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
**news from around the globe**

**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.

**spectrums**

**wrc-15 balances tv and mobile**

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

**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 last the 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/1mLAc7

**data protection**

**smart cities 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, which is not just the case if the presentation is “natural”. The FTC has published a guide to help businesses comply.

**advertising**

**fcC rules for converged services**

The US FCC has relaxed rules on local phone companies that require them to offer local and long-distance services, provided that alternatives are offered and small and rural customers are protected.

**berEC meetings**

BNetzA, the German regulator, 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/l3aGU

**events**

**10-11 February, Geneva**

**EBU Digital Radio Summit**

**22-25 February, Barcelona**

**Mobile World Congress**

**18-17 March, Brussels**

**IIC Telecommunications and Media Forum (TMF)**

**2-4 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 at a glance”, which includes the most recent national data for 213 economies on key indicators of ICT including access, quality, affordability, efficiency, sustainability and applications.

**fcC relaxes rules**

The US FCC has relaxed rules on local phone companies that require them to offer local and long-distance services, provided that alternatives are offered and small and rural customers are protected.

**berEC chairs**

Sébastien Sorio, 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 Escher, 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.
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.

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 2014 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’ – he believes 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 seasaw’ – 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 interfere 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 takeup 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 underwrite a $1 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 decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade. McKinsey gives a spread of $4–11 trillion, but whatever it turns out to be, seizing this decade of IoT 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 entrants 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.

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, and that 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 sites 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 called Aquila, and there 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 Blance, Telefonica’s global policy and regulatory affairs head, first described the way telcos are now competing with internet players as part of ‘a single universe’, but the internet is also changing, from a domain that used to be a public service to a domain that is more commercial, he said. In licence terms, he noted, it can lock in inefficient use of federal spectrum.

In the US, much of what the FCC wants to achieve is happening, such as rapid growth in cheapest reached markets. In China, there is no key for many reasons. When cable TV was first regulated in 1992, it owned 98% of pay TV — now that’s 53%; “Don’t regulate for regulatory sake but recognise it is a market in extreme flux — focus on modernising the regulatory approach,” she concluded.

Julius Fritz, from One Media, a new TV broadcast platform, asked how you would judge what has more value – a one-time licence fee, or a roaming fee from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, 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 is the future may be from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, Julius Fritz, from One Media, a new TV broadcast platform, asked how you would judge what has more value – a one-time licence fee, or a roaming fee from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, 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 is the future may be from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, 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 is the future may be from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, 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 is the future may be from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, 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 is the future may be from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, 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 is the future may be from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, 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 is the future may be from many IoT devices not just cell towers, which will be a further policy challenge. And coordinating global spectrum, 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.
INTERNET OF THINGS
Panelists on the IoT session chimed in with a number of introductory thoughts. Ericsson’s Bruce Gustafson noted there are two camps – a communications mindset that focuses on creating a network 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.”

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 industry, 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 many, the response to 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 IoT. Operators 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. For IoT, there will be questions about whether cellular networks can accommodate traffic, and perhaps operators will spring up to support certain applications in cities. An important issue is deskillung and automation – as connected devices become more prevalent, people may lose skills.”

Aaron Buzi, 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 all the new technologies involved. “As examples, he said consumers should still know about what sorts of data are being collected and how it will be handled, and other agencies’ 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 the rise 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 of mobile operators’ networks will be video, Pepper added.

As an aside he said: “There’s no such thing as a mobile network – what we’re really talking about is data transport.” 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 5G will lead to ultra high definition which will drive more data traffic. As for devices, by 2019 43% of connections will be machine to machine (M2M) but will only be 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 are likely to 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 International 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 the hack of Sony in response to the film about North Korea, which she said was beneficial applications such as in farming. For example, the response to 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.

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 – the session asked the question, “What do citizens want from their regulator?” There was comment that telecom 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 – the session looked at the rapid multiplication of content, protection v free speech, ‘must carry’ vs alternative content, identity, and linear vs non-linear.

Digital divide – regulators shared plans that address supply and demand, 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 plans that address supply and demand were highlighted.

SDGs and the WSS Review – A workshop by the ITU, the IC and Microsoft (see page 14).

2016 Vol 43 Issue 4 InterMEDIA 9

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

Countries could miss out on the economic benefits of IoT in sectors such as manufacturing, energy and healthcare.
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 telecommunications 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, specialized 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 privatization 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 privatized and a new legal framework was being discussed and I was fortunate enough 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.

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 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 Alcentra, 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.

Q: HOW ARE THE IFT COMMISIORS ORGANIZED?  
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 30 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 all applying for sharing 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 who 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. 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 broad neutrality principles in our new telecoms act.

Q: FINALLY, WHAT ARE YOU KEY AISMS?  
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, with professional and expert in our field, and the best regulator and competition authority in our region.
**Q** WHAT IS YOUR BACKGROUND?

A I’m from Colombia, where I obtained degrees in economics and law. I’ve worked in the office of the actual 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 Fido 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 has its eyes on 4G 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 its 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.

**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’s really a matter of being smart about what network delivers what bit, to what subscriber, at any point in time.

**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 propositions 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% on the demand side, we will see 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 DO YOU ADDRESS BOTH SUPPLY AND DEMAND AT MILlicom?

