created in China' one. Check out the programmes of the world's business schools – creativity in management is an increasingly identified source of discussion.

THE CREATIVE CITIZEN

Meanwhile, we have also witnessed the emergence of the creative citizen – a figure who has emerged through a track of thinking which, as in business, notes the explosion of collaborative possibilities opened up by the internet. The resulting DIY culture has learned its methods from open source software and user-shaped design, resulting in the 'maker' movement and an economy of sharing, which has given rise to corporate giants such as Google, Facebook, Twitter, Amazon and Uber on the one hand, while also transforming day to day communicative, design and making procedures for individuals, communities and organisations.

Our research questions for this work asked, how does creative citizenship generate value for communities within a changing media landscape and how can this pursuit of value be intensified, propagated and sustained? We deployed a range of methods, from interviews and surveys to co-created media interventions, which we then evaluated. The communities in which we worked included centres of the new online community journalism (sometimes called 'hyperlocal' media) in Wales and Birmingham; a community office-sharing venture in Moseley; a music and video platform created by young people in Bristol; and various communities in London facing challenges which extended from planning and service development to engagement with younger clients.

> **The creative economy is almost 10% of the whole in the UK in terms of gross added value.**

What we found was that the principles of co-design and co-creation, familiar in the design and software world for many years, are increasingly understood and demanded in other areas of economic and civic collaboration. We identified specific value generation through innovation in terms of community media, community generated planning and development initiatives; creative expression, promotion and media distribution; and creative business collaboration. We also constantly encountered the limits of digital: the need to modify digital tools to meet the specific complexities and circumstance of individual places, and the balance to be negotiated between leadership and expertise on the one hand and inclusivity on the other.

These findings contribute to our understanding of digitally propelled growth in community-level collaborations, while also demonstrating that without the principle of co-creation or co-determination at their heart, they lack legitimacy, momentum and impact. Among many insights, we note that securing the big picture, in terms of available digital and mobile communications infrastructures, is only half the job. If the specifics of place and the particularities of any given community are not also heeded and harnessed, digital communications risk being associated with distance and even alienation, rather than connectivity and collaboration.

This is illustrated in the way that a community in North London, bonded by resistance to a proposed development scheme, worked with our research team to develop digital media techniques to generate an alternative planning vision, using (for example) computer generated images which include recognisable and credible local people rather than 'catwalk avatars'. Or consider the technique used to show how a purely online community media service can strengthen itself by 'reverse engineering' into limited use of a traditional newspaper format, or re-engineer its approach to using Facebook.

CREATIVE INSIGHTS

What, then, are the insights which emerge from these four projects and from the creative economy story? I will make six points.

1 The creative economy is a big story. It is an aspect of the shift from advanced economies based on things and prioritising investment in tangible assets to economies based on services and prioritising intangible assets. The evidence suggests that growth in this zone of the economy has already in the past decade been consistently stronger than in the economy as a whole. This is just the beginning. The creative economy deploys the energies and skills of everyone: it offers a potential category shift in terms of engaged human productivity because of its superior powers of motivation.

2 Creative economy jobs are, by definition, the jobs that robots can't do. Most other jobs are more vulnerable. Creative jobs are also, relatively speaking, attractive in terms of job satisfaction.

3 Creative economy work straddles the formal workplace and more personal zones, resulting in accelerated growth of self-employment/freelance contracting as opposed to fixed labour. This shift causes sensitive tensions in 'work-life balance' because creative work has a habit of not being readily confined to 9 to 5 working and to labour rights. Self-employed drivers working for the taxi-hailing service Uber do not enjoy the same levels of employment protection as contractually employed full-time drivers, but their terms of work may be better and the service they provide delivers highly disruptive competition for the taxi industry and is welcome to consumers. This is a classic example of disruption through innovation.

4 The general wellbeing and growth of the internet is fundamental to the continued growth of the creative economy. Today, the creative economy has many enemies, most obviously those governments which restrict access and run penal supervisory regimes, thereby contributing to fragmentation. The internet's enemies, however, also include communications and media businesses intent on protecting at all costs existing business models, and democratic governments fearing loss of control. Competition authorities have an important role to play in ensuring that markets remain open to challenger companies. They also have an important role in accurately identifying risks of abuse of market power from large internet platform companies, while being astute enough to identify arguments based on self-interest from established business players bent on protection. Those responsible for security have a responsibility to negotiate police and surveillance powers in a way that is sensitive to issues of citizen trust. Long-running issues such as net neutrality will continue to run.

> **The wellbeing and growth of the internet is fundamental to the creative economy.**

5 The creative citizen is an important figure. She requires more and more access to cleaner and open public data to make a creative contribution to the development of her locality and she certainly will not tolerate a rolling back of freedom of information rights. Increasingly, creative citizens will find themselves co-creating services previously organised to a more industrial model – examples include libraries, childcare, care of older people, gardening, news services, health and sports facilities. The task of re-organising institutional and voting procedures suitable for an age of creative citizenship has barely begun.

6 Intellectual property rights and business models will continue to evolve in a direction which supports readier legal access to use.

IAN HARGREAVES *is professor of digital economy at Cardiff University, UK. He has been on the board of UK regulator, Ofcom, and also been in a regulatory and communications role in the UK airport industry. He was also in journalism, at the FT, the BBC and the Independent.*

REFERENCES **1** Media, Community and the Creative Citizen. creativecitizens.co.uk **2** REACT creative economy hub. react-hub.org.uk **3** Bakhshi H, Hargreaves I, Mateos-Garcia J (2013). A Manifesto for the Creative Economy. Nesta. bit.ly/18w2RTx **4** Hargreaves I (2011). Digital Opportunity: A review of intellectual property and growth. Department for Business, Innovation and Skills. bit.ly/1kTpPAQ **5** Hargreaves I and Hartley J (eds) (2016). The Creative Citizen Unbound: How social media and DIY culture contribute to democracy, communities and the creative economy. Policy Press.

SPECTRUM ANALYSER

A comprehensive book on spectrum policy is reviewed by **MARC BEISHON**. The key theme is liberalisation and its limitations and future

Spectrum is a subject that hardly sets the pulse racing. Its technicalities can be yawn inducing and the various strategies for allocating it to operators are enlivened only by the often eye-watering sums that they have to pay to buy capacity in auctions, which can be entertaining. Despite thousands of the world's policymakers and technical experts descending on Geneva at the ITU's latest World Radiocommunication Conference (WRC-15), where vital decisions about the economy's underpinning communications get hammered out, there's been little mention in national media.

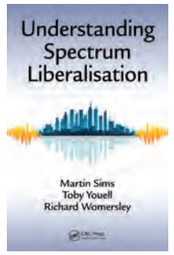
So it's a tribute to the authors of *Understanding Spectrum Liberalisation* that they have managed to turn this potentially very dry topic into a lively narrative that they feel achieves two main aims – to provide an introduction to spectrum policy to those new to the subject and who may well be 'puzzling' over it, and an interpretation of current developments for those already in the field. Further, by tracing the history of spectrum policy, the story parallels the way regulation in general has developed, and so makes a good and ongoing case study in regulatory policy.

STORY OF LIBERALISATION

The basic story is straightforward, and explains the title of the book. Up until about 20 years ago, spectrum was simply allocated by government agencies in the developed world under a command and control method to operators, mostly for no charge. Liberalisation, which of course has also opened up other markets in telecoms, then became the norm, recognising that operators should pay for using an increasingly valuable asset (the much-used comparison is with paying for different types of land by its value).

The liberalisers, the authors say, visualised a market where frequencies can be bought and sold, including under technology neutral licences, and this took hold in the US and then the UK and European Union, especially for mobile spectrum, and those eye-catching auctions became the norm. But by 2009 the story becomes much more interesting at a policy level, because it had become apparent that there were limits to liberalisation as demand for mobile spectrum soared. Operators couldn't practically buy spectrum from broadcasters or the public sector, and regulators didn't tell mobile operators to buy in the market, instead trying to reallocate spectrum at national level and at international level through the ITU.

"It was a tacit admission either that liberalisation alone could not deliver, or that it was inherently a slow process, unfit for its biggest challenge so far," say the authors. Spectrum trading in the secondary market, which was thought to be a plank of liberalisation, has also not taken off in the EU (although has been more successful in the US and Australia). Further, liberalisation does not lend itself to the growing interest in wholesale mobile networks, such as in Mexico, which could turn the sector back into one more like fixed networks, with one shared infrastructure, and indeed various forms of sharing is now very much on the agenda as part of a third phase of spectrum management, which the authors argue is now taking hold.



Understanding Spectrum Liberalisation, by Martin Sims, Toby Youell and Richard Womersley, is published by CRC Press. More details at: crcpress.com Martin Sims founded PolicyTracker, the spectrum management newsletter

BACK IN TIME

Delving deeper into the past, a chapter describes how commercialising spectrum licensing took place and how the 'father' of liberalisation, Ronald Coase, put the case for treating spectrum like any other commercial input (his seminal paper was published as long ago as 1959). The command and control system can have advantages, such as with the EU's GSM directive of 1987 that mandated certain bands and technology for mobile so there was no interference between countries, and this proved successful but was in the long run inflexible when operators wanted to update the technology. Other mandates failed quickly, such as the MAC satellite and ERMES paging systems.

Regulators shouldn't be picking winners and wasting public money, is the view, but the authors say that the GSM directive worked to put Europe ahead for some time because it applied to a new market with great latent demand, and not to established industries such as satellite. Licences can then be amended to make them technology neutral.

The commercial, liberalisation phase, while characterised by the massive auction windfalls for governments, also has had sharing in unlicensed bands, such as with the spectacular rise of WiFi, where there are low barriers to entry, and other technologies such as white spaces also have a 'commons' model. Licensing is only usually necessary to prevent interference.

Jumping ahead to the conclusions, it is said that liberalisation has not 'had its day' or been a failure, but has been disappointing in not being applied to broadcasting, not providing enough mobile spectrum and not stimulating much trading outside the US. (And command and control is still more than sufficient to meet the needs of many developing countries, where mobile broadband is not widespread and utilities are often government owned.)

The authors add: *"What has emerged from the attempts to apply a liberalised approach to the airwaves are the constraints under which any spectrum market must operate. There are the long time-lags associated with international coordination and the development of chipsets, the political pressures generated by the social importance of services such as broadcasting and defence, and the oligopolistic nature of the mobile market... The new emphasis on sharing is an attempt to overcome some of those limitations..."*

LIBERALISATION IN ACTION

The bulk of the book fills in the detail. Newbies will be pleased with the chapter that explains what spectrum is and how radio waves work. Then the book steps rapidly through the topics that show 'liberalisation in action'. First is the spectrum auction, which has become the default assignment mechanism (although many countries which hold them would stop short of trading or pricing public sector spectrum). Then there's a valuable chapter on how licensing is done – this does get somewhat technical, as licences need to ensure spectrum does not interfere with others, and it is more complicated with technology neutral approaches that give more flexibility, and the authors note there are limits to liberalising licensing.

The following all get a dedicated chapter:

- The public sector, where incentive pricing, or incentive to vacate, is discussed in detail (and where the UK is a leading player)
- Broadcasting (where digital terrestrial TV, DTT, is thriving in some markets despite its inferiority in technical terms to cable and satellite, and despite younger people watching less conventional TV, and where attempts to use market mechanisms have come to almost nothing)
- Satellite (where command and control mostly rules)
- Ultra-wide band (used for underlay networks but hard to implement)
- WiFi and the spectrum commons (unlicensed spectrum here is a great success but so too are standards and technology that make it work. There's a view that policymakers should pay more attention to the innovation that such spectrum can provide)
- White spaces (which may be a transient opportunity as incumbents may fill the gaps).

In the next section, the authors get to the heart of the issues. Is there really a capacity crunch? (A broadcaster looked at this closely in the last issue of *Intermedia* with the answer 'no'.) In the book, the authors largely agree but say there is undoubted, growing demand for mobile broadband – and (tongue in cheek) if so, can't the liberalisers and therefore the market decide? They add more on the obstacles to liberalisation, such as the need to address huge markets at global scale, the separation of handset makers from operators, and the political power of broadcasters, so it is mainly command and control that will transfer spectrum.

Another question: why does trading have such patchy success? Mobile markets are often oligopolistic and national, but where trading has been successful, in the US, networks are regional,

Delegates stand at a plenary session at WRC-15 on global flight tracking. The ITU has acted quickly on assigning spectrum for tracking after aircraft disasters. The book has an appendix on how the ITU works

and the US has also been able to trade in spectrum for declining technologies such as WiMax and mobile TV. Trading has done relatively well in lower value market sectors, it is noted.

Moving on, there is discussion of sharing and wholesale networks, and whether they are good or bad for competition and costs, and certainly moves to wholesale will mean changes to spectrum models. One of the more lengthy chapters deals with political issues that influence spectrum, and there is comment that national and international political constraints can exert a negative influence on spectrum policy reform. And criticism of auctions for allocating spectrum seems to be gathering pace, but "many more hits will be required to wrench the auction treasure chest from the grip of government ministers".

A TOOLBOX FOR THE FUTURE

In the final part of the book, the authors look for the right 'metaphor' for the changes ahead – not so much a paradigm shift but the use of a humble toolbox, they say. What's in the toolbox? In summary:

- Licensed shared access – where an incumbent user allows other users to share its spectrum. It has appeal as a speedy way around trading limitations but won't provide long-term, high-quality service.
- Cognitive radio – this senses when a frequency is used and only transmit when unoccupied and is used in 5 GHz WiFi (shared with radar), for example. Dynamic spectrum access (DSA), which uses databases to determine location rather than sensing, is becoming of more interest, the authors say, but progress is slow. A famous paper by Eli Noam in 1998 saying spectrum will be a true, real time, open market thanks to techniques in cognitive radio is though a vision that the authors say is a long way off but is a direction of travel that could eventually remove the obstacles to spectrum markets.
- Future technologies – 5G is the key one, and there are issues beyond spectrum such as the growth of small cells, but sharing and the use of higher frequencies (including above the radio bands) are likely to be important. Here the authors prefer not to speculate too much.

Overall, *Understanding Spectrum Liberalisation* is written in clear English, in short chapters and with minimal technical obscurity. What the book does well is cover almost everything likely to be important in the next five years or so.

Balancing act: a concept from the European Commission on the digital single market

CONVERGING ON DIGITAL

Taking the current European reform as model, **MONICA ARIÑO** puts forward three key pillars for regulatory framework reform in pursuit of convergence

Policymakers and communications regulators around the world continue to search for the most suitable regulatory approach for the communications industry as convergence takes hold. The European Commission published a green paper on the regulatory implications of convergence as far back as 1997,[1] and the issue has been, in one form or another, the topic of innumerable policy debates, conferences, consultancy reports, strategy papers and academic research for the best part of two decades.

It remains an ongoing challenge; convergence takes many different forms, it evolves, and businesses and consumers take advantage of it in unpredictable and varied ways, making yesterday's difficulties irrelevant tomorrow. Convergence can mean access to the same service over multiple networks. It can also mean the progressive amalgamation of fixed and mobile network architectures, the provision of combined services (voice, broadband and TV) as a single retail offer and the development of over the top (OTT) services, which are increasingly substitutes for traditional communications services.

