Inter MEDIA

THE WORLD'S MOST INFLUENTIAL TELECOMS AND MEDIA POLICY, REGULATORY AFFAIRS AND COMPLIANCE JOURNAL

JANUARY 2017 | VOLUME 44 | ISSUE 4

HOW THE INTERNET GOT TRUMP ELECTED

The IIC's

Telecommunications and Media Forum (TMF) 2017

Taking the debate around the world...

Dates for 2017

- 21-23 March 2017, Doha
- May 2017, Miami
- Dec 2017, Washington DC

Join the IIC

Members can attend TMF meetings free of charge

Discussion topics

- Innovation and investment
- Governance
- Spectrum
- Privacy and security
- Competition
- Content

Plus

- 5G
- Connectivity
- The Digital Ecosystem
- The Internet of Things

The IIC is a platform that brings together regulators and stakeholders for the exchange of ideas and experiences which, in my view, is the most valuable way to push forward new polices and projects

Jose M. Marín-Quemada
President
CNMC, Spain

Visit www.iicom.org
Call +44 (0) 20 8544 8076
Join the IIC's LinkedIn community for year round debate

Shaping the Policy Agenda

JANUARY 2017 | VOLUME 44 | ISSUE 4

CONTENTS

Inter MEDIA

THE INTERNET CONUNDRUM

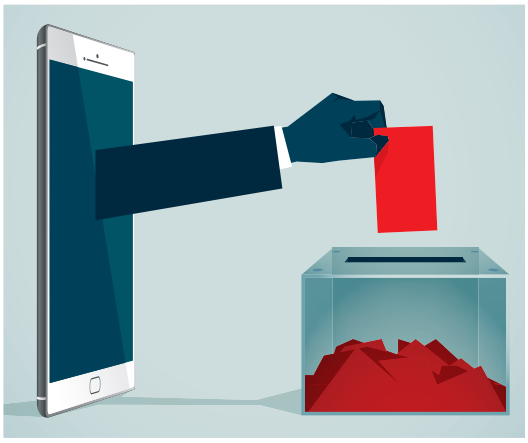
Just when you thought things couldn't get any more uncertain and dynamic in our telecoms and media world along come events that raise the most fundamental questions about cooperation, transparency and democracy itself. I refer to the impending UK exit from the EU (Brexit), the election of Donald Trump, and the rapid rise of concern about interference with elections and the proliferation of fake news, the latter at least being in play in the UK and the US, and which is being taken seriously now in other countries such as Germany. The internet of course is the enabler of fake news and hacking, but as Eli Noam explains in this edition, it is also an underpinning force in many aspects of society now, having effects on societal fragmentation, employment and inequality, and even political gridlock. I cast no political direction here, but 2016 may have shown that there is even more to the internet's influence than we knew. **Chris Chapman, president, IIC**

www.iicom.org

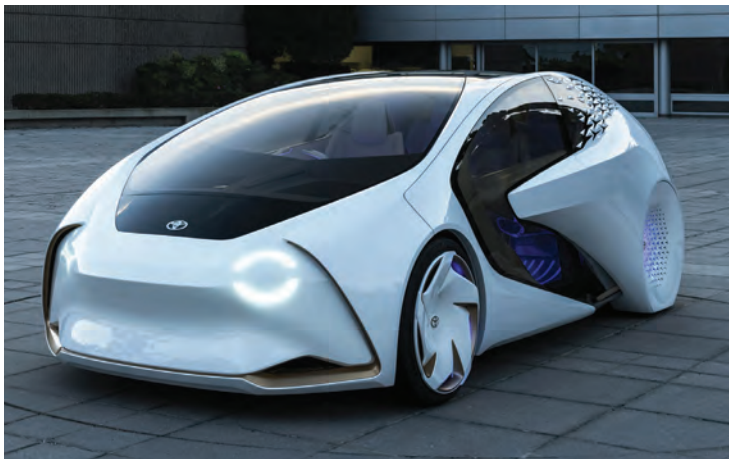
The International Institute of Communications is the world's leading independent, non-profit, membership forum engaged with digital media policy and regulatory affairs. IIC activities cover issues in telecommunications, broadcasting and the internet.

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

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



NEWS
FROM AROUND THE GLOBE



Above: a latest autonomous car concept, from Toyota. The European Commission has adopted a European strategy on cooperative intelligent transport systems (C-ITS), which it says is a 'milestone towards cooperative, connected and automated mobility' – see bit.ly/2jddsPX

INTERNET GOVERNANCE

CONCERNS ABOUT THE INTERNET

The Internet Society has urged the global community to redouble its efforts in addressing the wave of unprecedented challenges facing the internet. The organisation's CEO, Kathryn Brown, speaking at the 11th Internet Governance Forum in Mexico, said: "The open, trusted, global internet has delivered on its promise as a tool to change lives, enhance growth and provide essential human services – but the progress is uneven and threatened by challenges that have grown."

The lack of affordable access to the internet and the disparity in levels of access across the world remain key challenges. Internet growth rates are slowing, resulting in a deepening digital divide between those with access and those without. In addition, issues such as blocking of content, privacy, mass surveillance, cybercrime, hacking and fake news are all contributing to what is now a growing global erosion of trust among users. "Multiple security issues are damaging user confidence and have emerged as the existential threat to the future of the internet. We must act now to reverse this trend," added Brown.

As internet adoption and connectivity continue to grow, with 45% of the population online, so do the number of cyber-attacks. Mexico ranks as the second country with the largest number of cyber-attacks in Latin America after Brazil, with a 40% increase in reported cyber-attacks in 2014 alone.

"We still have time – but there is urgency," she concluded. "We must work together now to solve these significant emerging challenges facing the internet, using the value in the multi-stakeholder model and the power of collaboration to offer solutions for connecting the unconnected and increasing user trust."

■ The Internet Society, with Microsoft, has completed a series of meetings on internet fragmentation, which has become an important issue in the context of the global internet. The Global Commission on Internet Governance has also published a volume on internet fragmentation.

■ The Global Commission on Internet Governance has issued another paper, 'Corporate accountability for a free and open internet'.

■ The Global Network Initiative (GNI) has released a policy brief with recommendations for governments and companies to protect and respect free expression and privacy rights when responding to the challenge of alleged extremist or terrorist content online. See bit.ly/2d2Bc6K

CHILDREN

GLOBAL KIDS ONLINE

A majority of children say they learn something new online at least every week, but large numbers still face risks online, according to a report by a new initiative, Global Kids Online, produced by the UNICEF Office of Research and the London School of Economics. The project, launched at the Children's Lives in the Digital Age seminar held at UNICEF in New York, aims to build a global network of researchers investigating the risks and opportunities of child internet use, and a website is making research tools freely available worldwide. Another finding is that although a majority of children value the internet as a learning tool, they are rarely able to use it at school or to receive guidance from their teachers on how to use it. For details see: globalkidsonline.net

CANADA

BROADBAND IS BASIC

The Canadian Radio-television and Telecommunications Commission (CRTC) has declared that broadband internet service is now considered a basic telecoms service for all Canadians, and is setting 'ambitious' new speed targets and creating a fund that will invest up to CND$750 million over and above existing government programmes. The targets are:

● Speeds of 50 (mbps) download/10 mbps upload for fixed services

● An unlimited data option

● Latest mobile wireless technology not only in homes and businesses, but also along major roads.

Further, service providers should ensure that contracts are written in clear language, and should make available tools so consumers can easily manage their data usage; and all wireless service providers will have to offer mobile service packages that meet the needs of Canadians with disabilities. See bit.ly/2hebsJR

PRIVACY

LEVELLING THE FIELD

The European Commission has proposed a new regulation on privacy and electronic communications that it says will update existing rules and offer more business opportunities. The current e-privacy directive only applies to telecoms operators, so rules will also cover new providers such as WhatsApp, Facebook Messenger, Skype, Gmail and iMessage and, once consent is given for communications data, both content and/or metadata, to be processed, traditional telecoms operators will have more opportunities to use data. See bit.ly/2i99Kd5

EUROPE

ANALYSING THE COMMUNICATIONS CODE

There has been broad support for the European Commissions's proposed Electronic Communications Code, including from BEREC, the body of European regulators. It welcomes the introduction of an explicit connectivity objective alongside the promotion of competition, the internal market and consumer interests, while explaining that in practice, some of the new provisions on access regulation might not help the achievement of those objectives. Sectoral regulation, it adds, is only one of many levers – "It cannot, on its own, incentivise investment in high-capacity networks or indeed demand."

BEREC also welcomes the inclusion of a range of over the top (OTT) services in the framework, but is concerned that the proposal to fully harmonise consumer protection regulation will prevent regulators and member states from responding to emerging challenges in their respective markets, or indeed from deregulating where justified.

Also welcome is the proposed harmonisation of minimum competences for independent regulators, and the strengthening of the independence obligations. "However, the proposal to transform BEREC into an EU agency not only risks increasing the bureaucracy and cost of European telecoms regulation, but also undermines the benefits of the proposed strengthening of independence at the national level." Details: bit.ly/2i5cgRo

■ Mobile body, the GSMA, has published a position paper on the draft code. It calls for longer spectrum licence durations; 'realistic' coverage obligations and when assessing competition issues in the context of spectrum licences, member states should apply the same standards as they do in the significant market power framework. See: bit.ly/2h1rGp4

CYBERSECURITY

WHITE HOUSE URGES COOPERATION

The US government and the private sector must cooperate to improve the security of digital networks, a US presidential commission on cybersecurity recommends in a report. The commission, created by President Barack Obama last year, also recommends that the president and Congress accelerate the pace at which technology is updated in the federal sector and that the president appoint an ambassador for cybersecurity for efforts abroad. "Technological advancement is outpacing security and will continue to do so unless we change how we approach and implement cybersecurity strategies and practices," the report says. Among other recommendations, the report urges the US to seek harmonised international cybersecurity policies and global norms of behaviour. The report is at: bit.ly/2h5UMDU

RADIO

NORWAY TURNS OFF FM STATIONS

Norway has turned off its FM radio stations, making good on a decision made in April 2016, and following a radio digitisation mandate issued by the Storting (the Norwegian parliament) in 2011. The cost of transmitting national radio channels through the FM network was eight times higher than with the DAB network, and broadcasters were spending large sums on parallel distribution.

The government notes that DAB is far less vulnerable to transmitter failure in extreme conditions, permits tunnel reception of all channels, and allows simultaneous transmission of emergency messages on all channels.

A number of criteria were set for the switch-off, including 90% population coverage and affordable systems for cars.

EVENTS

6-9 February, Geneva
Digital Radio Week, EBU

22 February-2 March, Barcelona
Mobile World Congress

21-23 March, Doha
IIC Telecommunications and Digital Media Forum (TMF)

17-19 May, Edinburgh
European Platform of Regulatory Authorities

23 May, Miami
IIC Regional Regulators Forum

24-25 May, Miami
IIC Telecommunications and Media Forum (TMF)

IN BRIEF

ITU OPENS UP

The ITU started the new year by launching an access to information policy, committing to make more information and documents held, managed or generated by the ITU openly available online. It aims to bring public access to information for the ITU's main conferences and meetings in line with other international organisations like the World Bank, UNDP and UNESCO.

FTC TARGETS IOT

The Federal Trade Commission has filed a complaint against Taiwan-based computer networking equipment manufacturer D-Link, alleging that inadequate security measures taken by the company left its wireless routers and internet cameras vulnerable to hackers and put US consumers' privacy at risk.