A As I said, this is a business where money gets poured into the first, which we’ve done, but reducing the cost can be done with sharing – in Colombia we’ve built a 4G network with Telefonica 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 topups, 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 reform 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 government investment. As an investment challenge, governments that abolish say VAT on handsets can help greatly in the connectivity drive.

**Mauricio Ramos, CEO of Millicom**

---

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

---

**WWW.iicom.org**

**www.iicom.org**
The internet and advances in information and communication technologies (ICT) have revolutionised our lives – the way we fund 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 important socioeconomic factors. In 2000, only 6% of the global population had internet access.7 By 2015, that number had gone from 9% to 43% of the population in 2015.7

The internet and advances in ICT have transformed the 95% of businesses in the world which depend on proprietary applications globally, democratising access to technological innovations. Cloud computing builds networks that serve as a platform for other applications, transforming the competitive landscape and enabling IT-enabled SMEs to increase efficiency at lower cost.8

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 revenue 15% faster and create jobs almost twice as fast as other SMEs.9

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 productions by 70% by 2050 to feed an estimated population of 9.6 billion people, while also addressing the anticipated challenges 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 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 principle of the Charter of the United Nations and respecting fully and upholding the Declaration of Human Rights’.10

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 2015.4

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.6 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 lessons 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 2030.6 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’.4 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 consensus into action. This was a seminal document that reaffirmed 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.

The review process officially began in June 2015, when ambassadors Janis Mazeiks, permanent representative of the Republic of Latvia to the UN, and Lana Nussel, permanent representative of the United Arab Emirates to the UN, were named by the president of the UN General Assembly as the cofacilitators to lead the intergovernmental negotiation and create a preparatory process to produce the final outcome document. The cofacilitators created a process to integrate input from all stakeholders within the confines 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 dialogue 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 opportunity to create an academic context for the development of the information society. While the 2030 Agenda does not focus on ICT, the role of...
ICT in advancing the SDGs is recognised through mentions that technology and innovation are key in enabling a number of the SDGs and the WSIS action lines, giving examples of multistakeholder initiatives in enabling the SDGs and the WSIS action lines, as well as call for and challenges in sustaining such initiatives, development, and address cybersecurity capacity building as part of bridging the digital divide. Highlighted 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 Mazekis 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 to be forward-looking in how the SDGs action lines can help to realise such discussions. In the WSIS+10 review, 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:

**ADJUSTED INVESTMENT AND FUNDING** – this was a recurring theme during discussion. There needs to be greater focus on financial mechanisms that would not only break even and bottom-up approaches need to be combined and tailored to address and prioritise local/regional/investment needs. Participation of local/ public/private entities, local organisations and others all have a role to play. An enabling policy environment is also needed to incentivise and provide 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 PARTNERSHIP** – an ‘ecosystem of stakeholders’ was cited to present concerns in a number of implementation examples, and that “it is essential for stakeholders to work together to address and identify and 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 coordination of each other’s objectives, local communities and other stakeholders, we were able to deploy a solution that addresses real needs, reinforcing 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.

**SDGS AND 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** Establishment of competition
- **C7** ICT applications
- **C10** Ethical dimensions of ICTs
- **C12** ICT in development
- **C13** International and regional cooperation

**WSIS ACTION LINES**

- **C7** ICT in development
- **E1** Development
- **E2** Education
- **E3** Employment
- **E6** Environment
- **E7** E-government
- **E8** E-business
- **E9** E-learning
- **E10** E-health
- **E11** E-energy
- **E12** E-agriculture
- **E13** E-trade
- **E14** E-competition
- **E15** E-safety
- **E16** E-environment
- **E17** E-employment
- **E19** E-learning
- **E20** E-business
- **E21** E-government
- **E22** E-employment
- **E24** E-medical
- **E25** E-shipping
- **E26** E-telecommunications
- **E28** E-energy
- **E30** E-competition
- **E31** E-safety
- **E32** E-environment
- **E33** E-employment
- **E34** E-learning
- **E35** E-business
- **E37** E-government
- **E39** E-employment
- **E40** E-learning
- **E41** E-business
- **E43** E-government

**How the SDGs map against the WSIS action lines**

- **SDG 1**: No poverty
- **SDG 2**: Zero hunger
- **SDG 3**: Good health and well-being
- **SDG 4**: Quality education
- **SDG 5**: Gender equality
- **SDG 8**: Decent work and economic growth
- **SDG 9**: Industry, innovation and infrastructure
- **SDG 10**: Reduced inequalities
- **SDG 11**: Sustainable cities and communities
- **SDG 12**: Responsible consumption and production
- **SDG 13**: Climate action
- **SDG 14**: Life below water
- **SDG 15**: Life on land
- **SDG 16**: Peace, justice and strong institutions
- **SDG 17**: Partnerships for the goals

**REFERENCES**

- 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.
Searching for the Creative Economy

IAN HARGREAVES

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 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.

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 multiregional, 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 Laban 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.

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 many 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: the third big project, was launched in 2012 and ran 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.

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 400 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 do this work when I became aware of Hasan Bakhshi’s collaboration with scholars in Australia, which aimed to provide a method to publish their work.

Manuscript

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

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

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: the third big project, was launched in 2012 and ran 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.