These developments can challenge the delivery of wider public policy objectives such as universal broadband availability or the promotion of public interest content on connected devices. They also question the validity of current regulatory approaches to network access regulation (for example, what is the correct market definition, who is dominant, what is the right cost allocation and approach to pricing); consumer policy (for example, how to support effective switching processes for bundles); and audience protection (for example, how best to protect audiences from harm in an online environment).

Over the next five years, European policymakers will be considering these questions in the context of some of the legislative reforms announced under the umbrella of the Commission's digital single market (DSM) strategy[2] – a vision to create a market where everyone is able to purchase digital goods and access online services regardless of their country of origin. Two key legislative reforms will be the review of the frameworks governing electronic communications networks and services, and the provision of audiovisual media services (ie. TV and video on demand), with legislative proposals expected in 2016.

There is significant momentum around these, and the rest of the anticipated DSM proposals. Most stakeholders are contributing to the debate and consultations. There is a sense of urgency in Brussels, stemming from the perception that Europe is falling behind other regions, in particular the US and Asia. This perception might reflect a simplistic view of what success looks like and what comparisons are meaningful, but it carries political weight. In some areas, barriers to online trade seem indeed unjustified, and greater harmonisation of rules would benefit business and consumers alike.

> **There is a sense of urgency in Brussels as the perception is that Europe is falling behind.**

While anti-US sentiment risks clouding the debate, it is right that Europe should not be complacent, particularly given the risk of delays from its long and convoluted legislative processes. Regulatory reform to respond to (and prepare for further) convergence is needed to facilitate a truly digital economy.[3]

IMPROVEMENTS, RATHER THAN AN OVERHAUL

Reform does not necessarily mean a complete overhaul. In fact, despite some talk from Brussels about 'wholesale reforms', no revolutionary ideas have been presented to date. The fact is the existing European regulatory frameworks have worked well. They identify the right consumer and citizen outcomes and establish sound regulatory principles.

But there is room for improvement. This could include a relatively straightforward simplification of some of the rules on broadcast advertising regulation, or streamlining the process of market analysis (eg. potentially greater national discretion on the frequency of market reviews).

We could improve the suite of available access remedies, strengthen consumer protection and reconsider the rationale for universal service obligations and their scope and funding. Furthermore, as new converged business models become increasingly pervasive, regulators will need to be satisfied that they have appropriate powers to address competition concerns that might arise, including the appearance of new gatekeepers, particularly online.

One urgent area for attention is the extent to which regulators need and can address the consequences of oligopoly scenarios where no single firm is dominant. These scenarios might arise through market evolution or consolidation (eg. mergers in the mobile sector). In such situations, firms might, unilaterally or collectively, behave less aggressively, which could lead to poor consumer outcomes. This concern is already

recognised in the EU merger guidelines[4] that contemplate the risk that concentration of a market can result in a lessening of competition. A debate on whether and under what conditions intervention might be necessary has already started in Europe, with a report published by the Body of European Regulators for Electronic Communications (BEREC) in December.[5]

While not all oligopolies will cause concern, and the threshold for intervention should be high enough so as not to stifle competition or deter investment, it is appropriate and timely to consider this question as part of the Commission's review.

PILLARS OF THE REGULATORY ECOSYSTEM

In the above context, I would like to reflect on what I believe are three key components of a successful regulatory framework:

- A focus on **outcomes** backed up by regulatory powers, rather than detailed rules, preserving sufficient discretion and flexibility for regulators on when and how to intervene
- Related to this, the need for greater **coordination** among European regulators to maintain a consistent approach across Europe that can support the ambition of the digital single market
- Strengthened **independence** of regulatory authorities.

This article addresses each of these components.

FOCUS ON OUTCOMES, NOT OVER-ENGINEERED RULES

The newly adopted European rules on net neutrality are a good example of the benefits of a principles-based approach.

Since 2009, regulators were empowered (but not required) to intervene in quality of service on public networks, as and when necessary. In 2013, the Commission proposed to move away from this approach towards one of micro-regulation, seeking to define which specific commercial and technical practices network operators were permitted to engage in. For instance, it singled out and tried to restrict the provision of 'specialised services' (one but by no means the only way to prioritise traffic); it also attempted to constrain by law the technical interaction between such specialised (wholesale) services and internet access (retail) services.

Finally, it significantly limited the circumstances in which ISPs could legitimately manage traffic, failing to recognise that network congestion is neither temporary nor exceptional, and that users might legitimately request it (eg. to block spam or filter inappropriate content).

The Commission's intention was to pre-empt regulatory fragmentation across Europe, following the adoption of national net neutrality rules in the Netherlands and Slovenia, but in doing so it sought to capture in a legally binding text what are, essentially, engineering practices. The practicality of enforcing such rules seemed rather an afterthought. Stakeholders (including industry players across the value chain) and regulators alike expressed concern that the rules were insufficiently flexible and would quickly become obsolete. The CEO of UK regulator, Ofcom, said at the time:[6]

"I fear that over-prescriptive and detailed legislation may deliver the opposite of the intended effect; not more certainty but less, not the exercise of balanced objective judgement but the pursuit of skewed, self-interested litigation. The internet is an enormously complex and dynamic ecosystem, where the law of unintended consequences looms very large indeed". (Ed Richards, Ofcom chief executive until December 2014).

Instead, Ofcom and others favoured a framework based on clearly defined policy outcomes, eg. the need to prevent degradation in the quality of internet access services, which would serve as triggers and principles for intervention common to all. This would be complemented by enhanced powers for regulators to monitor quality and to intervene when necessary, such as through the imposition of minimum quality of service or other measures – to be defined by the regulators themselves, thus leaving national regulators the flexibility to respond according to the specifics of their national markets, and avoiding pre-emptive (micro-) regulation.

An approach along these lines was eventually agreed and is broadly consistent with the open internet order adopted in the US by the Federal Communications Commission in March 2015, though the FCC's discretion appears to be wider.

This principles-based model would work in other areas too, for example to simplify European broadcasting advertising rules. Rather than prescribing the detail of how programmes can be sponsored or products placed, the rules could focus instead on the relevant consumer protection outcomes (eg. ensuring vulnerable audiences are protected from harm, that the advertising and the editorial content is clearly distinct, that viewers know when they are being sold to, and that the editorial independence of the programme is preserved).

Regulators could then be empowered to intervene if these principles were under threat. Such an approach would better allow for innovative advertising techniques to develop, as increased consumption of IP-delivered audiovisual content (through connected TVs, tablets and other mobile devices) allows broadcasters to experiment with more sophisticated forms of advertising. If Europe is to maintain a competitive and thriving audiovisual industry, such opportunities for innovation should be supported and further encouraged.

> **Ofcom and others favoured a framework based on clearly defined policy outcomes.**

THE NEED FOR REGULATORY COORDINATION

A model based on outcomes rather than detailed behavioural rules presents some risks. It could increase regulatory fragmentation across Europe, seemingly undermining the goals of the digital single market. It could also provide opportunities for regulatory arbitrage or forum shopping in areas where European companies operate under a country of origin principle (such as broadcasting, e-commerce and data protection). This principle requires companies to comply only with the rules of the country in which they are established; some may choose their base to circumvent higher protection standards elsewhere.

The Commission is right to tackle the differentiated treatment of digital goods and services when such differentiation is discriminatory (eg. charging different prices for otherwise identical online transactions depending purely on the geographic location of the buyer) and to incentivise further cross-border commerce, for example easing administrative and regulatory barriers.

However, in some cases, regulatory differences between jurisdictions are legitimate and will inevitably remain. For example, in the audiovisual sector, the European framework only sets out minimum content standards for broadcast services because it recognises that there are enduring cultural specificities (countries can and have gone beyond this in their national legislation).

In telecoms, despite harmonisation at EU level, national markets maintain different characteristics – not least as a result of network topology and services that are mainly local in nature. And historic differences in the way countries use spectrum mean that it is impractical to move to a world in which all countries use all frequencies in the same ways. As a result, differences in implementation exist and will remain.

The scope and benefits of harmonisation are therefore more limited in practice than the Brussels rhetoric might imply. In fact, as convergence continues apace, detailed rules will fail to keep up with what is not only a highly complex area, but one that moves very rapidly. If Europe wants a regulatory framework that can sustain the test of time, it needs to accept the reality and confines of the single market aspiration. The focus on (harmonised) outcomes should be accompanied by a greater effort to deliver consistency of national implementation across jurisdictions by the national regulators themselves.

Such cooperation is no longer the luxury of those with time or resources. In some areas, cross-country coordination mechanisms are already enshrined in European law. For example, BEREC operates a formal process of peer review of its members' decisions on market analysis (market definition, identification of significant market power and design of remedies), in cases where the Commission has expressed concerns about the course of action proposed by the national regulator. Individual members are required to take utmost account of the opinion of their peers – and justify when they depart from it.

Such a mechanism could also be considered as a way to enhance the operation of the Radio Spectrum Policy Group (RSPG), which advises the Commission and which at the moment limits itself to the compilation of best practice reports. On the content front, it should be possible for the European Regulators Group for Audiovisual Media Services (ERGA, the new regulatory network for broadcasting regulators) to provide assistance and guidance on the implementation of applicable rules.

The time needed for discussions and preparation of reports is significant, and the difficulties in reaching consensus should not be underestimated. Nevertheless, such networks remain the best mechanism to increase the consistency of approaches across different jurisdictions to deal with similar problems and provide the right complement (and sometimes the necessary checks and balances) to the Commission's harmonisation efforts.

INDEPENDENCE IN STATUTE, AND BEYOND

The digital single market strategy recognises the need to 'enhance' the role of European bodies where member states' authorities are represented, such as BEREC or the RSPG, but provides no detail of what this may mean in practice. Beyond that, it hardly explores issues of regulatory governance, except for a timid reference (in the supporting working document, not in the main strategy), to the need to review the independence of media regulators in Europe.

> **Regulatory independence matters for predictability and to avoid politics.**

This is an area where clear and robust principles could usefully be set out at European level – and in fact the European framework already establishes explicit regulatory independence requirements for some sectors. For example, in telecoms, the Framework Directive[7] requires member states to guarantee the independence of the national regulatory authority (NRA), ensuring they do not seek or take instructions from any other body and limiting the grounds for dismissal of the head. It requires NRAs to have separate budgets that should be published.

Regulatory independence matters: first and foremost, because it provides regulatory predictability and supports investor confidence, but also because it avoids the risk of decisions being taken (or being perceived to be taken) for political purposes. It requires:

- Regulators' governance arrangements to be free from political influence (including the provision of the necessary safeguards in the processes for the appointment/removal of their heads)
- Regulators to have a transparent process of decision-making protected from political or industry interference, accompanied by sufficient investigative and sanction powers, security of funding and budgetary autonomy
- Regulators to have clear public accountability (for example, through parliamentary committees and courts).

In the audiovisual sector, there is no independence requirement at EU level. When the relevant European directive[8] was last reviewed, European governments rejected the Commission and Parliament proposal, resulting in a less than ideal compromise of an indirect and general reference on the need for 'independent'

regulatory authorities to cooperate (thereby assuming they are independent – which is not necessarily the case, and certainly not to the degree that would be desirable).

Since the directive was adopted, the question of independence of broadcasting regulators has gained an increasing profile in Europe and been the subject of a Commission study looking at best practices,[9] several regulators' meetings,[10] academic research, and a formal Commission consultation in 2013. This was also the subject of the first public statement by ERGA, which specifically asked the Commission, as the initiator of legislation, to identify "common characteristics that any independent regulator in our sector should be equipped with".[11]

It is very likely that the Commission will resurrect the proposal this time around. It remains to be seen whether political consensus can be achieved – and what this will mean in practice, given both the power of the media in opinion forming, and the risk of political influence. But to fail to make progress would be deeply unfortunate, given the essential role the media play in enabling healthy democracies. A clear political backing for regulatory independence, enshrined in European law, would have a strong impact both within and outside European Union borders.

Normative recognition is, however, only the first step. Regardless of how robust the statutory framework is, independence remains an intangible concept – one which is difficult to measure and one which needs to be fought for every day. This is why, as has been widely documented, a 'culture of independence' and transparency are critical if the system is to function well.[12]

Different European countries have different legal traditions. No amount of rules can replace the need for a value system that recognises and respects the regulator's independent function. Therefore, we will need complementary supporting actions, such as increased coordination between the EU and others (such as the Council of Europe and the Organisation for Security and Cooperation in Europe), on concrete actions promoting a culture of independence in practice[13] and the informal exchange of (good and bad) experiences between regulators.[14]

The challenge is handling what are regular, inevitable and indeed desirable interactions with government without fear or favour. This issue becomes more important as the lines between policy and regulation continue to blur, and as the complexity of the sector requires an ever greater degree of technical input into policy decisions.

POLICY AND REGULATION: WALKING THE LINE

Given the importance of regulatory independence, some might ask whether it is appropriate for regulators to depart from purely technical and enforcement work into the realm of policymaking, including making choices about the best way to achieve specific political objectives. We have seen this in the UK, and it is an aspect of the sector review launched by Australia's Department of Communications. At European level, and as sector-based regulatory networks grow stronger, we can expect them to play an increasingly active role in advising on policy development, which will keep this issue in the spotlight.

The fact is, the separation of policy and regulation can be somewhat artificial. While legislative frameworks can draw a clear delineation between the functions of government, regulators and competition authorities, in practice the line between policymaking and regulation is, and will continue to be, blurred. The complexity of the sector means governments might turn to the regulator for advice.