BAND IN PLAY

EU law makers have agreed legislation that will require every country to allocate, by 2020, spectrum in the 700 MHz band for use by wireless broadband providers. It aims to bring long-term regulatory certainty and is 'essential' for uptake of 5G.

5G CHALLENGE

The Future Communications Challenge Group has sent a report to the UK government that advises on what the country should do to be a world leader in 5G. The government has recently announced £1bn of funding to boost the UK's digital infrastructure. Report: bit.ly/2iiPowy

BULLETIN FROM BANGKOK

The IIC's annual conference in Bangkok, Thailand, in the autumn focused on regulatory and policy transformation for the digital economy and all its aspects. Report by Intermedia editor, **MARC BEISHON**

The IIC's 47th annual conference, part of the Communications and Regulation Week held each year, took place in Bangkok, Thailand, at the Eastin Hotel. It was preceded as usual by the International Regulators Forum (IRF), this year hosted by Thailand's regulator, the National Broadcasting and Telecommunications Commission, at its headquarters in the city (and as always, the IRF is a 'closed doors' meeting for regulators only, held under the Chatham House rule – see page 8).

TOWARDS DIGITAL THAILAND

The opening keynote on the first day of the conference was delivered by Vichaow Rakphongphairoj, managing director of True Corp, a converged telecoms operator in Thailand. He described how Thailand has made substantial progress in communications growth and reducing the digital divide in recent years during a period of political and regulatory stability. The country now lies in third position in the region according to the World Economic Forum's Networked Readiness Index, behind Singapore and Malaysia, and is up to 120% mobile penetration, and internet use exceeds 50%, driven by low-cost smartphones. The government, he added, is pushing a Digital Thailand agenda, which has six pillars, only one of which, the workforce, is lagging by much. There is also a programme for business start-ups.

> **"Technology convergence needs to also be understood by other regulators and government agencies."**

Although Thailand was late in adopting 3G mobile, said Rakphongphairoj, the country has now made rapid progress in opening up more spectrum, with two 4G auctions in 2015 for the 900 MHz and 1800 MHz bands, and is also angling for more international connectivity in an aspiration to be the leading digital hub in South-East Asia. To support this, there needs to be full connectivity on both sides of the Pacific and Atlantic, he added, as currently much traffic in the region comes east from the US.

REGULATOR ADAPTION

The first main session focused on objectives and priorities for regulators in adapting to digital transformation. IIC president, Chris Chapman, said that legislatures and policymakers are not providing sufficient intellectual leadership, regulatory frameworks, and joined-up roadmaps that are required in the face of unprecedented change. There have already been several digital 'tipping points' in areas such as data storage, pervasive communication, computational power, and social media and he posed the question: "What are the next tipping points, and are they just compound effects of previous tipping points, or are they again of an entirely different dimension?"

Shri Sudhir Gupta, secretary of the Telecom Regulatory Authority of India (TRAI), gave viewpoints from a developing country perspective, homing in on the broadband access challenge for many millions of people. Among the issues he raised are regulations that could hamper the deployment of public WiFi, and its interoperability with mobile networks, with interconnection and tariffing also to the fore, along with the promotion of cloud computing and critical applications such as mobile banking in a bid to give all Indians access to a bank account. This also means working with the financial regulator, he noted, adding that technology convergence needs to be understood by other regulators and government agencies.

Gupta also highlighted net neutrality – an issue he said is 'haunting' most of the regulators across the world, noting that India was among the first to regulate on prohibiting discriminatory tariffs for data services. Broadcasting is also a concern – there has been a long effort to gain an holistic view of the regulations in the broadcasting sector, and "we are working on a framework that would ensure equitable distribution of revenue to different stakeholders in the value chain". Concluding, Gupta said: "One cautionary note I would like to put is, though access is a priority, this must not be at the expense of competition at the network level as it could lead to undesirable social outcomes."

Adriana Labardini, a commissioner at Mexico's

Left: Vichaow Rakphongphairoj of True Corp delivering the keynote
Right: Delegates take in the session on goals for development

regulator, IFT, spoke about the goals for regulation and competition policy and keeping a firm eye on net social benefits. To this end, Mexico has addressed a number of supply side issues, including opening up more spectrum and embarking on a wholesale mobile access network that will aim to cover areas that competition has failed so far to serve. While there are challenges in deploying next-generation networks, competition has already seen much more affordable prices, she said.

But the bigger picture lies in realising the promise of the digital economy for more people, where many other issues come into play, such as cybersecurity, big data, cloud computing, artificial intelligence and automation, skills, and integration with other sectors such as transport and health. New tools and laws will be needed for coordination and the ability to act with more speed, said Labardini, and there will probably be more than the six pillars in Digital Thailand to be accounted for in future for an increasingly complex digital ecosystem.

Rabha Zeidguy, council member of the High Authority of Audiovisual Communication (HACA) of Morocco, added a content perspective, identifying pluralism as a key issue in her country – "Not only political pluralism, but also linguistic and cultural pluralism," she said. There is a new law that has given civil society a greater stake in media pluralism – but with many active civil associations and a new route to complain to the regulator there is a challenge in managing a big flow of complaints.

Pluralism is only one part of wider access, and also includes connectivity, coverage and special needs access – and Morocco is doing well in both public and private sectors overall, said Zeidguy, and there is also an important provision of the new law to make audiovisual operators comply with a right to access information.

The last perspective in this session came from Stephen Unger from the UK regulator, Ofcom. Connectivity is at the heart of most debates, he said, certainly in the current strategic review in the UK and the proposed new regulatory code from the European Commission. But there are different perspectives for telecoms and media regulators. For telecoms, the roadmap to gigabit speeds is a big civil engineering challenge, especially in a country like the UK with old infrastructure, and also making sure that some people are not excluded. This is where good universal service obligation policy is still needed, said Unger. On mobile, there is the question whether 5G is needed before people can truly consume video on the move; and for the internet of things, he said that the debate is less about spectrum and more about security and privacy. Underpinning these issues is oversight of industry structure, such as mobile operator mergers.

Ofcom is also a media regulator, and connectivity drives change in accessing content. Unger noted that young people are going online and are unlikely to watch conventional TV. For the regulator, this transformation raises concerns about child protection, given that traditional broadcasting rules no longer work, and he also highlighted the role of public service broadcasting (and the BBC in particular), and the importance of not crowding out commercial offerings. Media plurality is also a hot topic, he added.

> **"The roadmap to gigabit speeds is a big civil engineering challenge, especially in a country like the UK with old infrastructure."**

In concluding, he identified two key issues – how to achieve the vision of ubiquitous mobile connectivity, and the lack of regulatory levers for this (and so new tools are needed); and the investment climate in the new era of Brexit (the exit of the UK from the European Union).

GOALS FOR DEVELOPMENT

The conference moved on to the topic of linking ICT policy and regulation with the new Sustainable Development Goals (SDGs). Chairing the session, Rohan Samarajiva of think tank LIRNEasia, and a former regulator, set the scene by saying that

connectivity is a clear aim for ICT policy but there should be a much wider agenda for issues such as innovation, resilience, trust building and security. Natasha Beschorner, an ICT policy specialist at the World Bank, said that along with connectivity there is a focus at the bank on digital innovation, collaborating with teams working on trade and competitiveness issues, macro-economic management and finance, and legal and regulatory reforms, which in many countries are still very much underdeveloped – "Legal protections for electronic transactions in particular."

A third strategic area is what she termed digital platforms, but one that interfaces with many of the SDGs, ranging from e-health and e-education to road safety and intelligent transport systems.

Beschorner mentioned several World Bank initiatives, including connectivity in the Pacific islands, telecoms reform in Myanmar, and a digital platform in Mongolia. Her own specialism is transport, where the World Bank is working in countries such as Malaysia and the Philippines on traffic congestion and road safety projects using big data analytics.

Siope Vakataki 'Ofa, from the UN Economic and Social Commission for Asia and the Pacific (ESCAP), described the huge increase in broadband connectivity in the region, but there is also an increasing digital divide as the top rated countries in both connectivity and digital economy activities pull away from the lowest ranked – there are 20 countries in Asia Pacific that have very low broadband internet penetration and some are still missing undersea fibre-optic cable links. Prices are also too high in some countries. He said that ESCAP is promoting the Asia-Pacific Information Superhighway initiative, which is aiming to increase regional broadband connectivity.

There are actually only two ICT targets in the new SDGs, pointed out Basheerhamad Shadrach, at the Alliance for Affordable Internet, World Wide Web Foundation, although one on connectivity is wide ranging (but not specific) and the other concerns women, who often contribute more than men in economic activity. He picked up the theme of accessing and analysing information, noting that there is a long way to go in contextualising data for use by communities.

Cost of broadband access is still a major issue, he added, and the targets of the UN Broadband Commission should be challenged, and this is where the Alliance for Affordable Internet comes in, by widening the number and type of large and small organisations in the effort. What is needed are coalitions of industry, governments, regulators, civil society and the media that can address issues such as taxation, tariffs and universal access, and introduce initiatives such as universal service funds that are designed to overcome limitations exposed in the past concerning other such funds.

Syed Ismail Shah, who heads Pakistan's telecoms regulator, said that the SDGs are helpful in showing the 'big picture' as regulators can get weighed down with day to day firefighting. There are though barriers in rolling out supply side connectivity to

From top: Richard Bean, acting director of Australian regulator ACMA, talks about his country's National Broadband Network; an impassioned intervention from the floor; equally impassioned was Robert Pepper, now working for Facebook, making two points (at least); delegates from South East Asia during a coffee break

underserved areas not connected to the internet, and while ICT clearly plays a big role in many SDG targets such as education and health, there are competing demands – people in remote areas may well need clean drinking water as well as broadband access, for example. "We need to work in parallel though – we can't wait until all other problems are solved," he said.

Shah said that regulators need to embrace a new era of collaborative regulation that has the big picture in mind and that can promote and not inhibit new technologies, and this means the kind of broad coalition emphasised in this session, including with the big players such as Facebook and Google, and recognising that the internet has no country boundaries.

A lot of detail was picked up in the discussion, such as where universal service funds have gone astray, and why taxation of digital devices and services can be harmful.

AUSTRALIA'S NATIONAL BROADBAND NETWORK

One of the world's major initiatives on next-generation broadband is taking place in Australia, and this year's conference devoted a session to examining the issues for the National Broadband Network (NBN), as introduced by Peter Lovelock, director of Singapore-based think tank, TRPC. The project is a government owned wholesale network with a spend of about AUS$50 billion that is used by internet service providers, (or retail service providers, as called there). It is also a combination of networks and technologies. Early efforts to proceed with a partnership with the incumbent operator, Telstra, foundered over regulatory concerns, before it was decided that the government alone would build a fibre network, with a deal reached with Telstra on infrastructure.

The first years though didn't go well until a turnaround team with telecoms experience was appointed and a 'NBN 2.0' was born that has compromised on the full fibre rollout. Delegates heard that if a country is contemplating building a big new network – as many are – it's important to separate the executional network and engineering from the regulation. They are of equal importance but conflating them can create difficulties.

Michael Cosgrave, general manager of the infrastructure regulation division, Australian Competition and Consumer Commission (ACCC), gave his appraisal of the NBN, noting the inclusion of satellite may well be seen as one of the successes, and that if ambitious rollout targets are met Australia is on track to deliver 25 mbps download to 100% of consumers and 50 mbps to 90%.