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 400 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 do this work when I became aware of Hasan Bakhshi’s collaboration with scholars in Australia, which aimed to provide a method to publish their work.

Manuscript

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

In five months Sandbox delivered as much as some publishers have done in five years.
measure the creative economy, defined as comprising the economic outputs of everyone who does a creative job, whetheranuts getting between us towards a powerful creative economy story which has, unsurprisingly, gathered even greater political salience. UK Prime Minister David Cameron mentioned ‘creativity’ as a key UK asset in the climax to his short victory speech on the steps of Downing Street in May. President Xi’s 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, and China and the UK are on a long march from a ‘made in China’ economy to a ‘created in China’ one. Check out the programmes of the world’s business schools and see how creative 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 explosive of collaborative possibilities opened up by the internet. The resulting DIY culture has learned its methods from open source software and usershaped 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 Moosk; a music and video platform created by young people in Bristol; and various communities in London facing challenges which are extended from planning and service development to empowerment of younger clients. What we found was that the principles of codesign 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 examples of innovation through innovation in terms of community media, community generated planning and development initiatives; creative expression, promotion and distribution; and community collaboration. We also constantly encountered the logistics of digital: the need to modify digital tools to meet the specific complexities and circumstance of individual places, and the balance to be pointed leadership and expertise on the one hand and inclusivity on the other.

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

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

Taken together, these four pieces of work and their surrounding literature may be better negotiated between us towards a powerful creative economy story which has, unsurprisingly, gathered even greater political salience. UK Prime Minister David Cameron mentioned ‘creativity’ as a key UK asset in the climax to his short victory speech on the steps of Downing Street in May. President Xi’s 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, and China and the UK are on a long march from a ‘made in China’ economy to a ‘created in China’ one. Check out the programmes of the world’s business schools and see how creative 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 explosive of collaborative possibilities opened up by the internet. The resulting DIY culture has learned its methods from open source software and usershaped 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 Moosk; a music and video platform created by young people in Bristol; and various communities in London facing challenges which are extended from planning and service development to empowerment of younger clients. What we found was that the principles of codesign 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 examples of innovation through innovation in terms of community media, community generated planning and development initiatives; creative expression, promotion and distribution; and community collaboration. We also constantly encountered the logistics of digital: the need to modify digital tools to meet the specific complexities and circumstance of individual places, and the balance to be pointed leadership and expertise on the one hand and inclusivity on the other.

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

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

Taken together, these four pieces of work and their surrounding literature may be better negotiated between us towards a powerful creative economy story which has, unsurprisingly, gathered even greater political salience. UK Prime Minister David Cameron mentioned ‘creativity’ as a key UK asset in the climax to his short victory speech on the steps of Downing Street in May. President Xi’s 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, and China and the UK are on a long march from a ‘made in China’ economy to a ‘created in China’ one. Check out the programmes of the world’s business schools and see how creative 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 explosive of collaborative possibilities opened up by the internet. The resulting DIY culture has learned its methods from open source software and usershaped 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 Moosk; a music and video platform created by young people in Bristol; and various communities in London facing challenges which are extended from planning and service development to empowerment of younger clients. What we found was that the principles of codesign 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 examples of innovation through innovation in terms of community media, community generated planning and development initiatives; creative expression, promotion and distribution; and community collaboration. We also constantly encountered the logistics of digital: the need to modify digital tools to meet the specific complexities and circumstance of individual places, and the balance to be pointed leadership and expertise on the one hand and inclusivity on the other.

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

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

Taken together, these four pieces of work and their surrounding literature may be better negotiated between us towards a powerful creative economy story which has, unsurprisingly, gathered even greater political salience. UK Prime Minister David Cameron mentioned ‘creativity’ as a key UK asset in the climax to his short victory speech on the steps of Downing Street in May. President Xi’s 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, and China and the UK are on a long march from a ‘made in China’ economy to a ‘created in China’ one. Check out the programmes of the world’s business schools and see how creative 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 explosive of collaborative possibilities opened up by the internet. The resulting DIY culture has learned its methods from open source software and usershaped 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 Moosk; a music and video platform created by young people in Bristol; and various communities in London facing challenges which are extended from planning and service development to empowerment of younger clients. What we found was that the principles of codesign 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 examples of innovation through innovation in terms of community media, community generated planning and development initiatives; creative expression, promotion and distribution; and community collaboration. We also constantly encountered the logistics of digital: the need to modify digital tools to meet the specific complexities and circumstance of individual places, and the balance to be pointed leadership and expertise on the one hand and inclusivity on the other.

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

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

Taken together, these four pieces of work and their surrounding literature may be better negotiated between us towards a powerful creative economy story which has, unsurprisingly, gathered even greater political salience. UK Prime Minister David Cameron mentioned ‘creativity’ as a key UK asset in the climax to his short victory speech on the steps of Downing Street in May. President Xi’s 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, and China and the UK are on a long march from a ‘made in China’ economy to a ‘created in China’ one. Check out the programmes of the world’s business schools and see how creative 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 explosive of collaborative possibilities opened up by the internet. The resulting DIY culture has learned its methods from open source software and usershaped 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 Moosk; a music and video platform created by young people in Bristol; and various communities in London facing challenges which are extended from planning and service development to empowerment of younger clients. What we found was that the principles of codesign 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 examples of innovation through innovation in terms of community media, community generated planning and development initiatives; creative expression, promotion and distribution; and community collaboration. We also constantly encountered the logistics of digital: the need to modify digital tools to meet the specific complexities and circumstance of individual places, and the balance to be pointed leadership and expertise on the one hand and inclusivity on the other.