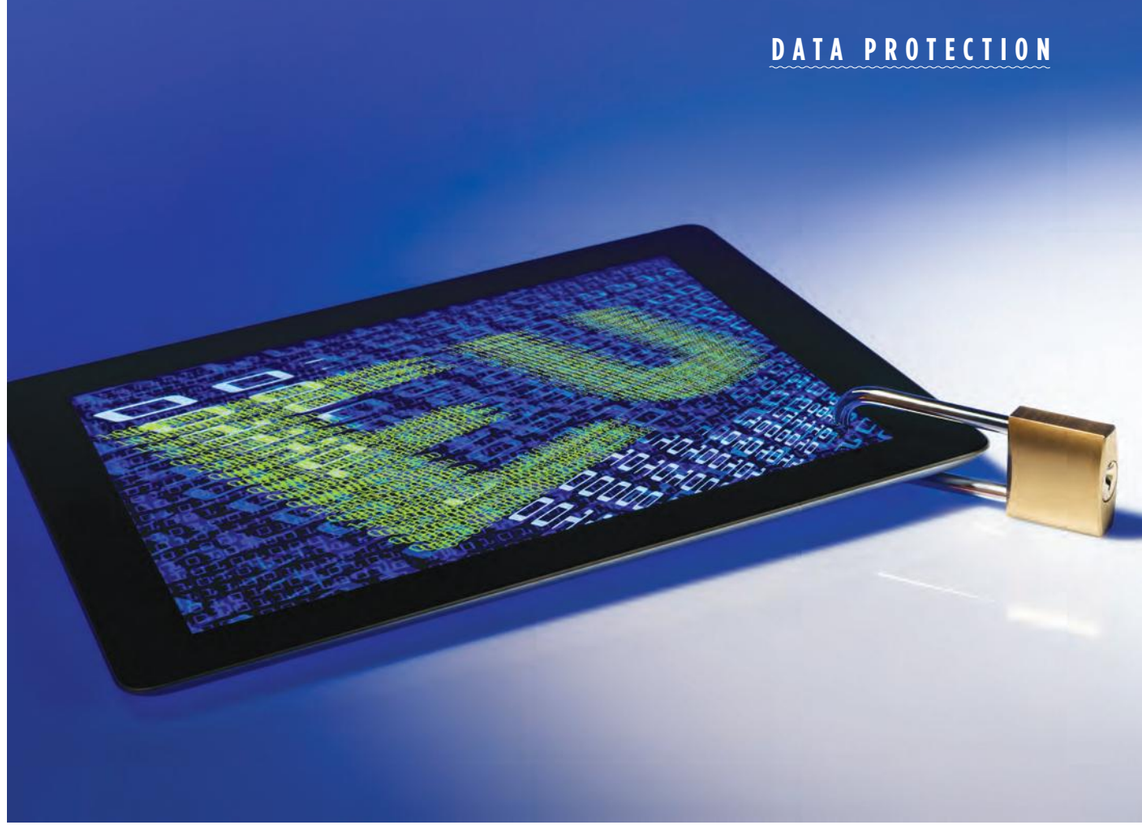
> **We can expect regulators to play a more active role in advising on policy development.**

In the past Ofcom has contributed to a number of public policy debates at the request of the UK government, such as on broadband universal service, public service broadcasting and media plurality. In practice, what is needed is an open dialogue between regulator and government in the pursuit of public policy goals.

If the regulatory framework evolves, as advocated above, towards one that is based on outcomes and principles, rather than detailed rules, coupled with greater flexibility and tools for regulators to intervene, such interaction will increase in some areas. Regulators will need greater flexibility at the point of implementation, and may have to make 'policy' choices alone, or as part of a wider regulatory network. It is important for regulators to build trust in their relationships with government and consult widely to ensure that decisions continue to be based on evidence and are in line with public policy goals. Ofcom has found that productive interaction with government is essential to secure independence in practice.

MONICA ARIÑO *is international director at UK regulator, Ofcom, and an IIC board member. The views in this article are those of the author and do not represent Ofcom's position.* *Thanks to Mark Caines and Camilla Bustani for comments on drafts.*

REFERENCES **1** European Commission (1997). Green paper on the convergence of the telecommunications, media and information technology sectors, and the implications for regulation. bit.ly/10h8zkd **2** Details of the DSM strategy are at bit.ly/1JRVhJl **3** Ofcom is conducting a strategic review of the UK communications sector, the outcomes of which will feed into European discussions. bit.ly/1LI0Xu **4** Guidelines on the assessment of horizontal mergers under the Council regulation on the control of concentrations between undertakings (2004). Official Journal of the European Union. bit.ly/1M8CNDh **5** BEREC (2015). Oligopoly analysis and regulation. bit.ly/1NZanks **6** Speech at IIC meeting, March 2014, Washington DC. **7** Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009. **8** Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the provision of audiovisual media services (Audiovisual Media Services Directive). **9** Hans Bredow Institute for Media Research et al. (eds) (2011). INDIREG. Indicators for independence and efficient functioning of audiovisual media services regulatory bodies for the purpose of enforcing the rules in the AVMS Directive. Study conducted on behalf of the European Commission. Final report. bit.ly/1IzrlCQ **10** The European Platform of Regulatory Authorities (EPRA) has discussed this issue at its meetings in Prague (2007), Tbilisi (2014) and Budva (2014). **11** ERGA (2014). Statement on the independence of NRAs in the audiovisual sector. bit.ly/1g4eofw **12** EPRA (2007). The independence of regulatory authorities. bit.ly/1XgFnig **13** A good example is the recent implementation of the INDIREG ranking tool in Albania as a result of CoE/EU cooperation. See: bit.ly/1R76ZI0 **14** EPRA has a long tradition in this regard. See: bit.ly/1ParqPw



FINAL COUNTDOWN TO DATA PROTECTION

A long overdue reform in European data protection law has finally taken shape, as **MAURIZIO MENSI** explains

Data protection is undergoing a significant change across the European Union. A major review of the current European data protection framework was initiated in 2009 to further harmonise data protection legislation throughout Europe, as its current fragmentation is overly burdensome to market operators with cross-border activity. So the EU is in need of a new deal on data protection able to facilitate data flows, both in the EU and with its trading partners, and to guarantee the rights of freedom to individuals.

For this purpose, the European Commission's proposals for a comprehensive reform of the EU's 1995 Data Protection Directive[1] aim to strengthen privacy rights and boost Europe's digital economy by modernising the principles enshrined in the 1995 directive, bringing them into the digital age. The Commission's 25 January 2012 proposals include a policy communication setting out the Commission's objectives[2] and two legislative measures: a regulation setting out a general EU framework for data protection (GDPR), and a

directive on protecting personal data processed for the purpose of prevention, detection, investigation or prosecution of criminal offences and related judicial activities (EU Data Protection Directive).

Following the review carried out by the committees of the Parliament, on 12 March 2014 the European Parliament passed the compromise texts of the GDPR together with the police and criminal justice data protection directive. This rather swift approval was significantly influenced by 'Datagate', the mass interceptions scandal of the US National Security Agency's Prism programme, which emerged from revelations of analyst Edward Snowden in June 2013, relating to the collection of data on millions of phone users.

On 15 June 2015, ministers representing the member states at the EU Justice and Home Affairs Council agreed on a 'general approach' to the proposed GDPR.[3] The adoption of the approach carried with it authority for the presidency to lead negotiations with the Commission and the Parliament, setting the stage for achieving a compromise text to be adopted as the final regulation. The tri-party discussions kicked off in June with a view to adopting a text by the end of the year. The debate on the EU Data Protection Directive as well as GDPR by the Parliament and Council have been carried out in tandem, as the institutions have agreed on a flexible roadmap.

Finally, on 15 December 2015, representatives from the European Commission, the European Parliament, and member states reached an informal political agreement on the data protection package.[4]

COMPROMISE RESOLVING INSTITUTIONAL CONFLICTS

The GDPR sets out proportionate action and fines ranging from a warning or reprimand up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, and sanctions are to be discretionary. A number of factors will be considered in setting the level of fines, including duration and gravity of the data breach, negligence and intention, and impact on users. Due regard should however be given to *"actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor"* (recital 118b).

The GDPR will establish a homogeneous set of rules on data protection in force across the EU uniformly. Recital 21 states: *"The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects as far as their behaviour takes places within the European Union."*

It follows that GDPR jurisdiction will extend outside the EU, as it applies to the offering of goods and services to, or the monitoring of, data subjects in the EU. Non-EU controllers that satisfy this jurisdictional connection will need to appoint an EU representative, "unless the processing it carries out is occasional" and "unlikely to result in a risk for the rights and freedoms" of individuals (recital 63).

Note that during negotiations, the Council of Ministers made important changes to the Commission's text and the present general approach differs markedly from the text adopted by the Commission in January 2012, as well as from the amendments to the Commission's text proposed by the European Parliament in its first reading in March 2014. A number of issues arise from disaccord among the institutions involved.

First, the GDPR brings forward a 'one-stop shop' for market operators and users, who will only have to deal with a single supervisory authority, simplifying cross-border operations and business. This apparatus is meant to guarantee consistency in the interpretation and enforcement of the regulation across the EU by supervisory authorities, significantly reducing costs and providing greater legal certainty in enforcement cases involving multiple data protection authorities. Nevertheless, the 'one-stop shop' provisions have been diluted by the Council, as in multi-jurisdictional breaches, where relevant supervisory authorities will need to be consulted and will be able to challenge the lead authority's assessment.

Moreover, in cases involving only one jurisdiction, the supervisory authority in that jurisdiction will preside over the matter, rather than the lead authority, as established by the 'one-stop shop' principle. This also implies a clarification of the competence of the supervisory authorities and the designation of a lead authority in cases of transnational processing. Data protection authorities should be ready to exercise their roles when the regulation enters into force, and determine proportionate and appropriate remedies and administrative sanctions on the basis of all relevant circumstances.

> **The GDPR brings forward a 'one-stop shop' for market operators and users.**

Second, the GDPR mandates prior consent to be agreed before collecting and processing users' data. Data subjects must always be informed of their right to withdraw consent to the processing of their personal data. Also, "the data subject should be informed about the existence of profiling, and the consequences of such profiling" (recital 48). 'Profiling' is defined as any form of automated processing of personal data evaluating personal aspects as long as it produces legal effects concerning the data subject. The text approved on 15 December 2015 has defined more narrowly the nature of the informed consent, defining the boundaries of the quality of consent that data controllers must obtain to provide a legal basis for data processing, as it bears the adjective 'explicit'. On the contrary, the previous Council's draft required that consent "should be given unambiguously", which would have given data controllers more leeway in the subsequent use of data that was not contemplated at the time of data collection. However, profiling in itself is not a source of concern. Instead, the absence of adequate information on the algorithmic mechanisms which prompt profiling and targeted advertising practices should be tackled though better transparency from data controllers, according to the general approach.

User profiling through possession of big data is central in some markets, such as online advertising, where there is the ability to create, through the technology of the internet, more accurate user profiles, which creates the ability to reach specific consumer types (by sending them targeted messages, with increasing levels of customisation) and to measure more precisely the effectiveness of advertising campaigns. In this perspective, strategic relevance is given to the collection of data about users, which constitute assets of crucial economic value, as they are likely to be included as part of the advertising industry. This calls for further neutrality and transparency on search-advertising platforms.

In this respect, Google has been accused of manipulating its organic search results to favour its own services. These allegations have often been accompanied by appeals for regulatory or antitrust intervention. They must nevertheless take into full account the two-sided nature of the search-advertising platform and the feedback effects that link the provision of organic search results to consumers, and the sale to businesses of advertising. The European Commission, in the framework of the digital single market strategy for Europe, launched in May 2015, plans to unveil a comprehensive assessment of the role of platforms and online intermediaries, which will cover issues such as transparency (eg. in search results), involving paid-for links and/or advertisements.

As for breach notification, the GDPR dictates that supervisory authorities and affected individuals must be notified of violations that are likely to jeopardise the rights and freedoms of individuals, with notice to supervisory authorities "without undue delay and, where feasible, not later than 72 hours". This approach differs from that pursued by the Commission in stipulating compliance obligations that must be fulfilled by all data controllers, which is less risk-tailored. The Commission initially suggested that notification of data security breaches be made within a period of no longer than 24 hours of the data controller becoming aware of the violation.

Another notable feature of the proposed regulation is the explicit enshrining of the right to be forgotten, which is now accepted as a European general principle, following the landmark case by the European Court of Justice (ECJ). On 13 May 2014, the ECJ held that, by searching systematically for information published on the internet, indexing websites, recording and making it available, the operator of a search engine is 'processing' personal data within the meaning of Article 2(b) of Directive 95/46/EC (see the Google Spain case).[5] Following its earlier decision,[6] the Court confirmed that, even when the information collected by the operator of a search engine had already been published elsewhere by others, the search engine's related activities still must be classified as processing under the directive.

The decision required Google to consider individuals' requests to eliminate links that they say impinge on their privacy. This provision would give anyone the right "to obtain from the controller the erasure of personal data [...] without undue delay" (the 'data controller' is essentially the entity that makes decisions about how and for what purpose data is processed). The GDPR explicitly acknowledges to the data subject the right to obtain from the controller the erasure of personal data without undue delay (see article 17).

REFORM OF THE E-PRIVACY DIRECTIVE

The year 2015 was undoubtedly one of great change. The new Commission, headed by Jean-Claude Juncker, ambitiously set the goal "to take, within the first six months of [his] mandate, ambitious legislative steps towards a connected digital single market". Even though the Connected Continent package was partially unsuccessful due to strong conflicts between the Council and Parliament (because its scope was curtailed to roaming and net neutrality), the Commission's digital single market (DSM) strategy is nevertheless a programme of welcome initiatives, ambitious in aim, scope and implementation timing.

> **The rationale of the GDPR has been supported and reinforced by the DSM strategy.**

The rationale of the GDPR has been supported and reinforced by the DSM strategy, which irons out 16 targeted actions to be delivered by the end of 2016. One of the actions calls for a reform of Directive 2002/58/EC (the e-privacy directive).[7] Privacy is a matter of great importance to EU citizens, as two-thirds are worried about not having full control over the information they provide online.[8] Indeed, adoption of the GDPR, which will replace Directive 95/46/EC, will have consequences also for the e-privacy directive, which is *lex specialis* (governing law) for the electronic communications sector.

In this vein, the DSM strategy calls for a reassessment of the e-privacy directive, particularly since most of the articles of the current directive exclusively apply to providers of electronic communications services – that is, traditional telecoms companies – and does not include in its scope information society service providers using the internet to provide communication services.

ECJ STANCE ON THE DATA RETENTION DIRECTIVE

European institutions must also adhere to the ECJ's judgment that declared the Data Retention Directive,[9] which related to telecoms data, invalid in 2014. The ECJ established that, although the retained data did not comprise the content of the communications, data could *"allow very precise conclusions to be drawn concerning the private lives of*

the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".

In other words, the ECJ held that the directive restricted subscribers' privacy because *"the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance"*. The directive did not ensure a retention period "limited to what [was] strictly necessary" as it instituted a minimum retention period of six months without distinguishing between different sorts of data or different types of users, and a retention period of between six months and two years without requiring any "determination [that the] period must be based on objective criteria".

For those reasons, the ECJ declared the data retention directive invalid, holding that it did not satisfy the principle of proportionality, and should have assured more safeguards to protect the fundamental rights of freedom of expression, respect for privacy, and protection of personal data, guaranteed by the Charter of Fundamental Rights of the EU.

As president of the European Parliament, Martin Schulz, remarked in response to the ECJ's ruling, any new proposal must *"respect in every detail the guarantees laid down in the Charter of Fundamental Rights [...], enshrin[ing] a high level of data protection – which is all the more essential in the digital age – thus avoiding disproportionate interferences with the private lives of citizens"*. Hence European institutions cannot ignore the ECJ's decision regarding personal data and privacy. In particular, the proposal for the EU data protection directive must be in conformity with the ECJ's ruling.[10] By the same token, the ECJ and the national courts have to take into account the Charter of Fundamental Rights in judging cases where EU law is at stake.

Interestingly, the advisory Article 29 data protection working party[11] also called on member states to gauge the consequences of the ECJ pronouncement on national data protection laws, remarking that *"there is no bulk retention of all kinds of data and that, instead, data are subject to appropriate differentiation, limitation or exception"*.