Focusing then on affordability and cost, he said it is far from clear how the network will operate after construction is finished, and he warned that infrastructure markets such as communications, "inevitably have the potential to be concentrated", and there is a "need to take dynamic, long-term impacts of competition and balance them against shorter term cost considerations". Embedding social policy objectives and particularly universal service obligations in a primary provider of network services can have significant distortionary effect, he added.

The incumbent in question, Telstra, was represented by Jane van Beelen, executive director of regulatory affairs. She outlined the implications for her company, including disconnecting copper and coax access networks and handing over certain assets to the NBN, so that Telstra will become a retail service provider. This has come at a loss of value for the company, she said, and Telstra still deploys copper to estates where the NBN won't reach and it also has an obligation to supply fixed line voice.

The disconnection programme in this structural separation process is complex, added van Beelen, and there have been many challenges – "It really needs a multi-stakeholder exercise to make sure that the providers of the various services all play their role in making sure that the customer can have as simple and seamless as possible migration to the NBN." She also said that removing the vertical integration can place retail suppliers further away from customers, and raises issues such as how cross-subsidies for serving low-income and vulnerable people will work.

Finally, Richard Bean, acting chair of the Australian Communications and Media Authority (ACMA), said the NBN is "creating a new technical and commercial environment – not only in terms of the multiple access technologies, but the fundamental change to the supply chain between the provider of various components of the services and the consumers". There are early signs, he said, of consumer confusion about who is responsible for services and problems that arise, which the ACMA is working to keep on top of. There are safety issues such as voice becoming mains powered and interoperability with emergency services. On the universal service obligation, he added: "The current legislation is all about the legacy fixed line telephone service and it's a very interesting and big question as to what it should be, if anything, in the future." Above all, he concluded, a high level consumers' view is needed on a project of this scale.

> **"If a country is building a big new network – as many are – it's important to separate the executional network and engineering from the regulation."**

DIGITAL TRENDS

The second day of the conference kicked off with a panel on the digital economy, including the internet of things. Chair Andy Haire suggested that discussion revolve around the key words, transformation, value and opportunity, and embrace all forms of communications and models, including the sharing economy.

Delegates heard an example of transformation – a tailor in a Vietnamese market using a website and social media to establish a global presence as a

micro-business – such businesses have more to gain than almost any other. A study by Deloitte has shown that small businesses that are online are twice as likely to be growing, and four times more likely to be hiring staff. Another transformation is in mobile use – there are now more Google searches on mobile than desktop in key markets such as the US and Japan, and the multinational nature of reach for businesses is also apparent in traffic, as with the tailor. Key enablers are connectivity, digital skills, and regulation and trade rules that allow small players the freedom to move data and goods.

> **IoT should largely be left to the market at this stage, but regulators should always watch out for consumer protection.**

Vodafone's senior legal and regulatory counsel, Agne Makauskaite, mentioned the findings of a study with Arthur D Little on the 'gigabit society' in Europe, and homed in on the internet of things (IoT), where companies are now no longer questioning its adoption but see it as critical to business, and the vast majority have increased IoT spend recently. She echoed the point about cross-border data flows, adding that data localisation requirements can be a huge restriction on cloud services. Numbering and roaming also remains as an obstacle to IoT, and Makauskaite said she was happy to see BEREC, the body of European regulators, conclude that IoT should largely be left to the market at this stage, but regulators should always watch out for consumer protection.

Ki-Joo Lee, commissioner at the Korea Communications Commission (KCC), said that IoT shouldn't be seen as just another technology development but a possible industrial and socioeconomic revolution that can lead countries towards much more growth. He described how South Korea is forging ahead towards the 'smart society' with various IoT projects and 5G. He recognised that regulating innovations such as self-driving cars can be difficult and mentioned a public-private committee that will focus on regulation, and there is a big emphasis on security with an IoT security alliance. Korea has also made important moves in protecting personal data.

Muhammad Aslam Hayat, head of corporate affairs at Telenor Pakistan, described the pressures on telecoms operators, including needing to cut costs and innovate while competing with over the top (OTT) players, and how regulation often lags behind and can introduce artificial barriers.

Finally, Johan Adler, Ericsson's head of government and industry relations, South East Asia and Oceania, picked up the innovation theme, mentioning technologies such as artificial intelligence, and systems such as Blockchain that could radically change a whole industry (in this case banking), and also commented on ethical dilemmas in innovations such as driverless cars. There will be need to be a step up in regulatory and moral thinking, he reckoned.

IN BRIEF: OTHER EVENTS IN THE IIC'S BANGKOK WEEK

The International Regulators Forum (IRF), held at Thailand's National Broadcasting and Telecommunications Commission, and involving 39 countries, focused on the following themes:

- Pressures of convergence – merging telecoms and media regulators, regulating market failure with an eye on the public interest, citizen protection, and modernising regulation were just some of the topics in this in-depth session.
- Cross-sectoral collaboration – clash of regulatory cultures (e.g. with financial over mobile money), the division between competition and regulatory oversight, regional coordination, and more.
- The level playing field – are we regulating with old rules in net neutrality vs traffic management? What are society's needs? Should the rules (which might include regulations or licence requirements) be based on what is consumed, rather than how it is supplied?
- Connecting the unconnected – how effective are universal service obligations? Is there a lack of incentives to lay cables where mobile is dominant?
- Spectrum and 5G – sharing continues to be a key topic, and discussion also took in hoarding, incentive auctions, and not least, pinning down a definition of 5G.
- Streamlining regulation – how regional regulator groups are working, and issues such as roaming and the jurisdiction of the cloud.

Breakout groups

The annual conference also has a set of breakout groups that are often very lively – this year's topics included the future of universal service obligations (a recurring theme throughout the conference); smart cities; tackling piracy (which was especially lively); spectrum allocation; and cybersecurity. The spectrum group heard that it is easy to get sucked into the 'mobile broadband bubble', but there are many other users of radio spectrum and other important systems such as satellite to consider.

Workshops

Two workshops took place during the annual conference.

- The first, on building a responsible advertising policy framework, examined issues such as ads in the 'burgeoning' digital ecosystem and collaboration among countries and with other national agencies.
- Eliminating spam and nuisance communications was the topic of the second workshop, run by the Canadian Radio-television and Telecommunications Commission. It included a number of case studies, including Canada's new anti-spam legislation, and discussed how to bridge the gap between policy and enforcement.

DIGITAL CONTENT

A key question addressed by the next panel was: In a highly competitive OTT world, what is being done to ensure high quality, market driven, accessible content with local culture and language also preserved? Moe Thu Zar Aung, director at Myanmar Radio and Television (MRTV), gave insight into how the country is opening up broadcasting with more content, including from private companies, and the transition to digital, and is also setting up a new content regulatory body, although like other countries there is debate about how online internet content fits in.

Joe Welch, who heads government affairs, Asia, for 21st Century Fox, pulled no punches in saying that there is a 'tilted' playing field, where traditional broadcasters are subject to content regulation, licensing and taxation, whereas the OTT players have less of all of these. Fox, said Welch, is also "playing in the OTT space" and would like less regulation for existing players, but "we do not wish for more regulation of the [OTT[guys". Welch said that the 'tilt' will probably sort itself out over time, country by country, but in the meantime: "Don't make it worse." He also touched on piracy, malware and pornography, saying that "the legal framework to deal with all this is totally outdated".

Kuek Yu-Chuang, managing director, Netflix Asia-Pacific, followed by saying that all can agree that more choice for consumers is a good thing. He said that Netflix has reached a global scale where it can invest in local content in local languages, and the OTT players are now adding such value in a number of countries. On piracy, he added that when Netflix enters a new market piracy rates come down. A recent OTT entrant, iflix, was represented by Michelle Landy, head of commercial and corporate affairs. The company is targeting online entertainment in emerging markets with a low-cost service, and she said a key barrier to take-up is lack of locally relevant content, and western content needs to be subtitled. Entering new markets also needs careful liaison with regulators on factors such as censorship guidelines, she added. As for piracy: "It is our biggest competitor."

Lastly, Tran Tuan Anh, director of policy and regulation, Vietnam Telecommunications Authority, described the current boundaries between telecoms and content regulation, and the challenges of maintaining a competitive environment given that much traffic and bandwidth originates from outside the country.

THE DIGITAL CITIZEN

The final main session of the conference was about the rights and priorities of people in a digital world. As chair Ann LaFrance commented, privacy and cybersecurity have become dominant issues recently and both government and industry face having to balance consumer protection with making use of data for various ends.

Cordel Green, executive director of the Broadcasting Commission of Jamaica, made a powerful case for new thinking about regulation and the need to act quickly, as new technologies

A panel at the International Regulators Forum gets underway

such as artificial intelligence and machine to machine communications are fast undermining conventional rules, while massive global apps such as Pokémon Go are busy collecting vast amounts of personal data. Green said that digital literacy is crucial and regulators could look to working with industry on technical privacy fixes. Above all, regulators cannot afford to sit and wait before intervening conventionally, he said – "That's outdated thinking."

Detailed analysis of privacy was provided by Christine Runnegar, director, security and privacy policy, at the Internet Society. Let's talk about 'meaningful privacy', she said, which is really vital for reinforcing trust in the internet and in society and a way forward is through 'data ethics', which allows people to exercise effective control and choice over their personal data. Runnegar went on to discuss a 'second wave' of data portability and the implications of Europe's new data protection regulation.

> **Digital literacy is crucial and regulators could look to working with industry on technical privacy fixes.**

Monica Desai, director of public policy at Facebook, highlighted that progress is being made in several areas of regulatory concern, including catering for people with disabilities and safety checks in emergencies, both of which Facebook now has tools for.

Donald Connor, group director for regulatory affairs at VimpelCom, noted the huge surge in cross-border data flows and that many countries do not have data protection regulation.

Rounding off the panel, Kyung-Sin Park from the Korea University School of Law, and director, Open Net Korea, said data protection laws are vital to protect powerless individuals who enter into data transactions with powerful agencies and companies. He also reiterated the need for companies to practise 'data ethics', which companies such as Google are doing, unlike some firms in traditional industries.

THE AGENDA FOR EUROPE

GEORG SERENTSCHY sets out the agenda for Europe in 2017, which looks likely to be critical in developing aspirations for the digital single market

This short article aims to list the key policy options and regulatory topics which are high up on the priority list of policymakers, regulators, digital firms and telecoms operators in Europe, and many of which are being closely watched globally. The driving forces for the current changes are the ongoing stream of new, innovative services delivered by OTT players, the growing importance of ubiquitous ultra-fast and very low latency (gigabit) networks and – in the European context – the draft Electronics Communications Code published by the European Commission in mid-September 2016.[1]

1 – A SHIFT OF THE REGULATORY FOCUS IN THE EU

- Connectivity and investment are becoming one overarching principle (in the previous EU regulatory regime it was solely competition).
- There is a need to revisit the concept of significant market power (SMP) regulation, taking into account operator's investment plans, coverage, universal service, public funds, symmetric regulation, treatment of copper and invitation for co-investing, as a driver to facilitate investment and lower the regulatory burden – a concept fit for purpose for the 'gigabit society'.
- The EU broadband cost reduction directive[2] is an important cornerstone to deliver ubiquitous connectivity faster and more efficiently.
- We see many markets developing towards tight oligopolies, and national regulators and competition authorities are struggling with this situation because general and sector specific competition law does not have good and proven legal instruments at hand. In this context, it makes sense to take a pragmatic stance, as a leading policy expert recently expressed, by stating that minimising network monopoly is more important than maximising retail competition.[3]

2 – MASSIVE PUBLIC FINANCING OF TELECOMS INFRASTRUCTURE

Such financing has not been seen for decades and raises some crucial issues.