6 The creative economy is almost 10% of the whole in the UK in terms of gross added value.
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 offers to sell 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 all a dedicated chapter 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 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 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 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 get more spectrum by buying 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, unfruit for the biggest challenge or so,” 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 it has been more successful in the US and Australia). Further, liberalisation does not lend itself to the growing interest in wholesale mobile network access, 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.

Back in time

Delving deeper into the past, a chapter describes how liberalising spectrum occurred long ago and how the ‘father’ of liberalisation, Ronald Coase, put the case for treating spectrum like any other commercial property (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 endpoint, where 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 control system. 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 in 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 usually only necessary to prevent interference. Just the very limited ones. It is said that liberalisation has not ‘had its day’ or been a failure, but has been disappointing in not being applied to broadcasting. 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.)

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 leading the way)
- Broadcasting (where digital terrestrial TV, DTT, is thriving in some markets despite its inferiority in technical terms to cable and sat of 1987 that 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)
- Broadband 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 unexploited, growing demand for mobile broadband – and (tongue in cheek) if so, can’t the liberalisers and technocrats decide? They add more on the obstacles to liberalisation, such as the need to address huge markets at global scale, the separation of incumbent operators 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, and where trading has been successful, in the US, networks are regional, 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 ministries’.

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 transmits when unoccupied and is used in 5GHz WiFi (shared with radar, for example). Dynamic spectrum access (DSA), which uses databases to determine location rather than sensing, is becoming more common.
- Blockchain – the authors say this 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 jargon. What the book does well is cover almost everything likely to be important in the next five years or so.
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 1999; 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 – 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.

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.

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 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 therefore taken place in Europe, with a report published by the Body of European Regulators for Electronic Communications (BEREC) in December 2014.

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 to consider this question as part of the Commission’s review.

**PILLS 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. However, in 2013, the Commission proposed to move away from this approach towards one of micro-regulation, seeking to define which specific commercial and technical practice networks operators were permitted to engage in. For instance, it singled out and tried to restrict the provision of ‘specialised services’ (one 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 issues. But the practicality of enforcing such rules seemed rather an afterthought. Stakeholders (including industry players across the value chain) and regulators alike expressed concern that this would provide opportunities for regulatory arbitrage or forum shopping in areas where European companies operate under a country of origin principle (such as broadcasting, ecommerce and data protection), this principle requires companies to comply only with the rules of the country in which they are established: some might even choose to base themselves in a less heavily protected standards elsewhere.

The Commission is right to tackle the disadvantage of service and when such differentiation is discriminatory (eg. charging different prices for otherwise identical online transactions depending purely on the geographical location of the user) 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 provides no detailed rules (eg. differentiated treatment of digital goods and protection standards elsewhere).

In telecoms, despite harmonisation at EU level, national markets maintain different characteristics – not least as a result of network topology and size. This means that differentiation of market power and thresholds for regulatory fragmentation across Europe, as and when necessary, such as through the imposition of minimum quality of service or other obligations – 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 reinvigorating the detail of how programmes are sponsored or products placed, rules could focus instead on the relevant consumer protection principles that are enshrined in the audiovisual directive. Perhaps this may be a timid reference (in the supporting working document, not in the main text) to the need to review the independence of media regulators in Europe.

This is an area where the Commission clearly states that viewers (and hence the regulator) should be able to choose and take instructions from any other body and limit the grounds for dismissal of the head. It requires NRAs to have separate budgets that should be published.

Regulatory independence matters: first and foremost, 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.

- **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 interference, accomplished by sufficient investigative and sanction powers, security of funding and budgetary autonomy**

In the audiovisual sector, there is no independence requirement at EU level. When the relevant European directive was last reviewed, European governments rejected the Commission and Parliament’s attempts to adopt an EU-wide solution that would result in a less than ideal compromise of an indirect and general reference on the need for ‘independent’
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 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 and two legislative measures: a regulation setting out a general EU framework for data protection (GDPR), and a
The rationale of the GDPR has been supported and reinforced by the DSM strategy.

The GDPR brings forward a ‘one-stop shop’ for market operators and users.

The GDPR is a piece of legislation that was adopted by the European Parliament and the European Council in 2016. It is a comprehensive framework for the protection of personal data and is known as the General Data Protection Regulation (GDPR).

The GDPR has a wide scope and applies to all EU member states, as well as to any processing of personal data in the context of the activities of an organisation established in one of those states. It applies to any processing of personal data that takes place within the European Union.