Increasing reliance on the possession of user data is a prominent feature of today's information society. Data is an extremely valuable asset in a number of sectors, for instance in online search advertising. It enables players in the search advertising industry to move swiftly into neighbouring markets, such as contextual, display, email and general, non-search advertising. The tendency towards convergence of these different formats of advertising, owing to the development of behavioural advertising and the trend to mix and match diverse advertising strategies by the major players in the industry, has been remarked on by the European Commission during the course of investigations into both Google/DoubleClick and Microsoft/Yahoo.[12]

At the same time, data possession generates barriers to entry by conferring to the incumbent advantages that cannot be replicated by potential entrants. In particular, other entities engaged in offering internet search advertising will barely be able to match the quality of the results offered by a dominant firm, which can strengthen its position by simultaneously playing in multiple, parallel markets where it can acquire, verify, test and obtain additional specification of the information gained in the normal search advertising context.

As a consequence, data-driven markets are likely to be much less precisely defined around a certain product or service, and much more on a participant's ability to use those data across different types of activity. Thus a crucial element in defining these markets is describing the scope to which the privacy policy specified in the terms of use of the website (or search engine) permits utilisation of the information received from the user in other contexts, as well as the provision of another service by the same company ('intra-company versatility') and for other companies to provide another or even the same service ('inter-company portability').

> **Increasing reliance on the possession of user data is a prominent feature of today's information society.**

INVALIDATION OF THE COMMISSION'S US SAFE HARBOUR AGREEMENT

Edward Snowden's revelations of mass surveillance on EU citizens impacted on the so-called safe harbour scheme, which includes a series of principles concerning the protection of personal data to which US undertakings may subscribe voluntarily.[13] Specifically, on 6 October 2015, the ECJ declared invalid[14] the European Commission's transatlantic data protection agreement from the year 2000, holding it does not adequately protect consumers. Indeed, EU privacy law forbids the movement of its citizens' data outside of the EU, unless it is transferred to a location which is deemed to have 'adequate' privacy protections in line with those of the EU.

The safe harbour agreement had permitted companies to self-certify that they would protect EU citizens' data when transferred and stored within US data centres, developing a single standard for consumer privacy and data storage in both the US and Europe, without the need to ask for consent, or to enter into bilateral agreements.

In fact, even the European Commission had previously expressed doubts on the appropriateness of the safe harbour scheme. In a communication in November 2013 it acknowledged the growing concern among some data protection authorities in the EU about data transfers under the scheme, and pointed out that *"some member states' data protection authorities have criticised the very general formulation of the principles and the high reliance on self-certification and self-regulation. Similar concerns have been raised by industry, referring to distortions of competition due to a lack of enforcement."*[15]

In its landmark ruling, the ECJ specified that the European Commission did not have the competence to restrict national supervisory authorities' powers in protecting the personal data of their citizens. Interestingly, the ruling came less than a week after the ECJ judgment in the Weltimmo case,[16] in which it held that international companies should abide by the data protection legislation of the jurisdictions in which they operate (the case concerned a property website company registered in Slovakia but was 'operating' in Hungary).

Following the invalidation of the safe harbour agreement, American companies, including internet behemoths such as Google, Facebook, Apple and Microsoft, must strive for striking 'model contract clauses' to authorise the transfer of data outside of Europe, thus guaranteeing an adequate level of protection in line with EU rules. In this vein, it is likely that big US companies will be building EU-based data centres to handle data for EU citizens.

Nonetheless, it should be noted that the EU is currently negotiating with the US for an upgraded safe harbour to meet the ECJ's concerns, while ensuring certainty and clarity.

COUNCIL OF EUROPE MODERNISATION OF CONVENTION NO. 108

In parallel with the legislation initiative of the Commission, the Council of Europe (CoE) in March 2012 presented its proposals for updating the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108).[17] In October 2011, the parliamentary assembly of the CoE made a recommendation backing the reinforcement and globalisation of Convention 108.[18] In November 2012, the CoE consultative committee adopted its final proposals for modernisation, and submitted them to the Committee of Ministers for adoption.[19] Eventually, the ad hoc committee on data protection of the CoE approved on 3 December 2014, after discussions and amendments, the modernisation proposals of the convention. A draft amending protocol is to be arranged on this basis and transmitted to the Committee of Ministers for examination and adoption.[20]

Although the EU and CoE share the same concerns on data protection, their approaches differ. The convention, which serves as a sort of universal standard, is less prescriptive and more focused on human rights (see its preamble).[21] But its coherence and compatibility with the European regulatory framework remain key objectives.

THE WAY FORWARD

Negotiations to reform EU rules on data protection are in the final stage. On 17 December 2015, the EU Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) voted on the informal agreement on the data protection package.[22] The reform package's final texts will be voted on and formally adopted by the European Parliament and Council later in 2016, probably in March or April. From then there will be a two year timescale for its entry into force.

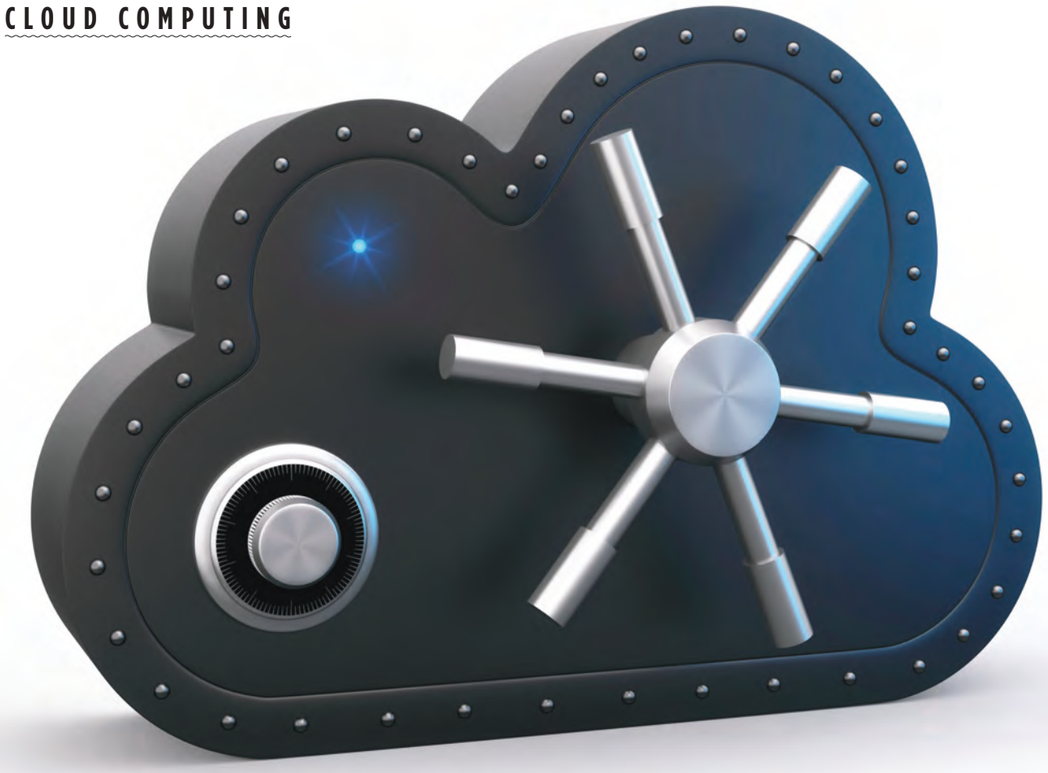
Against this backdrop, the DSM strategy will play a crucial role. The challenge is in dealing with highly technical matters while being confronted by strong political stances that are not always conducive to facilitating the path towards implementation. The DSM strategy is supposed to deliver different actions by the end of 2016, with the support of the Parliament and Council.

> **A balance should be struck between hyper-regulation and a dangerous lack of data protection.**

Because of these potential conflicts, a balance should be struck between the risk of a race to hyper-regulation – which would threaten to stifle the dynamic digital market – and a dangerous lack of comprehensive data protection within the European Union.

MAURIZIO MENSI *is professor of economic law at the National School of Administration (SNA) and of information and communications law at LUISS Guido Carli University, Rome. He is a member of the Rome Bar and has been admitted to practice before the highest court of Italy. Mensi focuses on communications and media, IT, privacy and data protection, copyright, cyberlaw and regulation of public utilities.*

REFERENCES 1 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. **2** Safeguarding privacy in a connected world: A European data protection framework for the 21st century. bit.ly/1IIhkye **3** Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Preparation of a general approach. bit.ly/1ShoM8T **4** Agreement on Commission's EU data protection reform will boost digital single market. EC press release, 15 December 2015. bit.ly/1J9ZUdt **5** Google Spain – judgement of 13 May 2014. bit.ly/1MKoqFS **6** Satakunnan Markkinapörssi and Satamedia – judgement of 16 December 2008. bit.ly/1LEUqHq **7** Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector. See the Commission's DSM strategy, pillar II, action 12. **8** Eurobarometer survey on data protection, June 2015. bit.ly/1LPx1Ho **9** Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, amending Directive 2002/58/EC. **10** Proposal for a directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25 January 2012. bit.ly/1Tj7acV **11** The Article 29 working party comprises a representative from the data protection authority of each EU member state, the European Data Protection Supervisor and the European Commission, as set out in Article 29 of Directive 95/46/EC. **12** See Case COMP/M.4731 Google/Double Click; Case COMP/M.5727 Microsoft /Yahoo Search Business. **13** Commission decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. **14** Judgment in Case C-362/14. The Court of Justice declares that the Commission's US Safe Harbour decision is invalid. 6 October 2015. bit.ly/1FUc1iu **15** Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU. bit.ly/19VRFqN **16** Judgment in Case C-230/14. Weltimmo s.r.o. vs Nemzeti Adatvédelmi és Információszabadság Hatóság. 1 October 2015. bit.ly/1VrPhIG **17** Convention for the protection of individuals with regard to automatic processing of personal data, adopted by the Council of Europe in 1981. ETS No. 10. **18** Council of Europe parliamentary assembly, recommendation 1984 (2011): The protection of privacy and personal data on the internet and online media. **19** Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data (T-PD). Modernisation of Convention 108: Final document. Strasbourg, 29 November 2012. **20** Ad hoc committee on data protection. 3rd meeting. 1-3 December 2014. bit.ly/1sumsTF **21** "Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing [...] recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples." Preamble, Convention No. 108. **22** New EU rules on data protection put the citizen back in the driving seat. European Parliament press release, 17 December 2015. bit.ly/1JECFse



DARK CLOUDS?

Are regulations being applied to cloud computing in a way that stimulates innovation, asks **KUAN HON**

It is clear that cloud computing offers society many potential benefits.[1] However, its take-up is still being held back by much fear, uncertainty and doubt among not just potential cloud users, but also some policymakers and regulators. The position is exacerbated by the fact that current laws are not technology neutral. Indeed, arguably, European Union (EU) laws are being applied so as to discriminate against cloud computing, in part perhaps because of fears regarding US technology companies' dominance in the cloud market and/or their excessive collection of EU residents' personal data.

This article gives some illustrative examples, and argues that the situation needs reconsideration. While the focus is on EU laws, the ways in which they have been applied have broader relevance to technology neutrality generally.

CLOUD – NO ONE SIZE FITS ALL

Essentially, cloud computing involves the self-service use of IT resources over a network, scalable up and down with demand/need.[2] Based on the US National Institute of Standards and Technology (NIST) service models,[3] where the IT resource used is a software application, such as email, word processing, social networking, photo sharing or a customer relationship management application, the type of service is termed SaaS (software as a service). Where the IT resources used over a network comprise 'raw' computing resources, ie. computing infrastructure that may be used for storage, computation and/or networking functions, the type of service is termed IaaS (infrastructure as a service). Where the IT resources comprise a 'platform' for the development and deployment/hosting of a software application of the cloud customer's own choice, the type of service is PaaS (platform as a service).

These resources are provided 'as a service' – customers need not be concerned with exactly how hardware/software infrastructure resources are marshalled behind the scenes to provide them with the requested service. Typically, public cloud involves the shared use, by separate customers simultaneously, of standardised commodity hardware or even software. The efficiencies and economies of scale, and resultant cost savings, that typify public cloud are enabled by this shared use (and the ability to redeploy underlying hardware/software for use by other customers, when one customer's usage ceases).

So it can be seen that the term 'cloud computing' encompasses a huge variety of different services. This means that a one size fits all approach should not be taken to cloud. Although these services have some common characteristics, reflecting the cloud service delivery model, each type of service often merits separate consideration, particularly when it comes to their regulation, because their differences may be as significant as their similarities, and these differences need to be taken into account by policymakers and regulators in order to regulate them appropriately.

Nowadays, in an attempt to future-proof laws against subsequent technological developments, policymakers and regulators often aspire towards technology neutrality.[4] However, a core problem with many existing laws and regulations is that they are far from being technology neutral. As data protection law issues often come up in the cloud context, examples from that field will serve well to illustrate many of the problems that arise from laws not being technology neutral – in this case the Data Protection Directive 95/46/EC, together with national implementing laws under the directive and regulators' and courts' interpretations of such laws.

TREATED AS 'PROCESSORS'

The first example is regulators' insistence that many cloud providers must be treated as 'processors'.[5] Recall that, under the directive, data protection obligations (and liability) are imposed on the controller, the person who controls the 'purposes and means' of processing personal data. A controller may engage a processor to process personal data on its behalf, but the controller remains primarily liable, including for its processor's actions or omissions in processing the data.

Recall also that, under the directive, 'processing' is very broad, and includes merely storing personal data passively, or transmitting personal data mechanically. This means that, strictly, a regulator's approach is correct: if a cloud service is used by a controller for processing any personal data, eg. file storage or sharing where the file contains personal data, then the provider is a 'processor', because it is at least storing personal data, even if only passively.

This also means that the directive's rules governing the use of processors apply when a controller uses a cloud service to store or otherwise process personal data, including a requirement that the controller must ensure it has a contract with the processor whereby the processor agrees to comply with the controller's 'instructions' in processing the personal data.

However, the processor provisions of the directive are based on 1970s outsourcing models.[6] Then, and indeed in the 1960s, controllers used computer service bureaux, which were handed personal data (stored on magnetic tape or even punched cards) to process actively for the controller in accordance with the controller's instructions, typically for payroll or accounts receivable processing. This is a far cry from a cloud provider, or indeed non-cloud hosting provider, passively storing personal data which the controller uploads, operates on and retrieves in self-service fashion, using the provider's software made available as part of the provider's service, without requiring any active action on the part of the provider.

The analogy I suggest is that of cooking.[7] If we liken the processing of personal data to the cooking of food, data protection laws assume that either you cook food yourself in your own kitchen (controller), or else you hire a caterer (processor) to cook food for you as per your instructions. But using IaaS, PaaS and certain SaaS cloud services is much more like renting a kitchen in which you then cook food yourself, or getting take-out or a ready meal which you then microwave yourself in your own kitchen. It seems obvious that laws intended to regulate the use of caterers would be difficult or impossible to apply to kitchen rentals or microwaving – they were not designed for the latter. So too with data protection laws' processor provisions and cloud computing.