- What will competition authorities say on co-investment?
- Invitation to co-invest will be a way to relax harsh regulation from the past, but this might be perceived as an invitation for regulatory gambling. Therefore, an invitation to co-invest must be reasonable and verifiable.
- This calls for a revised role of national regulators as agencies to help improve connectivity in an efficient and effective manner.

3 – MODELS TO BUILD (NATIONAL) FIBRE WHOLESALE NETWORKS

Some of these models are based on public-private partnerships, some on new build and others are carved out from incumbent's networks. They also raise new policy and regulatory issues.

- Investment and innovation incentives.
- Functional and ownership unbundling and potentially the end of vertically integrated telecoms players.

> **"Minimising network monopoly is more important than maximising retail competition."**

4 – VERY HIGH CAPACITY NETWORKS

The Commission has presented – as part of the new code – the concept of very high capacity (VHC) networks, including G.fast, a kind of last resort technology to exploit copper-based assets. This aims to achieve ubiquitous connectivity for the gigabit society by 2025 across EU but raises some questions.

- Is the principle of technology neutrality still in place and at the same time acknowledging that fibre is ultimately the superior infrastructure for both fixed and mobile networks?
- Is the inclusion of G.fast in the VHC concept the best way to achieve quick connectivity wins, or is this only a lukewarm compromise which will ultimately slow down investment in fibre?
- Or should copper be decommissioned earlier?

5 – OVER THE TOP (OTT) REGULATION

- Interoperability requirements for messaging platforms.
- Obligations for providing emergency call capabilities.

6 – NET NEUTRALITY

Net neutrality rules (including zero rating) will remain a hot topic everywhere.

- In the EU, the body of national regulators, BEREC,

REFERENCES

1 Proposed Directive establishing the European Electronic Communications Code. bit.ly/2caAmrr

2 See bit.ly/2jnEPcE

3 Feasey R (2015). Some comments on European regulation. bit.ly/2iwx5Fe

4 Roberto Viola (head of DG Connect at the European Commission), has said that "...800MHz awarding in EU was a disaster".

has recently published net neutrality 'guidelines' (which are in essence a new piece of legislation), on how net neutrality will work in practice and what it means for innovation.

- What kind of commercial practices (for example bundling of services under a specific data plan) will be accepted or not by authorities? In the UK, for example, Virgin Media (part of Liberty Global) has launched 4G mobile services that let users access WhatsApp and Facebook Messenger without using up their data allowance.
- Will there be a homogenous practice across Europe? Rather not, under the current regime.

7 – SPECTRUM

Spectrum, the life blood of the mobile industry, is becoming even more important.

- Will we see coordinated awarding methods and timing for the next series of spectrum bands (700 MHz, 2.1 GHz, 3.4-3.8 GHz) across Europe?
- Will there be perpetual licences (at least 25 years) for usage rights?
- Will Europe again miss the boat in international competition as happened in 4G?[4]

8 – DIGITAL SINGLE MARKET: REGULATORY OVERSIGHT

The digital single market is one of the hottest policy topics in the EU (and is also being considered in other regions such as Latin America). How will the EU square the circle to create an effective and workable regulatory set of policies and oversight for a digital single market, supported by national regulators (NRAs) and member states? The core issue is to orchestrate the interplay between different instruments to speed up ubiquitous connectivity by a combination of infrastructure competition, state-aid, co-investment, coverage obligations and universal service. But how will the regulatory oversight architecture in Europe be organised? Is the current system future proof, or should BEREC be transformed into a European agency, as the European Commission has proposed? A more realistic option – and a way to get out of the current entrenched situation – could be a three-tier model for the European Commission, BEREC and NRAs with distributed tasks and responsibilities, each of these dovetailing with the next level:

- European Commission in charge of the legal framework, and DG Connect taking care of policy setting, which has been much neglected
- BEREC in charge of translating the legal framework into principles guiding the operation of the NRAs and advising lawmakers on what works and what does not
- NRAs in charge of applying these principles in a bespoke manner depending on national/regional circumstances; monitoring market developments and enforcing rules.

9 – DIGITAL SINGLE MARKET: ROADMAP

High up on the EU policy agenda is the roadmap to create the European digital single market and to reach the connectivity targets. This requires a set of measures on both the supply and demand sides. The new communications code has these measures incorporated with wholesale products to ease market entry and to create harmonised offers on the supply side and harmonisation on the demand side (consumer rights). This sounds logical, but is it worth the high price at this point in time?

Wholesale offers, if designed for pan-European applicability, might no longer fit national demand; harmonisation for end-user rights might lead to opposition; and so transnational demand might be low. The current policy debate in the EU hovers between the political ambition expressed by the European Commission and a comparably low appetite of some member states to follow this route. Many countries prefer to follow a path based on the subsidiarity principle. BEREC officials call this 'BEREC's rootedness in its membership', meaning that independent NRAs will have the last say in BEREC and not the European Commission.

This raises the question, is it worth starting the battle for a fully-fledged digital single market right now given the current state of the debate? Further, would a digital single market built on the mobile sector be a suitable 'plan B', a kind of transitory option? Mobile is the innovative force and the end-user interface in many countries. The mobile industry is facing high investment and short innovation cycles but mobile devices are becoming a key tool in everyday life.

It would be much easier to develop a European industrial telecoms policy for mobile and so create harmonisation across Europe for this as a start. Would this be an option for the European Commission if its plans fail because of national resistance? What are the minimum requirements for such a partial single market – and is the potential of mobile reflected appropriately in the code and various EU policies?

I leave these questions open for other European and global commentators for the year ahead.

Andrus Ansip, the European commissioner in charge of the digital single market, spoke recently at the Digital Assembly in Bratislava, where he highlighted obstacles to data flows that are standing in the way of the development of the market, and the imperative to adopt the new General Data Protection Regulation. He said: "Within the single market, data has to be able to move across national borders and in a single data space. This is not what Europe has today. Instead, we have a series of legal and technical barriers that constrain cross-border data flows. I have heard advocates of these restrictions refer to data protection and security as reasons to keep limitations on free movement of data in place. Let me be clear. The vast majority of these constraints have nothing to do with protecting privacy or fighting security threats." Why, he asked, should company, financial and health data be stored forcibly inside particular borders in a single market? What the public authorities need is access rather than storage, he added, citing Denmark as recently changing its law on book-keeping data: companies can now store their data anywhere, as long as tax authorities have full access. "Forcible data localisation rules will not lead to better protection, but to fragmentation. This will be to the detriment of benefits for citizens, consumers, SMEs and society."

GEORG SERENTSCHY *is managing partner at Serentschy Advisory Services, Vienna, and senior advisor to global law firm Squire Patton Boggs in Brussels. He was CEO of RTR, the Austrian telecoms regulator, and chair of BEREC.*

UPHILL ROAD AHEAD FOR AUTONOMOUS VEHICLES

Connected and autonomous vehicles will be leading users of the internet of things and 5G technologies. But almost all of today's societal and regulatory issues will converge on road transport, as **JULIAN MCGOUGAN** reports

Ever since vehicles with internal combustion engines arrived they've maimed and killed their passengers and pedestrians, consumers have spent increasing amounts of their time inside them, and our environment has been paved over and filled with their noise and fumes. Millions of people are employed the world in the manufacture, service, repair and insurance of vehicles. Cars have provided freedom, made it possible to work in cities while living outside of them, and are often the most evident demonstration of wealth. In developing societies those who can afford a bicycle then want a moped; those who attain a moped then want a car.

But millions of consumers are effectively denied the opportunity for car ownership, temporarily or permanently, due to their age, insufficient funds, physical or mental health. Between 2001 and 2009, the proportion of all households in the US with no vehicle actually increased from 8.1% to 8.7%.

Even though a car is usually one of the most expensive items a family will acquire, for a large proportion of the time they sit motionless, parked and depreciating. And, in recent decades, climate change has meant that the view of the car has changed in the developed world.

Technology, in the form of connectivity and autonomy, is bringing its own changes, especially in parts of the developed world. But technology may be advancing faster than the readiness of governments, regulators and current car users to deal with their implications. Preparing for this new technology is

raising moral and regulatory questions that (currently) have no easy answer.

Too often new technologies are pushed to consumers on a 'because we can' basis, before the technology is perfected, and often before the problems they address have been identified. Fortunately for those pushing autonomous vehicles, there are a range of problems with current transport options which can be addressed by these new technologies. For instance, while the real cost of acquiring a car has fallen over time, Americans spend more money on cars (owning and running) than they do on food – and despite this their cars have a usage rate of only around 4%.[1] Estimates suggest that autonomous vehicles could multiply current utilisation rates by almost ten times.

In addition, the average speed of commuting in the US has been declining in all metro areas.[2] Congestion incurs significant costs in lost worker productivity and fuel. Research also suggests that congestion can dampen subsequent employment growth.[3] In the US, the National Highway Traffic Safety Administration (NHTSA) has indicated that congested roads are one of the main causes of traffic accidents. A road network largely designed for a population of 150 million, rather than more than 300 million today, is a contributory factor. In the UK, the cost of lost working hours due to congestion in 2015 has been estimated as £4.5 billion.[4]

The car is therefore a product that could perform so much better – certainly safer. There were 1.25 million road traffic deaths globally in 2013.[5] Around 30,000 people a year are killed on US roads, against fewer than 2,000 in the UK. Per head of population, the chances of a fatal accident in the US are nearly three times higher than in the UK.

Among all vehicles in the US, there is a fatality every 94 million miles (150 million km). Worldwide, there is a fatality approximately every 60 million miles (95 million km).[6]

In 2015, and after a steady decline over the last four decades, in the US highway fatalities suffered the highest annual percentage increase in 50 years. In the first six months of 2016, highway deaths jumped another 10.4%.[7] Insurance companies believe that the increasing use of electronic devices while driving is the biggest cause of the rise in road fatalities, so increasing numbers of connected cars (with entertainment and information streaming in) may add to the fatality count.

In the UK, driver error is believed to be the main reason behind over 90% of all crashes. In 2014, 44% of road accidents in the UK were caused by a failure to look properly.[8] Globally, the economic cost of crashes is estimated to range from 1% of GNP (low income countries) to 2% of GNP (high income countries).[9] Surely autonomous vehicles could do better than this?

LEVELS OF AUTONOMY

Unsurprisingly in these early days autonomous driving systems aren't infallible, but it is questionable how objective the media reporting of accidents – when these systems were active – has been recently. The high profile of Tesla means that many commentators focused on the unfortunate death of Joshua Brown when his self-driving Tesla Model S crashed in May 2016 in Florida, rather than on the 210 million kilometres that Teslas had driven with the autopilot technology engaged before this first known fatality.

As Tesla commented on the accident: "Statistically speaking, the autopilot is still safer than the average vehicle," a point which Brown may well have agreed with as in April 2016 he had credited Tesla's autopilot with saving him from an accident on an interstate highway, although this required him to take control back from the system.

Additionally, with 'fleet learning', autonomous vehicles share their learning. When a human in control of a vehicle has a near miss, or an accident they walk away from, they hopefully learn from that experience. However, when something unexpected occurs with an autonomous vehicle, that learning event can be shared with all other autonomous vehicles – or at least those from the same manufacturer.