The GDPR is based on several key principles, including:

- The right to be informed (data subject's right to know what data is held about them)
- The right to access (data subject's right to access their personal data)
- The right to rectification (data subject's right to have inaccurate data corrected)
- The right to erasure (data subject's right to have their personal data deleted)
- The right to restrict processing (data subject's right to prevent their personal data from being processed)
- The right to data portability (data subject's right to obtain their personal data in a structured, commonly used and machine-readable format)
- The right to object (data subject's right to object to the processing of their personal data)

The GDPR also introduces new requirements for data controllers and data processors, such as:

- The obligation to implement appropriate technical and organizational measures to protect personal data
- The requirement to obtain the informed consent of the data subject before processing their personal data
- The need to notify the data subject of any breach of their personal data

The GDPR has been implemented in all EU member states and is enforced by national data protection authorities. It has been praised for its emphasis on the protection of individual rights and freedoms, but has also been criticized for its complexity and the challenges it poses for businesses and organizations.

In conclusion, the GDPR is a significant piece of legislation that aims to harmonize data protection laws across the EU and to give individuals more control over their personal data. It is an important step towards ensuring a more transparent and trustworthy digital environment.

January 2016 Vol 43 Issue 4 | InterMEDIA
the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, or 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 subjected to the scrutiny of 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 and unremitting surveillance.”

The Directive’s retention period “limited to what [was] strictly necessary” as it instituted a minimum retention period of six months without the distinction between different sorts of data or different types of users, and a retention period of between six months and two years without requiring “[t]hat 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 Fundamental Rights i.e., enshrining a high level of data protection – which is all the more essential in the digital age – thereby averting an emerging surveillance of the private lives of citizens.” Hence European institutions cannot ignore the ECJ’s decision regarding personal data and privacy, the proposal for the EU data protection directive must be in conformity with the ECJ’s ruling.

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.

Increasingly, the advisory Article 29 data protection working party also called on member states to gauge the consequences of the ECJ pronouncement on national data protection laws, reminding that “there is no such thing as all kinds of data and that, instead, data are subject to appropriate differentiation, limitation or exceptions.”

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 society. Data is an extremely valuable asset in a society. Data is an extremely valuable asset in a society. Data is an extremely valuable asset in a society. Data is an extremely valuable asset in a society. Data is an extremely valuable asset in a society. Data is an extremely valuable asset in a society. Data is an extremely valuable asset in a society. Data is an extremely valuable asset in a society. Data is an extremely valuable asset in a society.

At the same time, data possession generates benefits or disadvantages, including some advantages that cannot be replicated by potential entrants. In particular, other entities engaged in providing internet search advertising 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 retention periods are likely to be much less precisely defined around a certain product or service, and much more on a per-person or per-account basis, depending on whether to use those data across different types of activity. Thus a crucial element in defining these models 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 possibility of service being provided by the same company (‘intra-company versatility’) and for other companies to provide another or even the same service (‘intra-consortium’).

**INVALIDATION OF THE COMMUNITY’S US SAFE HARBOUR AGREEMENT**

Edward Snowden’s revelations of mass surveillance on EU citizens impacted on the so-called safe harbor scheme, which includes a series of principles concerning the protection of personal data to which US undertakings may subscribe voluntarily.16 Specifically, on 6 October 2015, the ECJ declared invalid17 the European Commission’s transatlantic data protection agreement from the year 2000, holding it does not adequately protect personal data. Subsequently, fundamental freedoms and the movement of its citizens’ data outside of the EU, unless it is transferred to a location which is considered ‘adequate’ by EU governments, or is conducted in line with other models of the protection of privacy and fundamental rights, entered into force.

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 of 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 concerns about 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 competition.”

In its landmark ruling, the ECJ specified that the European Commission did not have the competence to entrust formal supervisory powers in protecting the personal data of its citizens. Interestingly, the ruling came less than a week after a preliminary ruling of the EU’s highest court, the ECJ, 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 company that secretly monitored email communications in Slovakia but was “operating” in Hungary).

Following the invalidation of the safe harbour agreement, US companies, including internet behemoths such as Google, Facebook, and Apple, must strive for striking ‘new deals’ to compensate the loss of a data protection 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 build 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 harbor to meet the ECJ’s concerns, while ensuring certainty and clarity.

**COUNCIL OF EUROPE MODERNISATION OF CONVENTION NO. 108**

In parallel to the legislation initiative of the Commission, the Council of Europe (CoE) in March 2012 presented its proposals for updating the Convention No. 108 and the Data Protection Directive with regard to Automatic Processing of Personal Data (Convention No. 108).18 In 2011, the panel addressing the modernisation project of the Convention No. 108, called “Data Protection Working Group”, issued a report, underlining the need for a more modern, flexible and effective framework, in particular to better adapt to the specific characteristics of digital environments and to the new opportunities provided by the enhancement of the powers of the supervisory authorities. The modernisation proposals include the introduction of a new article 8bis. A draft modernisation agreement was negotiated on the basis of the modernisation proposals and transmitted to the Committee of Ministers for examination and adoption.19 In November 2012, the CoE consultative committee adopted its final proposals for modernisation, and submitted them to the Committee of Ministers for adoption.20 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 No. 108. A draft amending protocol as to be arranged on this basis and transmitted to the Committee of Ministers for examination and adoption.21 Although the EU and CoE share the same concern 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). But its coherence and compatibility with the European regulatory framework remain key objectives.

**The Way Forward**

New EU rules on data protection are in the final stage. In the 17 December 2015, the EU Parliament’s Civil Liberties, Justice and Home Affairs Committee (LIBE) voted on the informal text of a data protection reform that has been very critical for its general formulation of the principles and the high reliance on self-certification and self-regulation. Similar concerns have been raised by political and business leaders and the European Parliament’s press office.