In particular, the contractual 'instructions' requirement makes no sense in self-service public cloud, which involves the use of standardised commodity resources that could not realistically be tailored to different customers' individual instructions.[8] If we look behind the instructions rule, its legislative objective was in fact to prevent unauthorised disclosure or unauthorised use by the processor. So, the policy aim of that rule could have been met, without needing to refer to any 'instructions', by requiring a contractual term prohibiting, more generally, any unauthorised use/disclosure by the processor (or by imposing a similar statutory prohibition). However, because that rule was based on outdated assumptions regarding outsourcing models/processes, cloud customers and providers are in the difficult position of either agreeing a meaningless contractual term, or breaching data protection laws.[9]

> **The processor provisions of the directive are based on 1970s outsourcing models.**

Another unspoken assumption underlying the instructions rule is this: the rule assumes that processors must always have access to personal data in intelligible form. Again, that was certainly true in the days of computer service bureaux, which needed access to intelligible data to perform the functions for which they had been engaged, such as payroll processing. However, this assumption does not necessarily hold true in cloud computing, because with many types of cloud application, such as file storage, customers are able (if they so choose) to encrypt their data before upload to the cloud, such that the cloud provider has no access to the decryption keys. In such cases, it seems pointless to require the provider to follow the controller's instructions regarding such data, or even to prohibit the provider from using or disclosing such data, because it cannot access intelligible data – no privacy risks arise from a provider that has no access to intelligible data, as it can't disclose or misuse data that it can't understand.

Some might argue that a cloud provider should be legally obliged to follow any instructions given by the controller to back up the controller's data. I suggest that this argument is misguided, particularly with encrypted data. Suppose that a controller of personal data decides to encrypt that data and then upload that encrypted data to a file storage service (cloud-based or not) offered by a service provider. The controller knows the

Coming out of the cloud: Rovio's Angry Birds relies on Amazon's Web Services

nature and content of that data, and took the decision to use the storage service. The provider does not; it simply makes a storage service available for self-service use by customers, perhaps even as a free service. In terms of logic and fairness, who ought to be legally obliged to look after that data, such as by ensuring that the data are backed up to another service or to the controller's own facilities, or even by paying the provider extra fees for a contractual commitment from the provider to backup that data elsewhere? Surely it should be the controller that is legally obliged to protect that data, not the provider, which has no idea what data are being stored by its customers using its service.

Forcing all cloud providers always to back up all their customers' data at all times in all cases would be too blunt a requirement. It would interfere with freedom of contract and controller choice (as to exactly how it wants its data to be backed up and at what price), raise costs generally, and even be detrimental for data protection, as ideally data ought to be backed up with a different provider at a different (and preferably far distant) geographical location in case of a provider's failure or insolvency or a natural disaster affecting the primary location. Although the EU's proposed General Data Protection Regulation (GDPR) looks set to impose certain obligations and liabilities directly on processors, it seems unfair to do so in situations where the processor is unaware that the data are personal, because the data are encrypted and the processor has no access to the key.

Indeed, it's arguable that, even if personal data are uploaded to the cloud in unencrypted form, with many types of cloud services (which I term 'infrastructure cloud'), notably IaaS, PaaS and pure storage SaaS services, the provider would still be ignorant of the nature or content of data uploaded to its services – unless and until it 'looks'.[10] In most cases, it will not bother to look. An infrastructure cloud provider is most like a computer rental company. If you rent a computer from a rental company, then what you use the computer for, what type of data you process using that computer and how, is entirely your own business. No one would seriously suggest that the rental company must be treated as a processor for data protection law purposes, should you choose to process personal data using its computer. The same logic ought to apply to infrastructure cloud.

True, a rented computer is legally owned by the rental company, not by you, and the rental company could well plant spyware on the computer to monitor you and even read the data you process using its computer. But if it does so (as happened with Aaron's, a computer rental chain in the US)[11] then it would become a controller in its own right, and liable as such. However, the potential for a computer rental company to install spyware on its rental computers does not mean that all computer rental companies should automatically be treated as 'processors'. And surely the same argument should apply to infrastructure cloud.

Going further, I argue that obligations should be imposed only on those with access to intelligible data, unless the policy decision is made to impose strict liability of some kind, such as for security measures. However, any such policy decision should be taken only after full consideration of the implications, including open discussion with all relevant stakeholders.

Currently, infrastructure cloud services, as substitutes for buying/renting computing resources and provisioning/deploying app hosting services in-house, have a very important role to play in enabling innovation. A European technology startup seeking to become the next Facebook or Google, or some novel type of service we may not even have considered yet, is very likely to want to use IaaS or PaaS to service its end users, because infrastructure cloud services offer speed to market, low upfront costs, and high flexibility and agility. Many mobile apps are built on top of IaaS or PaaS services; for example, Finnish company Rovio's popular Angry Birds game uses Amazon Web Services.[12] Some cloud providers may well be processors in the active sense, depending on the type of service. But constraining the use of computing resources (in the form of infrastructure cloud services) by deeming cloud providers to be processors, even with infrastructure cloud services or when data are encrypted pre-upload, seems unnecessary and counter-productive. Tarring all cloud providers with the same 'processor' brush could even deter innovation.

> **An infrastructure cloud provider is most like a computer rental company.**

Furthermore, the use of encryption by cloud customers (and indeed cloud providers, to prevent intelligible access by their sub-providers) should be encouraged by legally recognising that encryption may render data unreadable to unauthorised persons. Suppose you find a USB flash drive in the street but it contains encrypted personal data, so you can't read it. Now, you do control the purposes and means of processing the data on that drive. Should you be treated as the controller of that personal data (that you don't even know is personal data), with corresponding obligations and liabilities? If you give that drive to someone else to look after, should they become your processor? I argue not: surely legal obligations should only be imposed on those who can access intelligible data. Similarly, treating cloud providers as processors if they hold encrypted personal data, where they have no access to decryption keys, makes little sense. Yet the proposed GDPR would impose obligations and liabilities on such providers as processors.

Many non-technologists seem to mistrust encryption. Yet former US National Security Agency (NSA) contractor Edward Snowden, who revealed mass digital surveillance by the US National Security Agency and other intelligence/security agencies, has noted that encryption, used properly, could withstand "brute force attacks" from powerful spy agencies and others. "Properly implemented algorithms backed up by truly random keys of significant length... all require more energy to decrypt than exists in the universe".[13]

Security experts such as Bruce Schneier believe that encryption, if adopted en masse by internet users for storage and transmissions, should not only help to protect data against theft or loss, but also make wholesale state surveillance of internet users more difficult and expensive.[14] Policymakers need to recognise the critical role that technical measures such as encryption could play in protecting personal data, and encourage its use more widely. So where are the incentives for controllers (and processors) to apply encryption?[15]

USE OF SUB-PROVIDERS

As another example of non-technologically neutral laws adversely impacting cloud, consider data protection regulators' approach to the use of sub-providers in cloud computing.[16] In cloud computing, if a SaaS service is provided using underlying IaaS or PaaS infrastructure, the IaaS/PaaS provider is treated as a sub-provider. Regulators want all sub-contracts between cloud providers and their IaaS/PaaS sub-providers to mirror the controller-processor contracts, complete with the (meaningless in cloud) 'instructions' requirement. Again, however, cloud is completely different from traditional outsourcing.

Suppose you outsource data processing to a third party service provider, which buys or rents computing resources (servers, storage appliances, networking equipment) to provide you with that processing service. Regulators would not require 'mirror' contracts from the vendors of such hardware infrastructure in that situation, so why do they require them from infrastructure cloud sub-providers? Requiring mirror contracts where computing resources are sourced from cloud infrastructure service providers, but not when those resources are purchased or rented for exclusive use in the classic equipment rental sense, discriminates against the cloud model.

If the justification for the different approach to cloud is that infrastructure cloud providers could access data processed using their services, the same could be said of computer rental companies, and equally hardware manufacturers/vendors could also install 'backdoors' in their equipment to access data processed using that equipment. Indeed, reportedly the NSA intercepted routers in transit to targeted destination companies, to install such backdoors.[17]

So why is it that regulators don't require controllers who use routers and other equipment for their own internal processing to check for possible backdoors? Why don't they require controllers, when using non-cloud processors, to compel the processors to check the hardware they use (eg. servers in the processor's own data centres) to process personal data on controllers' behalf? The EU directive and related laws do require controllers to take appropriate security measures, and also require that controller-processor contracts must oblige processors to take certain security measures. It could be said that those general security requirements would, or could, implicitly extend to such checks, so no explicit requirement is necessary.

> **Where are the incentives for controllers (and processors) to apply encryption?**

However, if those general security requirements are considered sufficient to address the risks of backdoors in hardware used by controllers and non-cloud processors, why aren't they also considered good enough to address the risks of cloud provider/sub-provider access? Why should mirror contracts be required from cloud sub-providers in addition? Couldn't technical measures such as encryption, and specific contractual

A QUESTION OF BALANCE

Conflicts between different rights and freedoms

Another vital issue is how to strike an appropriate balance between the different rights and interests which democratic societies strive to safeguard and foster, but which may in certain situations conflict. A classic clash is that between privacy/data protection and freedom of expression, or freedom to conduct a business or indeed European Union citizens' freedom to work and provide services in any member state – all of which are enshrined as fundamental rights under the EU Charter of Fundamental Rights. Cloud brings these clashes to the fore.

Consider the policy objective of fostering e-commerce, to which end the E-Commerce Directive (2000/31/EC) introduced certain 'notice and take-down' defences for neutral intermediaries, whereby such intermediaries are liable only if they know about infringing material and do not remove it. A web hosting provider does not know the nature of the content hosted on its servers, unless it looks or is notified that the content is copyright-infringing. If it takes down the content on receiving such notice, this provides it with a defence against liability. However, the E-Commerce Directive does not apply to personal data. Therefore, if the content hosted is personal data, unlawfully posted to the website concerned, it seems that the hosting provider could be a 'processor' (and liable as such under the proposed GDPR).

If so, neutral e-commerce intermediaries, cloud or otherwise, would be liable for personal data regardless of their knowledge or control. Is this truly the intended policy objective? Have the full ramifications of such an approach been considered, such as increased costs for EU customers or even the potential withdrawal of certain services from them? The proposed GDPR would simply state that it is 'without prejudice' to the application of the E-Commerce Directive, which fails to clarify the uncertainty ('B is without prejudice to A, but A shall not apply to B' - so what's the law?). Policymakers should make it clear whether neutral intermediary defences will be available for personal data.

provisions (narrower than full mirror contracts) suffice to protect against such risks?

As mentioned, technology startups and other SMEs may wish to use IaaS/PaaS from cloud sub-providers for speed to market and cost-efficiency. However, SMEs rarely have the bargaining power to force large cloud sub-providers to enter into such mirror contracts, and it's a similar situation with European cloud providers that base their offerings on the services of large sub-providers. Large cloud providers, which have more control over their supply chain, are far more likely to be able to obtain mirror contracts from their sub-providers, and therefore are more able to offer law-compliant data protection processing. So, while regulators of course have the protection of data subjects in mind, when insisting on mirror contracts the (unintended) consequence is to favour large providers, most of which are not European. Has the impact of this approach on competitiveness and innovation been considered, as well as its effectiveness to achieve the underlying policy objective?

A related issue is the legal uncertainty regarding whether a data centre provider is or is not a cloud sub-provider, from which a mirror contract would also be required. Only the largest providers can afford to build their own data centres. Most providers, particularly SMEs, rent space/servers from third party data centre operators, many of which are large global organisations. If mirror contracts are required from such data centre operators, again SMEs are unlikely to be able to secure such obligations. Yet again, this approach seems to discriminate against cloud computing.

Similarly, suppose that, in a traditional outsourcing model, a controller engages as its processor a service provider that happens to use a third party data centre. If a non-cloud service provider uses a third party data centre operator, would a mirror contract not be required, and if not, why should it be required if the service provider uses the cloud model? The data centre operator's position and rights/liabilities in relation to the service provider are not likely to differ with whether the provider's service involves cloud or not.

And are telecoms operators that provide connectivity to data centres to be considered as sub-providers that must also sign mirror contracts? If this is required for cloud providers, why not for non-cloud services too?

CONSUMER ISSUES

I have focused mainly on infrastructure cloud services, but SaaS also merits mention. It seems that understandable concerns regarding the massive collection of EU residents' personal data, particularly by internet companies and advertising networks, have resulted in strong reactions on the part of policymakers and regulators, such as (arguably) parts of the proposed GDPR, which includes recitals that "consent should not be regarded as freely given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment", and "Consent is presumed not to be freely given, if it does not allow separate consent to be given to different data processing operations despite it is appropriate in the individual case, or if the performance of a contract, including the provision of a service is made dependent on the consent despite this is not necessary for such performance."

Such concerns may also have influenced regulators' attitude towards cloud. Indeed, reactions have been triggered on the part of consumers also, including the increasing use of ad blockers: the Interactive Advertising Bureau recently admitted that "we messed up... we built advertising technology to optimise publishers' yield of marketing budgets... Looking back now, our scraping of dimes may have cost us dollars in consumer loyalty."[18]

Consumers do enjoy some benefits from free, ad-funded services – cloud-based or otherwise, many of which use personal data in return for providing free services. It may be counter-productive to prevent such services completely, as could be the result if the proposed GDPR's recitals are taken to prohibit conditional consent altogether. Although that issue is not cloud-specific, again the difficult question is how to strike an appropriate balance: how to allow free services to be provided without excessive collection or use of consumers' personal data. The recitals quoted may reflect policymakers' understandable reaction against many free services' excessive collection/use of personal data, but care must be taken if consumers are not to be deprived of free services altogether. A more granular exchange of personal data for services might be ideal, if it can be achieved in a way that is not too time-consuming or burdensome for consumers or service providers.

In summary, fears about personal data collection/tracking may well be behind strict approaches to cloud computing. Furthermore, it seems to be inherent to assume that new things are risky and to be feared.[19] However, it is important not to take a one size fits all approach to cloud and bear in mind its potential uses for innovation. Policymakers and regulators need to be better informed about the technological, commercial and social environments to strike the right balance.