So how soon before autonomous vehicles are on our roads? Although fully autonomous driving may be a while off, connected cars have been in the market in developed countries for more than ten years and human drivers have been progressively ceding control with technology such as cruise control, ABS non-slip brakes, lane departure alert, parking assist and pre-collision systems to apply the brakes. Mobile 4G hotspots are also being enabled in cars, and 4G is being trialled in apps such as warnings of accidents and fast cars moving behind to overtake, and fully-fledged wireless infrastructure and standards for connected cars will no doubt arrive along with 5G as it integrates with 4G to enable massive real-time connectivity and low latency (see also panel, page 16).

"The cost of crashes is estimated to range from 1%–2% of GNP."

Because of the continual progress towards autonomy, a classification system for autonomous driving is often used, whereby at Level 3 drivers can engage the autopilot but they are expected to remain responsible for their vehicle and take back control when needed. Only with Levels 4 and 5 is no driver intervention required and, at level 5, there may not even be a driver or a steering wheel.

The Tesla Model S, the poster child for autonomous cars, currently operates at Level 3 autonomy, but in October 2016 Tesla announced that all future cars would be upgradeable to Level 5, with improved cameras and sensors, a more powerful computer to handle processing of data from sensors, and a future software update to make it all happen.

A month earlier, Uber started picking up passengers with self-driving test cars in Pittsburgh, Pennsylvania – with an engineer on hand to take control if necessary. In Milton Keynes, England, an autonomous car (with driver on board) has recently been tested for the first time on UK streets. In

France, the world's first driverless bus service began carrying passengers in Lyon – albeit, to comply with current legislation, this operates separately from other traffic.

Mary Cummings of the Humans and Autonomy Laboratory, Duke University, dampens operators' enthusiasm: "Right now, artificial intelligence is not nearly as smart as people would like it to be. We're nowhere near a car that can drive itself under all conditions at all times, but we will see cars that can drive themselves very reliably under slow conditions and in environments that are relatively structured, on freeways, for example, with additional sensors that we can put in the roads."

But autonomous vehicles are coming, so we should ask: Are drivers and policymakers ready, and what might the implications of mass adoption be for society?

KEEP ON TRUCKING

Certainly many consumers are currently apprehensive. According to a survey[10] released early in 2016 three out of four US drivers said they would be afraid to ride in self-driving cars. Then again, had customer surveys existed at the time of their introduction, the prospect of being a passenger in a train or a car may have produced similar results. We can expect familiarity to reduce the level of fear.

But while cars may take a while to overcome concerns – warranted or otherwise – the real short-term issue for autonomous driving to address, though, is probably trucking.

In the US, the trucking industry is the principal means of moving goods, and it's a huge business employing many people – in fact, truck driving is the most common job in the country. Yet partly because younger generations aren't attracted to these jobs, there's a shortage of drivers, and trucks need to operate almost around the clock to keep up with demand, a situation made worse by antiquated technology used by shippers, brokers and carriers. Drivers often sit idle, waiting for quotes or pick-ups.

As if that weren't enough, more truck drivers in the US are killed on the job than workers in any other occupation. In 2016, in the US more people will be killed in traffic accidents involving trucks than in all domestic airline crashes in the previous 45 years combined.

Driverless trucks will come because they have to – and they can drive nearly 24 hours per day, drive more fuel efficiently, and remove the labour cost of shipping freight. There will be a range of hazardous or inhospitable environments, such as northern Canada or the Amazon, where industry will be keen to avoid the cost of hiring trained truck drivers.

But might regulators, notoriously slow to adapt to new technology, be an obstacle to adoption? In the UK engaging self-driving mode is currently prohibited on public roads. This is changing – slowly – so that by 2019 UK consumers should be able engage self-driving mode and take their hands off the wheel for up to three minutes – but only on a motorway (highway).

In the US, things have progressed further, with the federal government addressing the potential obstacles to adoption presented by differing rules in US states by issuing an automated vehicles policy in September 2016, introducing guidance to states and best practice.

> **"Will pedestrians become more reckless around autonomous vehicles?"**

And to ensure that safety improvements resulting from autonomous vehicle use weren't reduced simply because electric hybrid vehicles (whether autonomous or not) can be so quiet that pedestrians may not register their presence, the US has already started recently requiring[11] that by September 2018 half of all new electric and hybrids must have audible alerts, with all new electric and hybrids by September 2019. This is estimated as preventing up to 2,400 pedestrian injuries a year.

SAFETY IN MIND

As might be expected, the greatest concern relates to safety – ensuring that autonomous driving doesn't add to accidents (taking account of how human drivers react to their presence) and how liability for accidents should be determined.

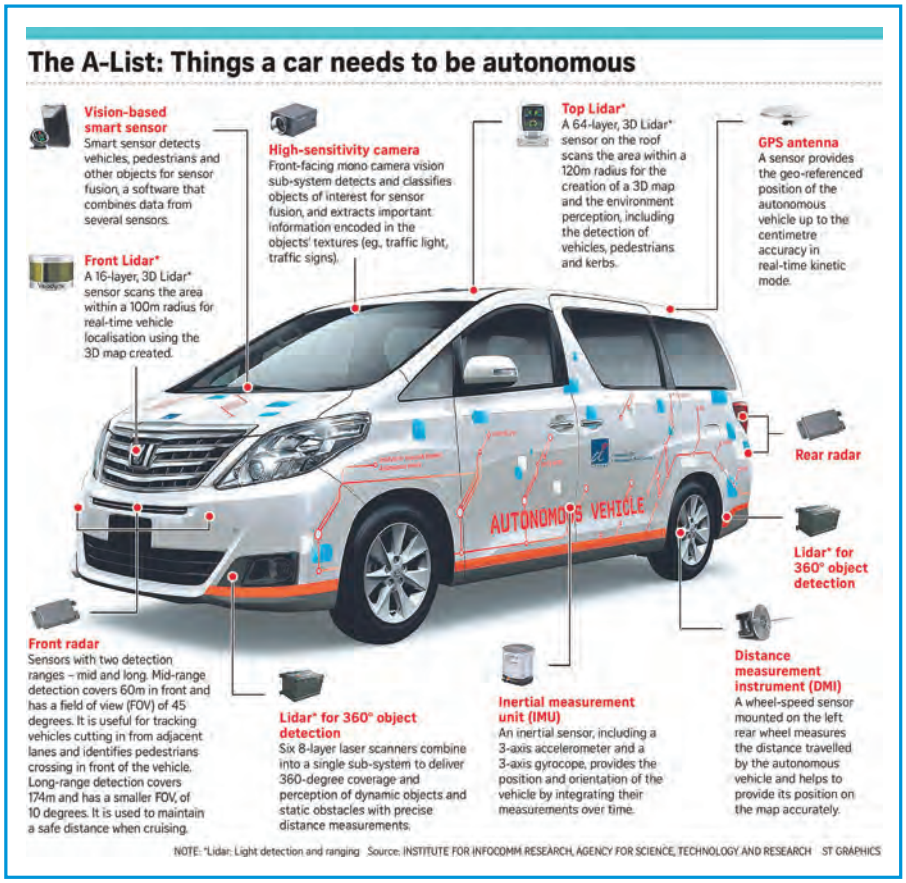
Despite the enormous progress made towards fully autonomous driving, there is a considerable difference between highway driving and driving in complex, urban environments, where the vehicle must be able to accurately identify and understand dozens of unique objects. As urban trials of autonomy are showing, there is a considerable range of events occurring which currently may need human intervention, such as sudden lane changes, illegal parking, broken down vehicles, and vehicles backing into main roads.

As Steven Shladover of University of California, Berkeley puts it: "Soon electronic chauffeurs will take us wherever we want to go, whenever we want, in complete safety – as long as we do not need to make any left turns across traffic. Changing road surfaces are a problem, too. So are snow and ice. It will be crucial to avoid traffic cops, crossing guards and emergency vehicles. And in an urban environment where pedestrians are likely to run out in front of the car, we should probably just walk or take the subway."

What if pedestrians actually became more reckless if they thought autonomous vehicles would see them and brake? What if drivers altered behaviour? Humans may not react the way an autonomous vehicle's artificial intelligence (AI) had been trained to expect. A widely-held view is that some drivers of Volvo cars drive more recklessly than drivers of other brands because they have a false sense of security.

Anticipating altered driver behaviour, a trial of Volvo driverless cars to be held in London in 2018 is planned to use unmarked cars after researchers suggested that human drivers may try to overtake and cut off cars identified as being self-driving because they would be perceived as being law-abiding and would take avoidance.

So, there is much work still to do. But having started down the road to full autonomy, stopping for too long on Level 3 may bring additional risks.



We have an indicator of how human drivers may react to partial autonomy in vehicles from the psychological research conducted by NASA into how aircrew react to automation: what applies in the cockpit may apply in vehicles. Unfortunately what NASA found is that the better automation works, the less we feel willing or able to monitor, having a false sense of security. This makes driving current Level 3 vehicles potentially more hazardous than their owners realise, and drivers have less time to react to events – and in two dimensions only – than aircrew do.

Germany's Federal Highway Research Institute (BASt) found that the autopilot feature of the Tesla Model S constitutes a 'considerable traffic hazard' after a Model S with autopilot engaged crashed into a bus in September 2016. The report found that the car didn't follow the right road markings in a construction zone – and when there were no road markings, the car simply followed the vehicle in front of it. Additionally the report highlighted that the 40 metres behind the car where the sensors currently look may be insufficient for the stretches of autobahn where there are no speed limits.

Of course machine learning would eventually adjust for such real world conditions. But in considering how best to introduce autonomous vehicles, governments and regulators must have regard to the special circumstance of the transition phase when roads contain both human and autonomous drivers. Over time, humans (drivers, passengers and pedestrians) would also adjust and, hopefully, most of their early anxiety would be laid to rest. But at least for now that anxiety is real, with a recent survey[12] finding that 41% of drivers would feel uncomfortable driving alongside an autonomous vehicle.

INCENTIVES AND DATA REGULATION

But government may conclude that 'nudging' late adopters to stop driving themselves is a worthwhile objective. Without nudges the transition period may be very long. This technology will tend to be offered first in vehicles which have above-average sticker prices before, like every other in-car technology before it, gradually being offered on cheaper vehicles. And while we wait for the technology to be fitted into the type of cars most drivers own, we need to recognise the millions of cars already on the roads. In the US, the household vehicle fleet continues to age – the most recent data shows the average vehicle owned by US households is 9.4 years old.

The obvious nudges to encourage humans to stop driving themselves are financial – increasing taxes over time on new vehicles that don't offer full autonomy. If autonomous driving does substantially reduce the number of accidents and injuries, we can expect that to be evidenced in very favourable insurance premiums for humans who give up the steering wheel – if insurance companies don't move quickly enough in that direction, expect car makers to offer their own tailored insurance.

There will also be some potential non-financial nudges, such as Level 5-only urban areas and lanes on highways with no speed limits, or driving licences which are easier to obtain specifically for Level 4 vehicles (since Level 5 vehicles will have no human driver, no driving licence may be required at all).

If driverless trucking is right around the corner, before many cars on the road are even capable of Level 3 autonomy, dedicated on- and off-ramps so human drivers can bring trucks to the freeways before the autopilot takes over may be desirable, as may dedicated highway lanes for slow-moving (driving more fuel-efficiently) driverless trucks.

As there will still be accidents involving autonomous vehicles, perhaps particularly so during the transition phase, insurers will want to determine liability, which means access to at least some of the data generated by the autonomous vehicles involved.