Council later in 2016, probably in March or April, as such, 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 the highly technical matters while being confronted by strong political stances and interests, 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. 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 data protection lacking of a 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 LUSS Guide, Canti University, Rome. He is a member of the Rome lawyer and former advisor to the highest court of Italy. Menzi focuses on communications and media, IT, privacy and data protection, copyright and regulation of public utilities.
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. However, its take-up is still being held back by much fratz, 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. Based on the US National Institute of Standards and Technology (NIST) service models, where the 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, i.e. 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 the 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 reallocate 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. 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’. 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, e.g. file storage or sharing where the file contains personal data, then the provider is a ‘processor’, because it is at least storing personal data (or transmitting personal data 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. Then, and indeed in the 1960s, controllers used computer service bureaux, which were handed personal data (and the ability to redeploy underlying hardware/software for use by other customers, when one customer’s usage ceases). You then microwave yourself in your own kitchen. It requires no processor to back up the controller’s data. The analogy I suggest is that of cooking. 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 microwave – 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 needs and instructions. 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 braving data protection laws.9

Another unsung 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 encrypts 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

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 happens with Aaron’s, a computer rental chain in the US,” then it would become a controller in its own right, in place of the consumer. However, the type of 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 fully 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 breaches. However, any such legal duty 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 simply a type of service we may not 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 flexibility and agility. Many mobile apps are built on top of IaaS or Paas services; for example, Finland-based company Rovio’s popular Angry Birds game uses Amazon Web Services. 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 by infrastructure cloud services or when data are encrypted pre-upload, seems unnecessary and counterproductive. Tarring all cloud providers with the same ‘processor’ label is a misapplication.

Furthermore, the use of encryption by cloud customers (and indeed your Govt. providers, to prevent intelligible access by their sub-processors) should be encouraged, recognising that encryption may render data unreadable to unauthorised persons. Suppose you find a USB flash drive in the street but it contains personal data, so you can’t read it. Now, do you control the purposes and means of processing the data of the person who used 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 information cloud.

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

So why is it that regulators don’t 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 such additional security requirements would, or could, implicitly extend to such contracts, so no explicit requirement is necessary.

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 providers/sub-provider access? Why should mirror contracts be required from cloud sub-providers in addition? Couldn’t 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?

USE OF SUB-PROCESSORS

As another example of non-technologically neutral laws adversely affecting computing, consider theGDPR protection regulators’ approach to the use of sub-processors in cloud computing. In cloud computing, if a SaaS service is provided using the use of computing resources (in the form of infrastructure cloud services) by deeming cloud providers to be processors, even by infrastructure cloud services or when data are encrypted pre-upload, seems unnecessary and counterproductive. Tarring all cloud providers with the same ‘processor’ label is a misapplication.

Furthermore, the use of encryption by cloud customers (and indeed your Govt. providers, to prevent intelligible access by their sub-processors) should be encouraged, recognising that encryption may render data unreadable to unauthorised persons. Suppose you find a USB flash drive in the street but it contains personal data, so you can’t read it. Now, do you control the purposes and means of processing the data of the person who used 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 information cloud.

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

So why is it that regulators don’t 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 such additional security requirements would, or could, implicitly extend to such contracts, so no explicit requirement is necessary.

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 could play in protecting personal data, and encourage its use more widely. So where are the incentives for controllers (and processors) to apply encryption?

USE OF SUB-PROCESSORS

As another example of non-technologically neutral laws adversely affecting computing, consider theGDPR protection regulators’ approach to the use of sub-processors in cloud computing. In cloud computing, if a SaaS service is provided using the use of computing resources (in the form of infrastructure cloud services) by deeming cloud providers to be processors, even by infrastructure cloud services or when data are encrypted pre-upload, seems unnecessary and counterproductive. Tarring all cloud providers with the same ‘processor’ label is a misapplication.

Furthermore, the use of encryption by cloud customers (and indeed your Govt. providers, to prevent intelligible access by their sub-processors) should be encouraged, recognising that encryption may render data unreadable to unauthorised persons. Suppose you find a USB flash drive in the street but it contains personal data, so you can’t read it. Now, do you control the purposes and means of processing the data of the person who used 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 information cloud.

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

So why is it that regulators don’t 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 such additional security requirements would, or could, implicitly extend to such contracts, so no explicit requirement is necessary.

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 could play in protecting personal data, and encourage its use more widely. So where are the incentives for controllers (and processors) to apply encryption?

USE OF SUB-PROCESSORS

As another example of non-technologically neutral laws adversely affecting computing, consider theGDPR protection regulators’ approach to the use of sub-processors in cloud computing. In cloud computing, if a SaaS service is provided using the use of computing resources (in the form of infrastructure cloud services) by deeming cloud providers to be processors, even by infrastructure cloud services or when data are encrypted pre-upload, seems unnecessary and counterproductive. Tarring all cloud providers with the same ‘processor’ label is a misapplication.

Furthermore, the use of encryption by cloud customers (and indeed your Govt. providers, to prevent intelligible access by their sub-processors) should be encouraged, recognising that encryption may render data unreadable to unauthorised persons. Suppose you find a USB flash drive in the street but it contains personal data, so you can’t read it. Now, do you control the purposes and means of processing the data of the person who used 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 information cloud.