DR KUAN HON *is a senior researcher working on cloud law projects at the Centre for Commercial Law Studies, Queen Mary University of London, and a consultant lawyer for Pinsent Masons. This article is written in her personal capacity. See kuan0.com or email k@kuan0.com*

REFERENCES **1** See: Uptake of cloud in Europe (2015). IDC follow-up report for the European Commission. bit.ly/1JUWKxb **2** Hon K and Millard C (2013). Cloud technologies and services. In: Millard C (ed). Cloud Computing Law. OUP. **3** Mell P and Grance T (2011). The NIST definition of cloud computing. 1.usa.gov/1umXAe3 **4** This aim is difficult to achieve, partly because technology neutrality has many possible meanings – see chapter 11 in: Reed C (2012). Making Laws for Cyberspace. OUP. **5** Leaving aside for now the issue that providers of some cloud services are in fact likely to be 'controllers'. See: Hon K et al. (2013). Who is responsible for personal data in clouds. In: Millard C (ed). Cloud Computing Law. OUP. **6** The directive was first drafted in 1990, based on the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, although the directive was not finally adopted until late 1995. **7** Hon K (2012). The 12 Cs of cloud computing: A culinary confection. SCL. bit.ly/1HCGq6h **8** Hon K et al. (2013). Chapters 4, 5, 8 in Cloud Computing Law. **9** Hon K et al. (2013). Chapter 8 in Cloud Computing Law; Hon K et al. (2013). Cloud accountability: The likely impact of the proposed EU data protection regulation. SSRN. bit.ly/108yfuL **10** With many SaaS offerings, it is clear that customers are using them for personal data, and providers of such cloud services may even be controllers, not just processors. This argument does not apply to them; the focus here is on infrastructure cloud. **11** FTC (2014). FTC approves final order settling charges that Aaron's Inc. allowed franchisees to spy on consumers via rental computers. 1.usa.gov/10BS40a **12** AWS case study: Rovio. amzn.to/10t75DB **13** Harding L (2014). Edward Snowden: US government spied on human rights workers. The Guardian. bit.ly/1ls640E **14** Schneier B (2013). NSA surveillance: A guide to staying secure. The Guardian. bit.ly/1bHCz49 **15** The proposed GDPR would recognise and encourage the use of encryption, in one sense, as personal data breaches need not be notified to data subjects if measures (eg, encryption) have been taken to render the data unintelligible to unauthorised persons (similar to some US breach notification laws). However, I argue that the implications of encrypted personal data being unintelligible to those without decryption keys need to be recognised more broadly, and considered and taken into account properly, by policymakers and regulators, bearing in mind the underlying policy objectives, notably protection of privacy. Isn't it time for a more nuanced approach that considers the status of such data in the hands of someone with the key, and someone without the key? The cynical might suggest that the lack of incentives in law for encryption may be deliberate, given some governments' anti-encryption stance and their (misguided) desire for encryption backdoors. **16** Article 29 Data Protection Working Party (2012). Opinion 05/2012 on cloud computing. bit.ly/1c8KILJ **17** See for example: Clark D and Yadron D (2014). Greenwald: NSA plants 'backdoors' in foreign-bound routers. WSJ. on.wsj.com/1nlimkh **18** Cunningham S (2015). Getting LEAN with digital ad UX. IAB. bit.ly/1VU6j28 **19** For example, the proposed GDPR seems to consider 'new technologies' as being high risk. However, new technologies are not automatically risky per se – it depends on what those technologies are and, most importantly, how they are used. Similarly, the proposed GDPR disfavours and would restrict transfers which are 'not repetitive', and concern 'only a limited number of data subjects', but arguably the emphasis should be on protecting transfers adequately, regardless of frequency or scale. Payment details are transferred in huge volumes securely every second, when online purchases are made. This shows that transfers may be protected by using properly encrypted connections, even when they are repetitive or relate to many individuals.

THINGS TO REGULATE

In part two of this briefing on the internet of things, **IAN BROWN** discusses the regulatory actions that could be necessary in this diverse technology sector

The deployment of internet of things (IoT) systems, and their potential impact on individuals and businesses, raises regulatory issues – some familiar to telecoms regulators, such as licensing, spectrum management, standards and competition – and others where a lead is often taken by other regulators, such as data protection, privacy and security.

A 2013 European Commission consultation exercise found a diversity of views on whether IoT-specific regulation is necessary.[1] Industry respondents argued that state intervention would be unwise in this young sector, and that general rules such as the EU's forthcoming data protection regulation will suffice. Privacy advocacy groups and academics responded that IoT-specific regulation is needed to build public confidence, as well as to ensure a competitive market.

Meanwhile, a US Federal Trade Commission (FTC) staff report suggested that IoT-specific legislation would be premature. It instead encouraged self-regulatory programmes for IoT industry sectors to improve privacy and security practices – while also reiterating the FTC's previous call for "strong, flexible, and technology-neutral federal legislation" to strengthen its ability to enforce wider data security standards and require consumer notification following a security breach, and for broad-based privacy legislation.[2]

I will now possible review actions taken by regulatory agencies that will enable the development and adoption of IoT systems in a way that should maximise their societal benefit.

LICENSING AND SPECTRUM

Licensing and spectrum management are important issues for ensuring availability and capacity for IoT communications. IoT devices communicate using a range of different protocols, based on their connectivity requirements and resource constraints. These include short-range radio protocols such as ZigBee, Bluetooth and WiFi, mobile phone data networks, and in more specialised applications such as traffic infrastructure, longer-range radio protocols such as ultra-narrow band (UNB).

To communicate with remote networks, IoT devices may send data via a gateway with a wired (PSTN, ethernet, power line or DSL) or wireless (2G, 3G, 4G/LTE or UNB) connection to the global internet or telephony network – or directly over one of these mediums. For consumers, the gateway will often be a smartphone or home wireless router. Businesses will frequently make use of their existing corporate data networks.

> **"Is IoT-specific regulation needed to build public confidence and competition?"**

Devices communicating over kilometres need access to the 300 MHz to 3 GHz spectrum range, while centimetre or millimetre contactless transactions may use near field communications at 13 MHz or EHF bands. Some IoT applications may also make use of AM/FM bands in the VHF range. Telecoms companies are experimenting with white space spectrum to make more use of often-

unused spectrum bands, while a US presidential commission has recommended the development of shared-space technology that enables government, licensed commercial users, and unlicensed users to cooperatively make use of a large amount of spectrum.

The US Federal Communications Commission (FCC)'s expert IoT working group predicts IoT will add significant load to existing services such as WiFi and 4G mobile networks. Regulators will need to give continuing attention to the availability of spectrum for short-range IoT communications and the capacity of backhaul networks that connect IoT gateways to the internet, and to the rollout of small cell technology such as 4G. If these conditions are met, the working group does not expect that new spectrum will need to be explicitly allocated to IoT communications.[3]

The FCC is also reviewing the use of spectrum above 25 GHz for 5G networks, and possibly for IoT. The Korean government plans to secure additional frequency of at least 1 GHz by 2023 and ensure 5G is commercialised by 2020 in response to the exponential growth it expects in IoT traffic.[4]

Studies for the European Commission have suggested that a licence-exempt model is most effective for IoT development, since it avoids the need for contractual negotiations before devices are manufactured and used, allowing the production of large numbers of cheap devices.[5]

SWITCHING AND ROAMING

Firms operating large networks of M2M devices via mobile telephony networks, with a fixed SIM in each device, may not find it easy to switch networks at the end of a contract, or if a device roams into a different network area, or for some time period they could get better service from a different provider. This roaming capability is important for devices that move between countries, and also for fixed location devices that may be used in an area with periods of service unavailability, often indoors.

Some technical standardisation work has been done to enable such services, with some of Apple's latest iPads including SIMs that make it easier for users to switch between mobile networks, while SIM supplier Gemalto is supplying reprogrammable SIMs for smart watches. The first steps have been taken in the Netherlands, which in 2014 allowed SIMs to be issued by organisations other than mobile network operators, such as utilities and car companies. The GSMA has developed standards for remote M2M device management, which are being supported by mobile operators including China Unicom and Telefónica.

Greater flexibility and competition would be possible if large IoT operators were able to act similarly to mobile virtual network operators – not least because they could then have wholesale access to mobile networks.[6] The German regulator, Bundesnetzagentur, consulted on the market for international mobile subscriber identifiers (IMSIs) in late 2014. An OECD analyst estimated that if German carmakers were able to issue their own SIMs and rent spare capacity on mobile networks, they could save $2.5 billion a year through lower prices and more flexible contracts.[7] The Belgian communications regulator BIPT is also consulting on the national number plan.

The electronic communications committee of the European Conference of Postal and Telecommunications Administrations (CEPT) has recommended that SIMs whose IMSI can be remotely updated should be implemented as soon as possible, and that CEPT countries consider more flexibility in assigning mobile network codes (MNCs) to IoT service providers. It has also encouraged ITU-T to consider updating recommendation E.212 to allow this flexibility, as well as to plan for the future use of MNCs to support a broader range of services. These changes have been under consideration in ITU-T study group 2.

ADDRESSING AND NUMBERING

To date, IoT devices may have a globally unique and routable communications address (requiring a very large protocol address space, such as that of IPv6); an address assigned by a gateway that allows limited inter-network connectivity; or make use of local networks only, to share data with and receive instructions from a nearby controller, such as a personal computer, smartphone, or specialised management device – in which case a globally-unique address is not required.

Enabling peer-to-peer connections between devices can increase the reliability of communications, rather than requiring a large and complex global network, and matches the common 'use case' of an individual discovering and interacting with nearby devices. But where devices must be globally reachable – most likely, via the internet – a large address space is required to individually identify each one.

> **The transition to IPv6 has taken longer than expected and may need encouragement.**

The number of unallocated addresses for the current version of the internet protocol (IPv4) is extremely limited, but the new version (IPv6) being rolled out by ISPs around the world has enough addresses for almost any conceivable number of devices. The transition from IPv4 to IPv6 has taken longer than expected, and policymakers may need to continue with programmes to encourage the transition in the medium term. The US government, for example, set up a federal IPv6 task force to move all federal agencies from IPv4 to IPv6, with one aim being to encourage the private sector to do the same. Other countries have also set up IPv6 task forces to encourage national transitions.

For any IoT identification scheme, there will be trade-offs between performance, scalability, interoperability, efficiency, privacy preservation, ease of authentication, reliability, flexibility, extensibility, and mobility support. As well as IPv6 addresses, the other main identification standards being developed are from ISO and GS1, as well as ITU-T recommendation E.212 for the use of IMSIs for machine-to-machine communications. The latter has the advantage of a well-developed authentication, payment and global roaming framework, operated by mobile telephony providers, with hardware security based on SIMs.

The ITU-T E.164 telephone numbering plan remains relevant for IoT. Applications using public networks, particularly mobile networks, will require E.164 numbering in the short to medium-term and will provide a bridge to an all-IP solution in the longer term. The European Communications Office (at CEPT) has noted that there is continuing demand for telephone numbering resources for vending machines, smart meters and in-vehicle communications modules.

COMPETITION

IoT technologies will likely have a range of impacts on the competitiveness of different markets. In the short term, firms adopting IoT systems will have better information on their business processes, enabling an increase in efficiency and more flexible responses to supply, processing and demand shocks. This could strengthen the market position of larger firms that have greater access to capital (to build their own IoT infrastructure) or brand loyalty (to increase sales volume to cover the price of third-party IoT services).

For products with 'network effects', greater sales volumes can increase the likelihood of consumers being locked into existing suppliers – especially if the supplier uses non-standard interfaces and sells complementary services. (Network effects are where the purchase of a product increases its value to existing purchasers – eg. a telephone service, where a new customer can call and be called by all existing customers.)

Over time, if IoT technology is adopted in ways that require high capital spending, increase firms' pricing power, or strengthen network effects, then adopters can drive out competitors. Market structure will also be affected if large companies can build their own IoT systems but smaller companies have to subscribe to them, or connect to networks of larger firms. If a core of large businesses adopts IoT, this could increase competition between them while reducing competition between core and peripheral firms. This could benefit consumers by turning quality based competition into price competition. But if firms feel they have to adopt IoT simply because competitors have, this could lead to overinvestment by incumbent firms and reduced entry into those markets by firms not willing to make this investment.[8]

The terms on which IoT service providers can access customers across the public internet will have a significant impact on their ability to enter new markets. Baseline access could be protected by network neutrality rules from regulators in the US, EU and elsewhere. IoT users with very high bandwidth or reliability requirements may be affected by neutrality rules that limit the ability of telecoms companies to discriminate between internet data from different sources. Such rules usually still allow telecoms providers to offer such customers 'specialised services' with specific speed or reliability guarantees. The terms attached to such services will be a key area of review for telecoms and competition regulators.[9]

In the longer term, an important aspect affecting competitiveness of IoT systems is the extent to which end users can gain access to the raw data gathered and stored by components. Systems usually process sensor data so that it is more useful when presented to users. While this makes systems more user-friendly, it reduces the ability of users to transfer data to different providers if a better service is offered. It also makes it more difficult for users to combine systems from different providers – which could become a competition issue if a provider becomes dominant in one area, and tries to extend that dominance into other areas by blocking interoperability with competitor systems.

One example of regulatory activity to promote competition is in Korea, where the government's telecoms strategy council has been given responsibility to adapt existing laws and regulations to ensure a liberal and competitive industrial environment for IoT. Where the council finds regulations that hinder ICT convergence, it can

POLICY AND REGULATORY MEASURES

What?	Why?	What is done today
Licensing and spectrum management	Ensure spectrum is available for a wide range of IoT applications, at short and long range, in licensed and unlicensed bands.	Monitoring availability of spectrum for short and long-range IoT communications and backhaul network capacity, and encouraging 4G deployment and use of small-cell technology.
Switching and roaming	Standard mobile telephony network SIMs and accounts are unsuitable for large M2M users, and mobile and fixed devices in areas of poor reception.	Mobile network operators are developing M2M-specific business units with appropriate billing and management. Further development and deployment of embedded, remotely provisioned SIMs in M2M systems.
Addressing and numbering	Very large address space is needed for globally addressable things.	Deployment of IPv6 by ISPs, public and private sector organisations. Use of IMSI for M2M applications.
Competition	Some market configurations of IoT services could strengthen position of large firms and increase potential for consumer lock-in. Limited user access to raw IoT data reduces ability to switch providers (and to understand privacy implications).	Ensuring competition regulators have capability to monitor IoT markets for abuses of dominant positions. Providing institutional mechanisms for ongoing review of laws and regulations for impact on IoT competitiveness.
Privacy and security	Security vulnerabilities in IoT systems let attackers access private data and cause physical harm in cases such as medical devices and connected vehicles. Many IoT companies have little internet security expertise. IoT device resource and connectivity constraints make security and vulnerability patching more difficult. Smart city vulnerabilities can be hard to fix but present significant safety issues (eg. in traffic lights). Innocuous sensor data can be linked together to create detailed individual profiles, and used to infer sensitive personal information, such as medical disorders. This may lead to discrimination in employment, and in financial and healthcare services.	Ensuring security and privacy from the outset of IoT system design processes. Development of co-regulation by all stakeholders to protect security and privacy. Further development of privacy and consumer protection rules to ensure security testing of IoT systems that process sensitive personal data.

request that related ministries improve these regulations. For new products and services, attention will be given to prompt processing and interim licensing.

At this relatively early stage of IoT market development, it is not clear whether the market will support more than a relatively small number of very large players, as is the case with existing internet markets such as search and advertising. Competition regulators will need to keep under review whether ex-post investigations of abuse of dominant positions will be sufficient to foster a competitive market and rapid innovation, including the ability of entrepreneurs to create new products and services.