The US Federal Government has recently proposed that "vehicles should record, at a minimum, all information relevant to the [crash] and the performance of the system, so the circumstances of the event can be reconstructed".[13] That record will then be shared with federal regulators and other manufacturers.

Manufacturers are nervous of what data sharing will entail. But in its response, Apple agreed that "companies should share de-identified scenario and dynamics data from crashes and near-misses. Data should be sufficient to reconstruct the event, including time-series of vehicle kinematics and characteristics of the roadway and objects. By sharing data, the industry will build a more comprehensive dataset than any one company could do alone. This will allow the industry to design systems to better detect and respond to the broadest set of nominal and edge-case scenarios."

In the UK, the insurers' trade body wants its members to have access to data covering a period 30 seconds before and 15 seconds after an incident. It would include the exact location of the vehicle, whether it was in autonomous mode or under the control of the driver, and whether the motorist was in the driver's seat and had a seatbelt on. In addition to supporting prompt insurance payouts, autonomous vehicle brands would benefit if insurers validated their faith in the technology.

The UN body which agrees international regulations on vehicle safety is due to bring in new rules on data collection in 2019 and the insurers are hoping to influence that process.

Many car brands developing autonomous vehicles have reservations about third party access to 'their' data, which is why companies have emerged offering to be neutral third parties, entering into arrangements with car makers and original equipment manufacturers (OEMs), making data available in accordance with prevailing regulations and business policies.

There is arguably a need for the insurance industry and OEMs to agree common standards for data access, usage and security. Additionally consumers will be looking for reassurance about how secure the data coming off vehicles are.

Chinese researchers hacking into a Tesla car in September 2016[14] and applying the brakes from 20 kilometres away won't have done much for consumer confidence, even if (on that occasion) the hacking experts reported their findings and Tesla deployed an over-the-air (OTA) software update within just ten days of receiving that report.

Should regulations have a role here, or is the reputational risk for each brand sufficient? Currently consumers shopping for a connected car have no more knowledge of how secure from hacking it may be than they do when shopping for a WiFi router or any domestic internet of things device, such as a baby monitor.

The speed at which society gains the benefits from adoption of autonomous vehicles or 'mobility as a service' (MaaS) could be reduced if consumers aren't confident about data security. Research[15] for the Internet Society (ISOC) found that 59% of internet users were likely not to do business with a firm that had suffered a data breach. When the 'thing' in question is a connected car or a healthcare device, ISOC says disclaimers aren't good enough, because "the hack can also extend to personal safety, potentially at the cost of life and limb".

CALLING ALL CARS

No matter how much processing of data is done by the car in real time or dumped to the cloud, for data to be accessed (legally or otherwise) it needs to be got off the vehicle. OTA downloads will also require connectivity. This is where any failings in connectivity (often a result of both coverage obligations and market forces, based on current demand characteristics), may hold back the progress autonomous vehicles could make.

And there could be a lot of data. Intel estimates that, by 2020, the average person will generate 1.5 GB a day, while the average autonomous vehicle will produce 4,000 GB a day. Presumably most of that data would never leave the vehicle, but Hitachi estimates that 25 GB[16] of data would be uploaded to the cloud per hour. Even if autonomous vehicles were able (or required by regulators) to roam across home market cellular networks, unless satellite connectivity were also integrated there would be losses of connectivity – in many rural areas, even in developed countries, there are plenty of holes in cellular connectivity.

Government and industry may have to work together, including utilising existing assets, to

DRIVING THE AGENDA

■ The US Department of Transport has an extensive portfolio of activities. In September 2016 it published a federal automated vehicles policy and is currently consulting on enabling vehicle-to-vehicle (V2V) communication technology on all new 'light-duty' vehicles, especially for safety applications. Guidance for vehicle-to-infrastructure (V2I) communications is expected soon. See also the Intelligent Transportation Systems Joint Program Office at: its.dot.gov

■ The FCC allocated 75 MHz of spectrum in the 5.9 GHz band as far back as 1999 for use by intelligent transport systems, not least to enable dedicated short-range communications (DSCR) and vehicle safety apps, and is looking at how the band can be shared.

■ In November 2016, the European Commission adopted a strategy on cooperative intelligent transport systems (C-ITS), "to facilitate the convergence of investments and regulatory frameworks across the EU, to see deployment of mature C-ITS services in 2019 and beyond". It was already running C-Roads, which gathers deployment activities in member states, and initial work on a C-ITS platform was reported on in early 2016. This is now in a second phase. See bit.ly/2eYdpoe

■ The 5G Automotive Association (5GAA), established in September 2016, has an 'A list' membership – Audi, BMW, Daimler, Ericsson, Huawei, Intel, Nokia and Qualcomm – and the goal of addressing "society's connected mobility and road safety needs with applications such as connected automated driving, ubiquitous access to services and integration into smart cities and intelligent transportation". In a white paper, it makes the case for cellular-V2X (C-V2X, or 'vehicle to everything') 3GPP-based technology at the radio level as an essential enabler for connected transportation services, rather than the IEEE 802.11p vehicular amendment to the WiFi family. See 5gaa.org

■ Qualcomm, as a wireless and chip player, has established a connected car reference platform and made a pitch to lead in 5G cellular C-V2X technologies. It says V2X will be much more than collision avoidance, with apps such as warnings of vulnerable road users and 'platooning' on highways, and says it requires harmonised spectrum of at least 70 MHz. The company is developing 4G technology called LTE Direct for device-to device communications, which can be used when a car is out of wide area coverage. A key aim of C-V2X is to increase reaction time over 802.11p/DSRC technology, as set out also by 5GAA. 5G and its new radio interface will then enable advanced applications such as fully autonomous driving and the ability to 'see' ahead of a truck in front of your car.

■ But the Car 2 Car Consortium, whose partner members include Audi and BMW, says that IEEE 802.11p, also known as ITS-G5, is an essential cornerstone towards safe, connected automated driving and the group "strongly supports the recommendation developed by the European Commission's C-ITS deployment platform to use this system for short range communication in the 5.9 GHz band". For details see car-2-car.org

increase connectivity to remove a potential obstacle to connected and autonomous vehicles delivering their full benefits.

One area that is receiving interest from regulators is the AI deployed in autonomous vehicles. Currently the inner workings of different AI systems are commercial secrets, yet how their algorithms work, what data they are fed, and how they are trained will affect the decisions they take on our behalf. For example, should an autonomous car always protect its passengers at the expense of pedestrians? And should child pedestrians be valued more highly then pensioners? Should passengers be responsible – and legally accountable – for such choices, or the AI providers, or regulators? Even the creators of systems cannot accurately predict the decisions they make.

As a research study[17] conducted during 2015 in the US found, if the ethics of the autonomous vehicle's AI were aligned with that of its passengers, it would put those passengers first. The authors also write: "If a manufacturer offers different versions of its moral algorithm, and a buyer knowingly chose one of them, is the buyer to blame for the harmful consequences of the algorithm's decisions?" Should regulators require that all self-driving vehicles' ethics share the same value of protecting the greatest good, even if that's not what the car's passengers would want?

BENEFITS AND WINNERS

Assuming that, encouraged or otherwise, consumers – at least in developing countries – adopt fully autonomous vehicles, there are a range of benefits beyond the considerable anticipated benefits of fewer traffic accidents and reduced emissions (if all planned autonomous vehicles are electric). The typical US commuter spends 250 hours a year in their car. The combination of autonomous driving and in-car entertainment will extend the office and the living room, the car becoming the second space people use for entertainment and leisure (potentially with more space and comfier seats than today's cars). There will be more time and space for consuming media streamed in by 5G, and communicating with friends, family and colleagues. Autonomous cars may undermine much of the attraction of rail. This may create a battleground for attention – a prize surely worth fighting for.

Freed from the inconvenience of when drivers want to work, goods will be delivered at the customer's convenience by vehicles designed purely for that purpose, with reduced cost.

One company, Veniam, is already turning fleets of connected vehicles into a mesh network with the capability of covering a city with public WiFi – the company describes itself as delivering the 'internet of moving things'. Combining real-time data from connected vehicles' sensors could provide traffic control and urban planners with invaluable insights, such as optimising signage or traffic lights at intersections or identifying potholes. There would no doubt be many companies (including insurers) who would like to be able to study behavioural data – will consumers be able to opt out of that?

The benefit most eagerly awaited is probably fewer vehicles on our roads, with fewer accidents (and resulting delays). However, although autonomous vehicles should be able to drive closer to other vehicles, accelerate and decelerate more quickly and safely, and potentially (communicating with each other) navigate intersections more efficiently, the real congestion game changer must be when adoption of autonomous vehicles enables adoption of MaaS.

Indeed, without MaaS, autonomous vehicles could increase the number of vehicles on the road as autonomous cars are used by many of those currently excluded from driving: those without a driving licence (including children), those with physical or mental disabilities. Door-to-door pick up and drop off provided by retail and entertainment destinations could also add to congestion. On-demand access to autonomous cars should usher in a new range of mobility solutions, providing a service between public transit and ownership, without the disadvantages of relying on taxis.

This could change our environment quite radically, in ways that we may not be prepared for. What might homes and commercial buildings look like when they no longer need parking attached? In London, front gardens, which have long been turned into precious parking, will start to re-emerge (with consequential benefits for dealing with sudden downpours). Bars and restaurants will sell more alcohol. Traffic lights may become obsolete. Vehicles may look quite different, come in very different shapes and sizes, and won't need to withstand crashes in the same way.

...AND LOSERS

There'll be losers, too. A world where far fewer new vehicles are purchased, and the value of the existing vehicle stock falls faster than their owners expected, is one where main dealerships filled with new shiny cars start to disappear; the car plants so beloved of governments and trades unions cancel overtime, shut down production lines, and finally start to close – with unemployment impact, including with those plants' supply chains; car financing will reduce in size. Lower income families in areas where MaaS isn't offered may pay more for insurance to continue self-driving, opening up a new 'digital divide'.

Many more are employed to build and maintain road and parking infrastructure and to regulate how they are used. Without the need to take a break from driving, highway service stations and motels start to look vulnerable. No more traffic police. But higher vehicle utilisation should keep employed those who service cars.

MaaS, expected to be commercially available by 2021, will take time to have impact. Many current drivers are likely to resist autonomous driving, but those who've never owned a car may never see the point in doing so. So let's anticipate the many potential benefits of autonomous vehicles, but recognise the limitations; particularly the period when some cars are autonomous, but most are not, and governments and regulators haven't had their initial rules tested much. We need to use the time we have to fine tune regulations and manage public attitudes (using nudges as required).