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

So why is it that regulators don’t 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 such additional security requirements would, or could, implicitly extend to such contracts, so no explicit requirement is necessary.

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 could play in protecting personal data, and encourage its use more widely.

So where are the incentives for controllers (and processors) to apply encryption?

USE OF SUB-PROCESSORS

As another example of non-technologically neutral laws adversely affecting computing, consider theGDPR protection regulators’ approach to the use of sub-processors in cloud computing. In cloud computing, if a SaaS service is provided using the use of computing resources (in the form of infrastructure cloud services) by deeming cloud providers to be processors, even by infrastructure cloud services or when data are encrypted pre-upload, seems unnecessary and counterproductive. Tarring all cloud providers with the same ‘processor’ label is a misapplication.

Furthermore, the use of encryption by cloud customers (and indeed your Govt. providers, to prevent intelligible access by their sub-processors) should be encouraged, recognising that encryption may render data unreadable to unauthorised persons. Suppose you find a USB flash drive in the street but it contains personal data, so you can’t read it. Now, do you control the purposes and means of processing the data of the person who used 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 information cloud.

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

So why is it that regulators don’t 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 such additional security requirements would, or could, implicitly extend to such contracts, so no explicit requirement is necessary.

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 could play in protecting personal data, and encourage its use more widely.

So where are the incentives for controllers (and processors) to apply encryption?
provisions (narrower than full mirror contracts) suffice to protect against such risks? As mentioned, technology startups and other SMEs may wish to use IAaaS/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 regulations 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 at the SME end, earn revenue 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, 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 be the same 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 service 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. One of the more interesting parts of the proposed GDPR, which includes recital that “consent should not be regarded as freely given if the data subject has no genuine and free choice and is unable to refuse 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. Moreover, for some sensitive data processing operations (such as medical data), consent should not be regarded as freely given if the data subject is in a situation where she is forced or unable to refuse or withdraw consent without incurring a disadvantage, detriment, or significant other disadvantage.”

Such concerns may also have influenced regulators’ attitude towards cloud computing. 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.” Consumers do enjoy the benefits of 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 cloud contracts are 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 reluctance against many free services’ excessive collection of consumer 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 intrusive 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 the nature of cloud computing. It is therefore not surprising that cloud computing is under consideration for the cloud model? The data centre operator’s position and rights/liabilities in relation to the service provider are not likely to be the same 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 service too?

Is IoT-specific regulation needed to build public confidence?

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 Industry respondents argued that questions 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 specific IoT regulation 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.1

I now consider 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.

ECHELON AND SPECTRUM

A significant issue for IoT is the licensing and spectrum management. Spectrum management is a significant issue for IoT, as it is for any technology sector. IoT devices need some form of medium for communication between the devices themselves and the outside world. Most devices will need to use wireless spectrum to do this, and there are many different frequencies and technologies that can be used for wireless communication.

Due to the explosion in the number of connected devices, the demand for spectrum is increasing rapidly. This has led to a number of spectrum management challenges, including the allocation of spectrum to different types of services, such as IoT, and the management of spectrum congestion.

In the United States, the FCC is responsible for spectrum management. The FCC has been working to implement a number of initiatives to improve spectrum efficiency and availability, including the creation of a national spectrum database and the development of new spectrum allocation methods. The FCC has also been working to promote the development and adoption of new technologies and services that can operate on low-frequency bands, such as IoT devices.

In Europe, the ETSI (European Telecommunications Standards Institute) is responsible for spectrum management. The ETSI has been working on a number of initiatives to improve spectrum efficiency and availability, including the creation of a national spectrum database and the development of new spectrum allocation methods. The ETSI has also been working to promote the development and adoption of new technologies and services that can operate on low-frequency bands, such as IoT devices.

It is clear that there are many different frequencies and technologies that can be used for wireless communication, and that the demand for spectrum is increasing rapidly. This has led to a number of spectrum management challenges, including the allocation of spectrum to different types of services, such as IoT, and the management of spectrum congestion. In the future, we can expect to see continued efforts to improve spectrum efficiency and availability, as well as the development and adoption of new technologies and services that can operate on low-frequency bands, such as IoT devices.
unused spectrum bands, while a US presidential commission has recommended a flexible allocation of a well-developed space of shared, flexible spectrum. This Belgium-based commission has recommended that the available spectrum for shared-space technology in the United Kingdom. The US Federal Communications Commission (FCC) has also recommended that spectrum be made available for shared-space technology for government, public safety, and homeland security. The European Telecommunications Standards Institute (ETSI) has also recommended that spectrum be made available for shared-space technology for government, public safety, and homeland security.

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 may use 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 reach of communications, rather than requiring a large and complex global network, and matches the current need for a push-down of a product and its value to the internet – a large address space is required to individually identify each one.

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 every 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 may also set up IPv6 task forces to encourage national transitions.

For any IoT identification scheme, there will be trade-offs between performance and reliability, efficiency, privacy, security, scalability, and mobility support. As well as IPv6 address space, other identifiers can be used to uniquely identify devices in the internet and in different sources. Such rules usually allow telecoms providers to offer such customers’ ‘specialised services’ with specific speed or reliability guarantees.