PRIVACY AND SECURITY

Privacy and security are two significant (and closely related) issues in large-scale IoT deployment. There are already technologies available that address some of the underlying technical issues, particularly in sensors, such as key diversification and reader authentication. But these can have a significant impact on device size, cost, functionality and interoperability.[10]

Without adequate security, intruders can break into IoT systems and networks, accessing potentially sensitive personal information about users, and using vulnerable devices to attack local networks and devices. This is a particular issue when devices are used in private spaces, such as individuals' homes, for example with baby monitors. The operators of IoT systems, and others with authorised access to the data produced, are also in a position to "collect, analyse, and act upon copious amounts of data from within traditionally private spaces".[11]

Electronic attacks could also lead to threats to physical safety, for example if carried out against medical devices such as pacemakers and insulin pumps, or car engines and brakes. Information about building occupancy could be used by burglars to target unoccupied premises, while location-tracking data might enable physical attacks against specific individuals.

If compromised IoT devices can connect to systems elsewhere on the internet, this provides a potential route for further attacks. One security company announced in 2014 it had discovered hundreds of home devices – including smart fridges – sending unsolicited email. While a further analysis found this to be inaccurate, it also warned of recently discovered malicious software targeting Linux-based IoT devices.[12] Another common security and privacy issue is the use of default passwords on devices, which users are not required to change when setting up a device. One website has claimed to have found 73,000 webcams accessible over the internet using a default, known, password.[13]

IoT devices can be harder to secure than personal computers. Many companies building IoT devices do not have previous experience of dealing with internet security issues in their products. IoT devices are often inexpensive and resource-constrained (notably on power and battery life), which puts strong pressure on security costs and additional hardware or software to deal with threats. Combined with the limited internet connectivity of some devices, this may make it more difficult to develop and apply regular security patches when vulnerabilities are discovered – and for companies to afford ongoing support.

Most IoT devices contain multipurpose computers and can be reprogrammed beyond their intended purpose – with limited mechanisms for users to monitor the device. And they frequently share operating systems, embedded chips and drivers, meaning that a single vulnerability can often be used to attack a wide variety of devices.[14]

> **"Many companies building IoT products do not have internet security experience."**

In large IoT systems such as smart cities, IoT insecurity can create significant vulnerabilities, and be extremely complex to address given interdependencies and links to older public and private sector systems. One threat assessment found 200,000 vulnerable traffic control sensors in cities such as Washington DC, New York, Seattle, San Francisco, London, Lyon and Melbourne. The assessment also found such vulnerable technologies being developed and used in critical infrastructure without security testing, and that it can be difficult for third-party security researchers to gain access to devices to carry out their own tests, due to their expense and limits on sales to governments and specific companies.[15]

Companies developing and operating IoT systems will need to conduct security testing, and consider how security vulnerabilities discovered after devices are sold can be fixed during their likely lifetime. Where security flaws cause consumer harm, consumer protection agencies may be able to take action to require that those harms be remedied, and better security processes be put in place to reduce the risk of them recurring. EU rules require organisations processing personal data from IoT systems to carry out security assessments, and make use of relevant security certifications and standards.[16] And companies need to ensure that where they use external service providers to manage IoT devices and data, those providers also take reasonable security precautions.

To meet these security and privacy challenges, regulators have suggested that companies developing IoT devices should follow a security and privacy 'by design' approach, building security and privacy functionality into the device from the outset of the development process, when it is much more likely to be effective.[17] The 2014 international conference of privacy regulators declared that this "should no longer be regarded as something peculiar. [It] should become a key selling point of innovative technologies." An example of this type of functionality is the ability of users to deactivate or disconnect devices from networks.

That said, there is so far little evidence of market demand for privacy friendly services – partly because of the difficulties for individuals in assessing and weighing up complex privacy risks. And while regulators have been discussing privacy by design for over a decade, the specifics of implementation have so far only been developed to a limited extent.[18] Companies can undertake privacy impact assessments when designing IoT systems to consider how different design options have different privacy effects. This can also reduce the risk of the need for expensive delays and redesigns of systems that are found to be non-compliant with privacy rules – as was debated during the development of the Netherlands' smart meter programme.[19]

A significant amount of work has already been done on security and privacy issues by policymakers and regulators in the EU and US. Under the general data protection regulation now given the green light by the European Parliament and Council of Ministers, there will be stronger regulatory incentives for companies developing systems that process personal data to protect security and privacy by design. The FTC also suggests companies follow a 'defence in depth' approach, considering security measures at several different points in their systems, such as using access control measures and encrypting data even when users are making use of encrypted links to home WiFi routers (which will not protect data between the router and the firm's servers, or if the router is badly configured).

Privacy is a particularly strong regulatory issue in European countries, where it is included in a comprehensive legal framework that includes the Council of Europe's European Convention on Human Rights and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the EU Charter of Fundamental Rights. This framework has been influential in the development of comprehensive privacy laws now in force in over 100 countries around the world.

The EU already has a very detailed legal framework regulating the public and private sectors' use of personal data, with the Data Protection Directive (95/46/EC) relevant to IoT device manufacturers, social media platforms and app developers that access IoT data; and an e-Privacy Directive (2002/58/EC) also relevant to IoT device manufacturers. The European Commission has sponsored a process to create an RFID privacy code of practice, developed collectively by industry and civil society and approved by the EU's data protection authorities.

These authorities have issued a detailed opinion on the implications of IoT for privacy protection. They note that IoT produces high-volume flows of personal data that could present challenges to traditional data protection regulation – for example, individuals will not necessarily be aware when data is shared, or be able to review this data before it is sent to other parties, creating a risk of self-exposure and lack of control.[20]

A further privacy issue is the amount of personal information that can be derived from seemingly innocuous sensor data, especially when it is combined with user profiles and data from other sources. As European privacy regulators note: "Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed." Smart meter data, for example, can be surprisingly revealing of individuals' day-to-day activities – even which programmes are being watched on a television.

Researchers have found that smartphone sensor data can be used to infer information about users' personality types, demographics, and health factors such as moods, stress levels, smoking habits, exercise levels and physical activity – and even the onset of illnesses such as Parkinson's disease and bipolar disorder.[21]

This kind of information has obvious applications, such as in pricing health insurance, but also for other decisions related to employment, credit and housing. This could lead to economic discrimination against individuals classified as poor credit and health risks, and potentially to "new forms of racial, gender, or other discrimination against those in protected classes if IoT data can be used as hidden proxies for such characteristics".[22]

To protect individuals' privacy, the FTC has suggested that notice and consent be required when personal data is collected by IoT applications outside the reasonable expectation of consumers, based on the context of transactions and companies' relationships with consumers. Similarly, the EU data protection authorities have noted that IoT data collected for one purpose may be analysed and matched with other data, leading to a range of secondary purposes – which should be compatible with the original purpose of collection and known to the user (this is known as purpose limitation).

IoT data collection and analysis could particularly affect privacy when it includes data from private spaces like homes and cars, and even make it difficult for individuals to go about their daily life in the largely anonymous way they took for granted. When IoT applications process personal data that can reveal sensitive data under EU data protection law – racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life – explicit consent is required from the individual concerned. Under EU law, individuals must be able to withdraw their consent to all or specific data processing at any time, without "any technical or organisational constraints or hindrances" using tools which are "accessible, visible and efficient".

POTENTIAL REGULATORY MEASURES

Licensing and spectrum management	Further experimentation with use of white space and shared-space technology. Encourage development of LTE-A and 5G networks, and keep need for IoT-specific spectrum under review.
Switching and roaming	Global agreement on updated E.212 standards, making appropriate use of GSMA standards, and provision of mobile network codes to IoT service providers.
Addressing and numbering	Universal IPv6 adoption by governments in their own services and procurements, and other incentives for private sector adoption.
Competition	Consider measures to increase interoperability through competition and consumer law, and give users a right to easy access to personal data. Support global standardisation and deployment of remotely provisioned SIMs for greater M2M competition.
Privacy and security	R&D on more hardware and software security and privacy mechanisms for resource-constrained IoT systems, particularly targeted towards startups and entrepreneurs who lack resources to easily develop this functionality. Incentives for companies to develop new mechanisms to improve transparency of IoT personal data use, and for gaining informed consent from individuals concerned when sensitive data is gathered or inferences drawn. Greater use of privacy impact assessments by organisations building and configuring IoT systems. Development of further guidance from global privacy regulators on application of the principles of data minimisation and purpose limitation in IoT systems. More cooperation between telecoms and other regulators such as privacy/data protection agencies.

A range of mechanisms could be used to obtain consent, including choices at point of sale or device setup; QR codes or barcodes on a device that could take a user to a website; privacy dashboards, for example in smartphones; and by learning from consumer behaviour, such as through privacy preferences set on other related devices.

Data minimisation remains an important privacy-protective principle for consumer IoT devices, limiting the amount of personal data collected or retained, and hence reducing risks from data breaches and use of the data in ways not expected by consumers. The FTC foresees more flexibility for IoT services in collecting data not initially required to provide a service, while under stricter European rules the EU data protection authorities "cannot share this analysis".[23]

IoT mechanisms to protect individual security and privacy will also be useful to protect sensitive corporate information. The information that will flow from IoT-enabled production and logistics processes, for example, could provide strategic value for industrial competitors and at a national trade relation level. Further technical tools and regulations relating to trade secrecy may be required to protect such data.

CONCLUSIONS

While it is difficult to make precise forecasts about the global impact of IoT, analysts are almost unanimous that it will be extremely significant – with tens of billions of devices deployed, and trillions of dollars of annual impact within the next decade. IoT technologies could make an important contribution to global challenges such as improving public health and quality of life, moderating carbon emissions, and increasing the efficiency of a range of industries in developed and developing nations.

The pace of IoT deployment will partly depend on the development of cheaper, more reliable, well-connected systems. Common networks, technical standards, system components, and infrastructure, as well as strong public-private partnerships, can reduce the costs of IoT systems. Open data and platforms can make it easier for new systems to be developed, especially by entrepreneurs, startups and SMEs. Innovation centres and incubators can further encourage new businesses to enter IoT markets, increasing competiveness. Governments can take further steps to encourage national transitions to IPv6, updating all their own systems and providing incentives to private sector providers to do so, hence ensuring addresses are available for all IoT devices that connect directly to the internet.

Large-scale IoT systems like smart cities and international logistics chains need very cheap sensors that can last for long periods of time without needing repairs or new power sources, as well as the bandwidth to share data – whether infrequent bursts, or streams of high-resolution video. M2M systems need continued growth in coverage of 3G and 4G networks, and support for remotely provisioned embedded SIMs for more reliable and competitive communications.

This is the area where telecoms regulators can have the greatest impact, by supporting the continued development and deployment of high-speed cellular networks, and keeping under review the need for IoT-specific spectrum. Decisions on licensing and spectrum management are important to ensure IoT systems can be developed cost-effectively, and have the necessary bandwidth to communicate. By agreeing updated standards (such as the ITU's recommendation E.212) and providing mobile network codes to M2M service providers, better services could be provided at a significantly lower cost. Shared-space technology has the potential to offer much greater bandwidth for IoT and other communications services.

Common technical standards will be key to a low-cost, interoperable IoT, and can be encouraged by continued cooperation between standards bodies, and government support for standards use and participation. National and local government authorities can stimulate the availability of open IoT datasets, platforms and components. Municipal governments are playing a key role in smart city and open data programmes, and can find it easier to experiment with new technologies and policies than national governments.

Some countries are taking a relatively hands-off approach to IoT regulation, with the focus of promoting economic growth and innovation. For example, Korea has recently planned to reduce IoT (as well as e-commerce and internet finance) regulation to support a dynamic ecosystem for growth, while still protecting users, preventing abuse of market dominance and protecting internet networks, and will decide on which restrictions to maintain through social consensus. Other countries and regions, notably the EU, are taking a more proactive approach to protect social values such as privacy as the IoT develops, while still promoting the economic benefits.

Regulators can play a role in encouraging the development and adoption of the IoT, while promoting efficient markets and the public interest. Competition regulators will need to keep under review whether ex-post investigations of abuse of dominant positions will be sufficient to foster a competitive market and rapid innovation.

Particular attention will be needed from regulators to IoT privacy and security issues, which are key to encouraging public trust in, and adoption of, the technology. While many telecoms regulators already have responsibility for network security, this is an area where they could do more by cooperating with national privacy and consumer protection regulators to encourage development of a trustworthy IoT.

***IAN BROWN** is professor of information security and privacy at the Oxford Internet Institute. This article is adapted from a paper presented at the ITU's Global Regulators Forum. The author is grateful for comments by Rudolf van der Berg, Pierre-Jean Benghozi, Mailyn Fidler, Simon Forge, Ben Hawes, Gilad Rosner, and ITU staff.*

REFERENCES **1** European Commission (2013). Conclusions of the internet of things public consultation. **2** FTC Staff Report (2015). Internet of Things: Privacy and security in a connected world. 1.usa.gov/1XnX947 **3** FCC Technological Advisory Council. Internet of Things working group. See slides at: bit.ly/1SpsYTA **4** Master plan for building the internet of things (IoT) that leads the hyper-connected, digital revolution. Republic of Korea Ministry of Science, ICT and Future Planning, 8 May 2014, p4. **5** Schindler HR et al. (2013). Europe's policy options for a dynamic and trustworthy development of the internet of things. RAND Corporation. bit.ly/1SptvVz **6** OECD (2012). Machine-to-machine communications: Connecting billions of devices. bit.ly/10x71RD **7** The endangered SIM card. The Economist, 20 November 2014. econ.st/1LFGQ6x **8** Schindler HR et al. (2013). op. cit. **9** Marsden CT (2010). Net neutrality: Towards a co-regulatory solution. Bloomsbury. **10** European Commission (2013). op. cit. **11** Schindler HR et al. (2013). op. cit. **12** Thomas P. (2014). Despite the news, your refrigerator is not yet sending spam. Symantec official blog. symc.ly/1Q5fgpH **13** Tofel KC. (2014). Got an IP webcam? Here are 73,000 reasons to change from the default password. Gigaom Research. bit.ly/1EleYIm **14** Soltani A (2015). What's the security shelf-life of IoT? Tech@FTC blog. 1.usa.gov/1InZ4Er **15** Cerrudo C (2015). An emerging US (and world) threat: Cities wide open to cyber attacks. IOActive Labs white paper. bit.ly/1MpCIkL **16** Article 29 working party (2014). Opinion 8/2014 on the recent developments on the internet of things. p18. bit.ly/1smejQi **17** Mauritius Declaration on the Internet of Things (2014). bit.ly/1XAJdIi **18** See: Koops BJ and Levene R (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data protection law. International Review of Law, Computers & Technology 28 (2): 159-171; ENISA (2014). Privacy and data protection by design. **19** Cuijpers C and Koops BJ (2012). Smart metering and privacy in Europe: Lessons from the Dutch case. In: S Gutwirth et al. (eds). European data protection: Coming of age. Springer. **20** Article 29 working party (2014). op. cit. **21** Peppet SR (2014). Regulating the internet of things: First steps towards managing discrimination, privacy, security and consent. Texas Law Review 85: 115-16. **22** Peppet SR (2014). ibid. **23** Article 29 working party (2014). op. cit.