JULIAN MCGOUGAN *is head of technology at techUK, a body that represents the UK technology industry. A passionate advocate for the potential for technology to improve people's lives, he has extensive knowledge of television, radio, mobile (cellular), spectrum, IoT and communications infrastructure.*

REFERENCES **1** National Highway Traffic Safety Administration. nhtsa.gov **2** National Household Travel Survey. nhts.ornl.gov **3** Hymel K (2009). Does traffic congestion reduce employment growth? Journal of Urban Economics 65 (2): 127-35. **4** Lex Autolease (2015). Where next for company cars? bit.ly/2fiYjNX **5** World Health Organization. Global Health Observatory (GHO) data. who.int/gho/en **6** Tesla (2016). A tragic loss. bit.ly/2i08Gla **7** Shepardson D (2016). US road deaths jump 10.4% in first half of 2016. Reuters. reut.rs/2dvbJ74 **8** Department of Transport (2014). Contributory factors to reported road accidents 2014. bit.ly/1KwSIAh **9** World Health Organization (2004). World report on road traffic injury prevention, bit.ly/1VQtFqL **10** American Automobile Association (2016). Three-quarters of Americans 'afraid' to ride in a self-driving vehicle. bit.ly/21FDQ8G **11** NHTSA (2016). NHTSA sets 'quiet car' safety standard to protect pedestrians. bit.ly/2i0RL8j **12** Goodyear/London School of Economics. Joint research on autonomous vehicles and driver attitudes. See: thinkgoodmobility.goodyear.eu **13** US Department of Transportation. Federal automated vehicles policy. transportation.gov/av **14** Petersen A (2016). Researchers remotely hack Tesla Model S. Washington Post. wapo.st/2h30S6E **15** Internet Society (2016). Global Internet Report. bit.ly/2ghHh3d **16** Connected cars will send 25 gigabytes of data to the cloud every hour. Quartz. bit.ly/1EfOswU **17** Crespi S (2016). When is it OK for our cars to kill us? Science. bit.ly/2h3UmOY

STRESS TESTING THE US PRIVACY FRAMEWORK

Two major planks of US privacy regulation, including controversial new broadband rules, are discussed by **AARON BURSTEIN** and **JOSHUA BERCU**

Two of the major developments in privacy over the past year highlight the unique system of privacy laws in the United States (US). The first is the EU-US Privacy Shield framework that the European Commission (EC) and the US government finalised in July 2016. Privacy Shield offers a simplified mechanism for companies to transfer personal data of European Union (EU) citizens to the US in a manner that satisfies the requirements of EU privacy laws. The second is the emergence of the Federal Communications Commission (FCC) as a key regulator of privacy and data security, particularly through a set of new privacy and data security rules it imposed on broadband internet access service providers ('broadband providers').

Privacy Shield and the FCC's rules are independent developments, but they illustrate the challenges that the US faces as privacy becomes an increasingly important issue for governments, consumers and international trade relationships. Privacy Shield demonstrates that US privacy law – and the web of US government agencies that handle privacy issues – can change in relatively short order to produce a unified response that meets complex challenges. The FCC's rules, however, demonstrate that the force of the shared principles underlying existing US privacy laws has limits. The FCC determined that broadband providers have "unique access to consumer data"[1] and used this finding to justify creating a distinct privacy regime for broadband providers that does not apply to other online actors.

OVERVIEW OF US PRIVACY LAWS

For much of the recent past, privacy law in the US has been treated as a set of mostly separate domains: the commercial realm, law enforcement, national security, and civil government data collection and use. Within the commercial realm, the US lacks a comprehensive privacy law that is akin to the EU's Data Protection Directive of 1995 and the member state laws that implement it. The Obama administration has described the US privacy framework as "flexible and effectiv[e]", resting on "industry best practices, FTC [Federal Trade Commission] enforcement, and a network of chief privacy officers", as well as federal "data privacy statutes [that] apply only to specific sectors, such as healthcare, education, communications, and financial services..."[2] Proponents of this basic consumer privacy framework – FTC authority across broad swathes of the economy, in addition to sector-specific laws – have said it provides a good deal of flexibility and reserves more prescriptive rules only for personal data that is particularly sensitive (e.g. health and financial information), or settings in which the use of personal data could be particularly harmful to individuals (e.g. for determining creditworthiness).

Critics have argued that the current framework fails to provide clear rules of the road outside of the sector-specific laws. Others have argued that changes in technology and markets have eroded the lines that divide industries regulated by sector-specific privacy laws from the rest of the economy. For example, health apps and wearable health devices generate personal health information that generally is not covered by HIPAA, the federal health information privacy law, even though the information may be the same as what doctors – who are covered by HIPAA – collect. The result is a system

that is difficult for companies and government agencies themselves to navigate for purposes of enforcement, compliance and policymaking.

If anything, this may understate how much the privacy landscape is changing. The separation of privacy into commercial, law enforcement, intelligence, and civil government domains looks increasingly questionable in practice. High-profile policy issues, including electronic surveillance law reforms, law enforcement assistance requirements, and encryption policy, routinely produce complex privacy questions that require input from multiple governmental and private sector stakeholders to answer.

PRIVACY SHIELD: A SUCCESSFUL RESPONSE TO A SERIOUS PRIVACY CHALLENGE

The most severe test of the US privacy framework in recent years is the aftermath of former National Security Agency contractor Edward Snowden's 2013 revelations of US signals intelligence collection activities. A focal point for the reaction to Snowden in Europe was the US-EU Safe Harbor framework, a voluntary data transfer framework that had been in place since 2000. The challenge to Safe Harbor became a crisis in October 2015, when the Court of Justice for the European Union struck down the EC adequacy decision that underlay Safe Harbor. The US and the EC met this post-Snowden challenge by finalising Safe Harbor's successor, the EU-US Privacy Shield Framework, in July 2016.

On the US side, this achievement required an unprecedented whole-of-government approach to overcome the institutional and legal barriers that separate commercial, law enforcement, and national security privacy domains. Privacy Shield also accentuates the FTC's role at the apex of consumer privacy enforcement agencies.

FROM SAFE HARBOR TO PRIVACY SHIELD

To appreciate the significance of the US approach reflected in Privacy Shield, it helps to understand the origins and purpose of its predecessor, Safe Harbor. Safe Harbor provided a way for companies doing business across the Atlantic to comply with the 'adequacy' requirement of EU privacy law, which comes from the 1995 Data Protection Directive, and which generally prohibits personal data transfers from the EU to countries that have not been found by the EC to provide an 'adequate' level of data protection. The US did not seek an adequacy determination, and by 1999 it became clear that the lack of adequacy (and the limitations on other grounds for legally transferring data from the EU to the US) posed a threat to US and European economic interests.

Safe Harbor provided a way to transfer data to the US with the assurance of adequate data protections even in the absence of a general adequacy determination for the US. At its core, Safe Harbor consisted of a set of data protection principles that companies could commit to follow. These commitments were enforceable by the FTC (and, for air carriers, by the US Department of Transportation). In July 2000, the EC determined that the Safe Harbor principles, together with FTC enforcement and the US Department of Commerce's oversight of Safe Harbor registrations, made Safe Harbor an 'adequate' system of data protection. This finding allowed companies that participated in Safe Harbor to transfer personal data from the EU.

Although Safe Harbor had its critics, only after the Snowden revelations did their criticisms gain sustained traction. In November 2013, the European Commission (EC) issued a list of 13 demands to change the terms of Safe Harbor, including changes to US surveillance practices. These demands became the basis for negotiations between the EC and the US Department of Commerce.

In the meantime, a lawsuit filed in Ireland against Facebook was making its way to the Court of Justice for the European Union (CJEU). The plaintiff in this case, Max Schrems, alleged that government access to personal data transferred to the US under Safe Harbor was subject to mass and indiscriminate government surveillance and therefore inconsistent with the fundamental right of data protection as defined under EU law.

In October 2015, in Schrems vs Facebook, the CJEU found merit in these claims and effectively killed Safe Harbor. The Schrems court did not hold that the Safe Harbor principles were insufficient, nor did it pass judgment on US surveillance (or commercial) practices. Instead, the CJEU held that the EC's Safe Harbor adequacy decision did not assess government access to consumer information, including any governmental privacy intrusions, and thus could not guarantee that data transferred under Safe Harbor receives adequate protections.

Still, the Schrems judgment posed an immediate challenge to the transatlantic economy. About 4,400 companies had signed up for Safe Harbor and relied on it to transfer data from Europe to the US. Unless they had alternative arrangements in place, those companies faced the risk of enforcement actions by European data authorities and the possibility of the suspension of data transfers.

WHAT PRIVACY SHIELD SAYS ABOUT THE US PRIVACY FRAMEWORK

The looming shadow of this possibility had stimulated a US government-wide response to the EC's Safe Harbor demands in 2013. Part of this response led to consequences for companies, which must meet more stringent standards under Privacy Shield than under Safe Harbor. For example, Privacy Shield imposes stricter accountability requirements for 'onward transfers' from a Privacy Shield company to a third party.

The more remarkable differences between Privacy Shield and Safe Harbor lie in the roles that US government agencies play in the new framework. Although Safe Harbor and Privacy Shield both contain derogations for "national security, public interest, or law enforcement" purposes, Privacy Shield includes detailed statements about safeguards that apply in these contexts under US law and policy. Specifically, Privacy Shield includes a letter from the Office of the Director of National Intelligence that explains the privacy and civil liberties protections that apply to the US intelligence community's signals intelligence activities, a commitment from Secretary of State John Kerry to provide an ombudsperson to handle inquiries from EU national authorities about the handling of personal data transferred under Privacy Shield, and a letter from the Department of Justice describing the privacy and civil liberties protections that apply to US criminal investigations. This whole-of-government effort is a sharp contrast to the Safe Harbor framework, which had no statements from US officials on intelligence or law enforcement matters.

On the commercial front, Privacy Shield spends much less space explaining the sector-specific privacy laws that govern commercial data practices in the US. Whereas online privacy enforcement was in its infancy when Safe Harbor was completed – the FTC's letter notes that the FTC brought its first online privacy case under FTC Act Section 5 in 1999 – the field has become far more mature. The FTC's letter in Privacy Shield states that the FTC brought nearly 40 Safe Harbor-related enforcement

actions and nearly 500 privacy-related cases in total,[3] engages in active order monitoring, and has obtained civil penalties from companies that apparently violated the FTC privacy or data security order issued against them.

Some important industry sectors are not eligible for Privacy Shield because they are exempt from FTC enforcement authority, including banks and telecoms common carriers.[4] But the picture that emerges from the FTC's submission to Privacy Shield is one of an agency that has broad authority, which it has used consistently and effectively to enforce consumer privacy rights.

HOW THE FCC'S ROLE AS A PRIVACY REGULATOR TESTS THE FRAMEWORK

While US government officials have touted the success of the FTC's approach to privacy abroad, a separate agency, the FCC, has emerged as a key and somewhat controversial regulator in the realm of US privacy and data security. Telecoms carriers, which now include broadband providers, are squarely under the FCC's regulatory authority, but 'edge' service providers – social networks, email services, and other online services – are not. The FCC approved new privacy and data security rules for broadband providers that are largely premised on the notion that broadband providers are uniquely situated compared with providers of other online services – a notion that the broadband industry has strenuously rejected.

FROM CPNI TO PII AND FROM TELECOMS TO BROADBAND

Privacy is not a new issue for the FCC – it has long imposed privacy and data security restrictions on telecoms carriers. In the Telecommunications Act of 1996, the US Congress set out a framework to cover carriers' protection and use of customer information, affording the most stringent protections to 'customer proprietary network information' or CPNI. This includes information related to a customer's use of a telecoms service such as the phone numbers called by a customer; the frequency, duration, timing and location of such calls; and any services purchased by the customer, such as call waiting. The FCC first implemented the statutory framework through rules in 1998. It since has amended the rules from time to time, with significant amendments in 2007 to address concerns about 'pretexting', which is the practice of pretending to be a particular customer or other authorised person to obtain access to the customer's call details or other private communications records.

Until recently, the FCC's privacy rules and enforcement activity focused on voice telephone service providers and their protection and use of CPNI. The FCC did not generally focus on other categories of customers' personal information (general, personally identifiable information, or PII). In the past two years, however, the FCC has expanded its privacy focus and role through two significant actions.