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

POLICY AND REGULATORY MEASURES

What? Why? What is done today

License and spectrum management
Ensures spectrum is available for a wide range of IoT applications at short and long ranges, in licensed and unlicensed bands.

Monitoring availability of spectrum for short and long range IoT communications, and technical, geographical, capacity, and security requirements.

Switching and roaming
Standard mobile telephony networks (3G and above) are non-routable, making them unsuitable as NEMs, and mobile and fixed devices in areas of poor network.

Mobile network operators are developing NEM-specific business models for roaming and interworking with the existing network.

Competition
Some remote configuration of IoT devices over the internet requires position of large firms and increase potential for consumer lock-in. Limited user access to raw IoT data and access ability to switch providers (avoids underpriced philanthropic implications).

Enabling competition regulators have capability to ensure IoT markets for abuses of dominant position.

Privacy and security
Security vulnerabilities in IoT systems in attacks on devices and cause loss of service to critical medical devices and connected vehicles.

Ensuring security and privacy from the outset of IoT system design.

Further development of privacy and consumer protection laws to ensure device and network security. Ensuring security and privacy from the outset of IoT system design.

InterMEDIA | InterMEDIA | January 2016 Vol 43 Issue 4 | InterMEDIA
request that related ministries improve these
regulations. For new products and services,
attention will be given to ... Issue 4 www.iicom.org
Many companies 
building IoT 
products do not 
have internet 
security experience.
B riefing
...
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”.

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 new, 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 competitiveness. Governments can take further steps to encourage national transitions to IPv6, updating all their 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 bandwidth to support the enormous amounts of 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 codes, to support 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. Competitions need to be put in place to encourage who will encourage the development of new IoT services. They can increase the flexibility of IoT services in collecting data not initially required to provide a service. While the European Union’s legislation fundamentally provides a legal framework to address these issues, it is up to the national and local government authorities to implement them in the right way.

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.

Dr. Pierre-Jean Benghozi is Research Director at the Global Regulators Forum. The author is grateful for comments by Rudolf van Berg, Pierre-Jean Benghozi, Mailyn Fidler, Simon Forge, Ben Hawes, Gilad Rozenoer, and ITU staff.

REFERENCES

European Commission (2015). Conclusions of the internet of things public consultation. 21 Staff Report (2015). Internet of Things Policy and security in a connected world: A joint report on the Internet of Things (IoT) and the hyper-connected digital revolution. Republic of Korea Ministry of Science, ICT and Future Planning, 4 May 2014. 22 Lichtenberg K et al. (2014). Europe’s policy options for a dynamic and inclusive development of the Internet of Things. IAB-Consultation. 23 Marsden CT (2014). Machine-to-machine communications: Common policies of devices. bit.ly/1K0qFvP. 24 Net neutrality: Towards a co-regulatory solution. November 2014. 25 European Commission (2015). op. cit. 26 Net neutrality: action plan. December 2014. 27 Telecommunications (2016). 28 Internet of Things: Privacy and security in a connected world. 29 European Commission, 30 November 2016. 31 ENISA (2014). Privacy and data protection developments on the internet of things. p18. bit.ly/1smejQi 32 ENISA (2014). Opinion 8/2014 on the recent developments on the Internet of Things: Privacy and security in a connected world. bit.ly/1smejQi 33 Bouchetey, Pierre-Jean Benghozi, Mailyn Fidler, Simon Forge, Ben Hawes, Gilad Rozenoer, and ITU staff. 34 Cerrudo C (2015). An emerging US (and world) threat: Cities wide open to attack. bit.ly/1SpsYTA 35 IRC Technological Advisory Council. Internet of Things (2015). bit.ly/1h0dUO8 36 LinkedIn was a prison. 37 4G was a parking space. 38 Despite the news, your refrigerator is not yet sending spam. 39 Facebook cannot be found under ‘F’ in the index of his book, “The World is Flat: A brief history of the twenty-first century” and the year the 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. 40 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. 41 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. 42 For regulators to more fully address the challenges of digital disruption a different regulatory focus will 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. 43 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

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:

Two years ago was perhaps one of the most significant years in modern communications history, when consumer access to the internet was at its infancy. Microsoft was just launching its first web browser (Internet Explorer), the

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

INTERMEDIA | January 2016 Vol 43 Issue 4 44
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 bookeller 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 built on the back of 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® 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 largely taken-for-granted smartphone world into the ambient world of devices and objects that surround us. Through which we shall see development potential that may be simply unparalleled 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: "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 been a fundamental and major disruption across the economy and strategy that suggests that as connectivity improves and devices and software become even more powerful and cost-effective, the whole world will continue to fundamentally change, in ways it is hard to predict. And if the patterns of previous disruptive technologies is repeated, this change will transform our way of thinking to a stage in which development of such a potentially transformative technology, the most sensible thing we can do is to play a facilitative role so that this market can find and test its own propositions for this space."

In other words, to either know or to remain involved in the development of potential uses where we can, or to stay out of the way, by for example, ensuring that there is regulatory engagement with regulatory interventions where they might be necessary. And "We must remain engaged but resist the temptation to indulge in regulatory activism."
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.3

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

“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