DEALING WITH DISRUPTION

As regulators start to fundamentally review their remits, **CHRIS CHAPMAN**, the incoming president of the IIC and chair of Australia's ACMA, details the extent of digital disruption and possible regulatory response, in this two-part article

Over the past ten years since the Australian Communications and Media Authority (ACMA) was created we have most certainly observed significant changes occurring in Australia's communications and media markets – in citizens' expectations of the way they interact with digital technologies, and changes in the type and scale of risks and harms experienced by all stakeholders – industry operators and citizens. The original challenge arising from the digitisation of content and carriage has been further compounded by the emergence of IP-enabled communications and content over the past decade.

These changes have been documented by our various tracking studies of market and technology developments and longitudinal studies of the Australian community's changing media and communications practices. We drew this work together in a strategic framework, presented in a recent paper.[1] For regulators to more fully address the challenges of digital disruption a different regulatory focus is likely to be needed. It must necessarily include a discussion about the breadth of industry and social activity that should form the focus of any revised regulatory framework or remit.

So what are the deep currents of change that confront us? When Thomas Friedman updated his book, *The World is Flat: A brief history of the twenty-first century*, he recounted how many of the things that were informing current debate had not been thought of in 2005 – the date of the first edition and the year the ACMA was established. He noted that:

- Facebook cannot be found under 'F' in the index of the first edition of the book
- Twitter was then a sound
- Cloud was something found in the sky
- 4G was a parking space
- An application was something you sent to college
- LinkedIn was a prison
- Skype was a typo.

In a 2015 tribute to Alan Rusbridger, who had for 20 years edited the UK newspaper, the Guardian, Emily Bell observed that:

"Twenty years ago was perhaps one of the most significant phases in modern communications as consumer access to the internet was in its infancy. Microsoft was just launching its first web browser (Internet Explorer), the

global penetration rate of mobile phone ownership was 1%, and the world's largest internet company was Netscape – valued at more than a whopping $5bn. Amazon was starting life as a bookseller in Jeff Bezos's garage, and Larry Page had just enrolled in the Stanford PhD programme where he would bump into fellow student Sergey Brin and write a thesis paper which became Google."

And of course, all this was brilliantly anticipated by that telecoms genius, Nikola Tesla, in 1926:

"When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."

The contemporary view is, for me anyway, neatly summed up by veteran Australian media and ICT observer, Tom Burton:[2]

"The digital era is still a work in progress, but what we are seeing play out is the combination of ubiquitous connectivity, powerful intelligent devices and an extraordinary web of software, driving applications and services. There has already been rapid and major disruption across the economy and history suggests that as connectivity improves and devices and software become even more powerful and intelligent, our world will continue to fundamentally change, in ways it is hard to predict. And if the pattern of previous disruptive technologies is repeated, this change will almost certainly be far more fundamental and profound than simply a new way of working."

To put it then at its most conservative, the pace of technological change refuses to slacken. In the past year or so alone we have seen the onrushing tide of innovation bring us the Apple Watch and other wearables, virtual reality viewers, 3-D printers that are also scanners, drones, the ultra-high-definition format (4K) for TV and gaming, very high-resolution screens on phones, and faster mobile networks. You can now buy a fast, high-end computer that fits in your pocket – the list goes on.

NATURE OF TECHNOLOGICAL CHANGE

For a more detailed look, the Pew Research Center (as part of a sustained effort throughout 2014 to mark the 25th anniversary of the creation of the web) looked at the future of the internet, the web and other digital activities. It canvassed 2,558 experts and technology builders about where we will stand by the year 2025 and found striking patterns in their predictions.[3] To a notable extent, these experts agree on the technology change that lies ahead, even though they disagree about its ramifications. Most believe there will be:

- A global, immersive, invisible, ambient networked computing environment built through the continued proliferation of smart sensors, cameras, software, databases and massive data centres in a world-spanning information fabric, the internet of things (IoT)
- 'Augmented reality' enhancements to real world displays that people perceive through the use of portable/wearable/implantable technologies
- Disruption of business models established in the 20th century (notably in finance, entertainment, publishers, education)
- Tagging, databasing, and intelligent analytical mapping of the physical and social realms.

The IoT is indeed currently a hot topic and deservedly so. It is not a novel concept; machines have been talking to machines at least since the start of factory automation and SCADA[4] protocols. However, there is now a palpable sense that we are on the threshold of another step change – that the environment of ubiquitous devices and constant connectivity is about to spread from the widely taken-for-granted smartphone world into the ambient world of devices and objects that surround us. And, of course, such a development potentially gives rise to a huge number of devices, colossal numbers of connections and generates stupendous amounts of data, much of it to be collected, analysed and further utilised.

From my own perspective, I suspect it will be a considerable while before we witness the massive form of the IoT. There are doubtless a number of things to be resolved before such a vision fully comes to pass. Standards must be settled, spectrum needs to be available, citizen and consumer worries and harms must be allayed and addressed, and market economics settled.

"Just because it can be connected, should it or must it be connected?" one might ask. For the ACMA, as one of the relevant regulators in the Australian context, and at this stage in the development of such a potentially transformative technology, the most sensible thing we can do is to play a facilitative role so that the market can find and test its own propositions for this space. In other words, to either resolve impediments to development of potential uses where we can, or to stay out of the way, by forbearing to weigh in with regulatory interventions where they may be feasible, but will probably be of marginal utility or, indeed, be counterproductive.

> **We must remain enagaged but resist the temptation to indulge in regulatory activism.**

Which is not to say that we should abandon our remit to protect the public interest where it may be materially threatened. To detect and differentiate such eventualities we must therefore remain engaged and watchful, but resist the temptation to indulge in regulatory activism.

Put another way, one might ask, "What might be the 'killer app' for the IoT?" As a writer in Quartz put it:[5]

"The internet of things's disruptive potential has been deathly slow to realise, in large part because the commercial landscape is not ready for it. Much of the delay resides in linking the vast islands of digital data from sensors and applications to an information highway, primarily wireless technologies. Those of us involved with intelligent industrial products working toward integration for IoT opportunities repeatedly face what we term 'last' challenges ... for example, 'last mile' deployments to extend cellular infrastructure, the 'last hundred metres' to connect sites, 'last rooms' referring to wireless dead spots and even the 'last square mile' when investigating satellite coverage of oceans and deserts. In each case, the world lacks ready solutions to make that 'last link'."

In the home automation field, for example, a developer may sort through as many as a dozen alternatives to complete their 'last' links, including prominent alternatives such as WiFi, Bluetooth or LTE, to less familiar ones like ZigBee or Z-Wave. But with little incentive to innovate these last links, each of the currently available options typically falls short on at least some dimension. And in addition to this home networking issue, we can find comparisons or perhaps early examples of trying to network things in the evolution of smartcards and various payment systems such as NFC (near field communications).

Nevertheless, I certainly acknowledge that the market will keep throwing up propositions for consumers and industry (and perhaps the regulator) to test. One such proposition to which I give some credibility is the notion of 'My internet of things'. In this scenario, the smartphone acts as the gateway to the collection of connected devices related to an individual, giving them access and appropriate control of devices in their personal 'ecosystem'. Smartphones have the apps and computing power to resolve different protocols and pull together data from 'the (multiple) things' of different vendors in the device of the consumer, and perhaps then to share relevant data with selected intermediaries on a permission basis. To all intents and purposes, the smartphone user is then running their own IoT. And for this, mobile broadband will be an essential ingredient, as well as various other modes of wireless communication.

FORCES OF DISRUPTION

The IoT and other developments such as those chronicled above by Pew Research are unleashing what is often discussed as 'forces of disruption'. Catherine Livingstone, chair of Telstra, Australia's major telco, put it this way in a recent address:

"At the heart of this disruption is connectivity. Mass connectivity. This connectivity has enabled human generated data, and now machine generated data, to flood through our global networks of fibre and copper. Combined with orders of magnitude increases in computing power, what and who is possible to know is almost limitless. And in real time. We thought that the connectivity enabled in the mid-1990s by the fixed line internet and browser technology was disruptive; that was before 2007, when the mobile internet became a reality with the first smartphone. But that is nothing compared with the disruption we will see with the advent of the internet of things."

There are a number of other ingredients feeding into the mix headlined by the IoT – cloud computing, 'deep learning' algorithms fed by big data, the smart devices in the hands of citizens and the connectivity platforms which support disruptive business models currently storming many established industries.

Netflix choice in Germany: the firm is going after global scale

Research firm Frost & Sullivan put it this way:[6]

"Convergence and connectivity is disrupting, transforming and collapsing industries, redefining the future of business and how executives will manage companies in the future. The interplay between cloud computing, mobile technology, big data and the internet of things is driving the surge in digital transformation and rapidly accelerating the pace of connectivity and convergence across all industries, radically changing lives; transforming the way we work, relax, learn and manage our health."

A news item about Greg Baxter (the Australian technologist who is leading Citigroup in its digital battle) caught my eye.[7] Because, in his view, artificial intelligence, robotics, big data, and exchanges like Bitcoin and peer-to-peer lenders, are all emerging as serious prospects, he wanted to capture the serious attention of senior Wall Street colleagues. "*So he presented Citi executives in New York with a financial analysis of incumbent business models in the music, video, travel and media industries that had been turned upside down by digital disruption*." Presumably so that the bank's approach to risk is much better attuned.

This is a space the ACMA knows well, and a pace it is also adjusting to. For the past decade, we in the communications and media industries have become almost accustomed to the constantly renewing cycle of technological change underlying the business models of previously well-established industries. By and large, however, these have been the information industries, which have been transformed into shapes and forms that are often essentially unrecognisable as their former selves. I am thinking of the obvious examples of encyclopaedias, recorded music, book retailing, voice telephony, newspapers. BrandData, a daily ranking index services, has reported that Australia's top six bloggers now have a larger combined audience than the highest-selling magazine, newspaper and TV programme collectively.

Streaming video (which has made a somewhat belated appearance in Australia with the recent entry of Netflix) is putting significant pressure on free-to-air and subscription broadcast television. The then Channel Ten CEO, Hamish McLennan, commented on the challenge for local broadcasters from tech-media startups and offshore online video competitors:

"The vast majority of all video consumed today on any device is broadcast quality content. We need to look at redefining the industry. The headlines are so wildly exaggerated about the death of television or that TV is dying. It's just not the case. People are watching as much TV as they have ever done but they're doing it on many screens and devices so it just opens up the opportunity to redefine TV."

He noted that to justify their valuations, the new media outfits are going after global scale – and local publishers and media need to prepare for this. He said, *"Our competitive set is not a seven, nine and ten play anymore. We have to compete with overseas technology companies, so our universe is much larger than ever before."*

We are now familiar with over the top (OTT) services such as streaming video and voice over IP telephony and how they are disrupting or have disrupted established players such as broadcasters and telcos. I have found it interesting how smart devices in consumers' hands can allow them to step completely out of the established communications system. For example, 'mesh networking' allows users to communicate wirelessly by bouncing a message from one phone equipped with FireChat (within 210 feet of them) to another via WiFi or Bluetooth antennas and so allows them to send and receive text messages entirely without mobile data or the internet. The encrypted message then keeps bouncing from phone to phone without touching carrier or ISP networks, thus avoiding costs and usual interception methods, until it reaches the intended recipient. The creators of the FireChat app estimate that as long as 5% of a city's population has it, messages can be delivered in around ten minutes. While originally designed for people to get in touch with each other at crowded events, FireChat apparently became hugely popular in Iraq last year, after the country faced internet use restrictions, and was an integral part of the 2014 Hong Kong and 2015 Ecuadorian protests.[8]

At a micro-level, this confirms the paradox in the contemporary world of networks that the distinctions between layers are not quite the 'bright' lines we may have optimistically ascribed to them five or so years ago. While the notion of layers is useful to aid our navigation and understanding of the networked world, they are not themselves new, inviolate touchstones. Today's network layers (let alone how those in the future seem to be shaping) are not, as the engineering origin of the concept might suggest, neat and clearly delineated functional constructs. They are instead increasingly permeable, interconnected and virtualised, meaning that much of what functions as 'infrastructure' is software defined, and many content layer applications can deliver an 'infrastructure-like' connection or service.

IMPACT ON THE 'REAL WORLD'

Broadly speaking, the disruptive changes of digital transformation to date have involved industries of the 'virtual' world of media and communication, where information is the key ingredient. Certainly over the past few decades ICT capability and innovation (mainframes, then networks of smaller computers and the internet) have transformed other more 'physical' established businesses. However, while of course banking, insurance, manufacturing and mining have all been changed, generally they have not been to date fundamentally disrupted and remain recognisable as banks, insurers, factories and mines.

My proposition is that we are now arriving at the point of witnessing digital disruption bringing irreversible effects into the 'real' world, the world of banking, insurance, manufacturing and perhaps even mining.

Ray Kurzweil, a pioneer of computer science, likes to talk of "the second half of the chess board". On the second half of the board not only has the cumulative effect of innovations become large, but each new iteration of innovation delivers a technological jolt as powerful as all previous rounds combined (it's from the old fable about doubling grains on each successive square).[9]

As Kai Riemer, associate professor at the Digital Disruption Research Group at Sydney University Business School, puts it:[10]

"Disruption is much more of a profound thing than just the launch of a new app or a new technology coming into market... Disruptive change is path-breaking change. It is not a linear extrapolation of the past, it is not a change that we could predict."

Perhaps some of the disruptions we currently see around us are the signs that the 'real world' jolts from ICT innovation in a real sense have only just started. Tom Goodwin is clearly onto something when he notes that:[11]

> **Each iteration of innovation delivers a jolt as powerful as all previous rounds combined.**

"Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate. Something interesting is happening."

The new breed of companies are the fastest-growing in history. Uber, Instacart, Alibaba, Airbnb, Seamless, Twitter, WhatsApp, Facebook, Google: These companies are indescribably thin layers that sit on top of the vast supply systems of others (where the costs are) and interface with a huge number of people (where the money is). This gives rise to what some have termed 'Uber-isation', a phenomenon that Kai Riemer (while he does not use the term) describes thus:[12]

"Uber, Airbnb, none of them own the actual assets that deliver the service, but they are disruptive because they are better at orchestrating the information flow, therefore reallocating risk and suppliers and appropriating rent from this game. They turn physical into digital industries."

The value is in the software interface, not the products, or as Catherine Livingstone suggested, in the connections and connectivity. An illustration is Aerosolve, a tool used by Airbnb to help people figure out the best price for their Airbnb rooms and apartments. It synthesises a variety of factors and data items to suggest a nightly room charge and uses 'machine learning' algorithms to get smarter over time. Airbnb has released Aerosolve as a free download for developers to build into their own apps, presumably with the aim of connecting even more customers, and therefore consolidating Airbnb's position in the market.

This fundamental shift and threat to established business models is again vividly illustrated in the world of finance. JP Morgan CEO, Jamie Dimon, warned in his annual letter to shareholders that startups are coming for Wall Street, innovating and creating efficiency in areas that are important to companies like his bank, particularly in lending and payments.[13] And, I would add, you can insert the