First, in October 2014, the FCC embraced new legal theories under which it can address carriers' practices involving information significantly broader than CPNI, including virtually any personal information about customers. Specifically, the FCC asserted that while the relevant statute imposed specific obligations for the protection and use of CPNI, the statute's reference to "a duty to protect the confidentiality of proprietary information of, and relating to ... customers"[5] indicated that the statute applies to a broader category of information – 'customer proprietary information'. The FCC deemed this class to include information that customers expect their carriers will keep private, including but not limited to CPNI and personally identifiable information.

The FCC also claimed that it could address data security practices, including misrepresentations about practices, through its authority to ensure that carriers' practices are "just and reasonable". It has since brought privacy and data security actions against major carriers and a cable company, and cited its new legal theories in other proceedings.

Second, in February 2015, the FCC altered the regulatory classification of broadband internet access services, placing such services within the statutory framework for telecoms carriers. Although the FCC's stated goal was to establish so-called open internet or net neutrality rules, the decision had implications for privacy by subjecting broadband to the CPNI framework.[6] The FCC's existing voice-centric CPNI rules, however, cannot be easily mapped onto broadband services. So the FCC began a proceeding to establish new privacy and data security rules for broadband providers.

FTC VS AT&T MOBILITY: CEMENTING THE FCC AS A PRIVACY REGULATOR?

A court decision in 2016 further complicates the US privacy framework, with significant implications for the FTC's and FCC's respective roles in regulating the privacy practices of telecoms service providers.

On 29 August, a panel of the US Court of Appeals for the Ninth Circuit held that the common carrier exemption to the FTC's general authority applies to any entity that has common carrier status, rejecting the FTC's claims that the exemption is narrow and applies only to common carrier activities. The case, which arose from the FTC's challenge to certain contracting and advertising practices connected to AT&T's 'unlimited' mobile data plans, leaves the scope of the FTC's authority uncertain.

Under the decision, it is clear that an entity with common carrier status is categorically exempt from the FTC's enforcement authority, regardless of what non-common carrier services (e.g. home automation services) such entity is providing, at least in the states covered by the Ninth Circuit. But it is unclear whether separate but related corporate entities, such as a wholly-owned non-common carrier subsidiary, are also exempt.

Although the court's decision had no legal impact on the FCC's authority, it could affect how the FCC decides to assert its role as a privacy regulator in light of any perceived regulatory gaps. When the FCC reclassified broadband service, it was understood that this removed the FTC's authority over broadband services. But FTC vs AT&T Mobility raised the question of whether the FTC ever had authority over certain broadband providers – namely those that also provided a traditional common carrier service like voice telephony. Further, it indicates the FTC lacks authority over broadband providers' non-common carrier activities – authority which the FTC asserted it had retained even after the FCC's reclassification.

The FTC has petitioned for a rehearing of FTC vs AT&T Mobility by the full Ninth Circuit. Appeal to the Supreme Court remains an option, as does the possibility of a legislative fix.

WHAT THE BROADBAND PRIVACY RULES SAY ABOUT THE US PRIVACY FRAMEWORK

In early 2016, the FCC proposed new privacy requirements for broadband providers. The FCC's proposed rules combined the FCC's historical approach to the protection and use of CPNI with the agency's more recent legal theories regarding its authority to address information practices with respect to any customer information. The result was a prescriptive and restrictive privacy framework that contrasted sharply with the FTC's more flexible approach. For instance, the FCC's proposed rules would have required a broadband provider to obtain a customer's opt-in consent before using or sharing any of the customer's personal information or CPNI, except in certain limited circumstances.[7]

In contrast, the FTC generally requires opt-in approval before using or sharing sensitive personal information, a point that FTC staff made in comments to the FCC. According to the FTC staff, an approach that treats sensitive and non-sensitive data the same does not reflect consumers' expectations and, as a result, "could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful".[8] Moreover, the FTC staff indicated that "impos[ing] a number of specific requirements on the provision of [broadband] services that would not generally apply to other services that collect and use significant amounts of consumer data" produces an "outcome [that] is not optimal".

Proponents of the FCC's proposal argued that broadband providers are 'gatekeepers' to the internet, and consumers have no choice but to share their information with them. They argued further that a broadband provider has no way of knowing whether information that traverses its network, such as what websites a customer visits, is sensitive. They claimed, therefore, that broadband providers must treat all information they can collect from and about customers as sensitive.

The broadband industry had argued that broadband providers lack unique or comprehensive visibility into customers' traffic and should be regulated the same way as other internet ecosystem players. This argument was based on the rise of encryption, virtual private networks, and consumers' reliance on multiple broadband providers (e.g. home, mobile, office, and public WiFi), all of which mean that other online services (e.g. social networks, email providers, and ad networks) have access to at least as much commercially valuable data as broadband providers; but these other services still would be subject to a less stringent regime. Broadband firms claimed further that restrictive privacy rules will inhibit their ability to compete in the online advertising market, where they are new entrants challenging dominant online providers. Industry also argued that the FCC's approach, including its application to information beyond CPNI, would exceed the agency's legal authority. Given their policy and legal concerns, broadband providers urged the FCC to adopt an approach consistent with that of the FTC.

Several groups have suggested Congress should extend the FCC's approach to all online services.

On 27 October 27 2016, by a 3-2 vote along party lines, the FCC approved broadband privacy rules that bear a closer resemblance to the FTC's framework than the FCC's initial proposal but that still depart from the FTC's framework in some significant ways. Specifically, similar to the FTC's approach, the final rules establish a customer approval regime that distinguishes between sensitive and non-sensitive customer information, generally requiring a customer's opt-in consent only for the use or disclosure of sensitive information.[9] But the FCC's rules categorise a broader range of information as 'sensitive' than the FTC does under its framework. Most notably, 'web browsing history' – including the domain names with which a customer communicates[10] – is deemed sensitive under the FCC's final rules but not under the FTC's framework.

Thus, the FCC's final rules permit broadband providers to engage in advertising and other activities based on web browsing information that they collect through the provision of broadband service, albeit pursuant to a customer's opt-in consent. In contrast, companies subject to the FTC's jurisdiction can continue to conduct similar activities without necessarily obtaining consumers' opt-in consent.

The exact implications of the FCC's departure from the FTC's approach remain to be seen. For broadband providers, in the opinion of dissenting Republican FCC commissioner Michael O'Rielly, the end result is "the lost opportunity and revenues for broadband providers precluded from competing against internet companies in the online advertising space[.]" For others in the internet ecosystem, the FCC's rules could set a new baseline that privacy advocates ask the FTC, Congress, and states to apply more broadly. In fact, several groups already have explicitly suggested Congress should now extend the FCC's approach to all online services.[11]

Ultimately, whether these developments will lead Congress, or an FCC led by an appointee of President-Elect Donald Trump, to consider seriously changing basic elements of the US consumer privacy framework – something it has long resisted doing – warrants close attention in the months ahead. For instance, a Republican-led FCC could revise or eliminate the new rules. One thing is clear: absent congressional action, the sector-specific privacy framework in the US will continue to face new challenges as evolving technologies and business models become more data-intensive and regulators jockey for a position in leading policy and law enforcement responses.

AARON BURSTEIN *and* ***JOSHUA BERCU*** *are attorneys at Wilkinson Barker Knauer, a Washington, DC law firm that focuses on telecoms, privacy, intellectual property and energy. This article does not constitute legal advice.*

REFERENCES **1** FCC (2016). Protecting the privacy of customers of broadband and other telecommunications services. Report and Order, WC Docket No. 16-106. fcc.us/1N6BNyI **2** White House (2012). Consumer data privacy in a networked world. bit.ly/1FQW1XF **3** This total appears to include FTC actions under Section 5, the Do Not Call Rule, the Fair Credit Reporting Act, and other specific privacy laws, and spans a timeframe that goes further into the past than Safe Harbor's beginning in 2000. **4** Privacy Shield annex at 61 (FTC letter). Whether the common carrier exemption to the FTC's enforcement authority restricts the FTC from addressing non-common carrier practices of a common carrier recently was addressed by a US appellate court. This significant decision is discussed in the panel on p20. **5** See: 47 US Code § 222 – Privacy of customer information. bit.ly/2gEyXqw **6** At the time, it was commonly understood that the FCC's decision removed broadband providers from the FTC's privacy and data security jurisdiction. The court case discussed on p20, however, indicates that at least certain broadband providers may never have been within the FTC's privacy and data security jurisdiction, irrespective of the FCC's reclassification decision. **7** The FCC's proposal also would have imposed certain transparency, data security, and breach notification requirements, which in many ways depart from the rules under which other entities are subject. **8** Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission to the Federal Communications Commission, In the matter of protecting the privacy of customers of broadband and other telecommunications services, WC Docket No. 16-106 (27 May 2016). **9** Privacy Report and Order, paras 177-195. The final rules permit providers to use non-sensitive information on an opt-out basis, and providers may also infer consent to use information or disclose information for a narrow set of purposes (e.g. providing service, protecting a carrier's rights or property, and limited first-party marketing). **10** Privacy Report and Order, paras 183-185. **11** See: Americans win significant broadband privacy rights in historic FCC decision. Center for Digital Democracy 27 October 2016. bit.ly/2hxEm75 / Consumer Watchdog welcomes FCC's new broadband privacy rules passed on 3-to-2 vote. Consumer Watchdog, 27 October 2016. bit.ly/2hoKuOJ

HOW THE INTERNET GOT DONALD TRUMP ELECTED

The factors that combined to help elect the new US president have the internet as a common denominator, reckons **ELI NOAM** – and these factors are now inherent in an internet-based economy and society

Internet advocates have long taken credit for anything progressive that has been happening politically around the world. The Arab Spring. The Obama election. Popular rebellions against the regimes in Iran, Turkey, Hong Kong, and Myanmar. The Occupy Wall Street movement. And maybe China, next. Wherever one looks, it seems that the internet is a force for social progress.

Conversely, when something happens that runs counter to such progress it must be the result of leaders who are behind the times technologically and of followers who don't get it by reason of education or age. If they only had been connected, this would never have happened! Thus, the conventional wisdom is that the internet is good for democracy and for progressive politics. Sceptical voices have been rare.

It is therefore jarring to face the fact that it is not the absence of the internet that has led to the election victory of Donald Trump but rather its prevalence. How is that possible, one might ask, given that the candidate did not even have a computer until 2007, rarely uses email directly, and had a low-visibility online campaign outside of idiosyncratic Twitter bursts?

What are these internet-based factors that favoured Trump and led to his election? There are several inherent to the internet and independent of any particular candidate. Some of these factors have been around for a long time but have accelerated.

1 THE EMPLOYMENT IMPACTS OF THE INTERNET

The most obvious reason is the changing economy. The internet disrupts, but the disruptees don't just shuffle away; they vote. In the US, industrial blue collar jobs have disappeared at the rate of 350,000 industrial jobs each year for two decades now. With a multiplier effect on other employment, this adds up to a job loss of about half a million each year.[1]

Of course, many of these jobs would have disappeared anyway to low-wage countries, but more slowly. The internet has accelerated the outmigration of jobs by making it much easier and cheaper to transact and control production processes over large distances. The pace of a fundamental transition is important. A slower change gives people more time to adjust, retrain and relocate.

Next, the pink collar jobs in retailing and clerical staffs began to shrink as retailing moved online. In America, the drop in retail jobs since 2007 has been pronounced, with a reduction of 900,000 jobs in five years, a nearly 6% decline per year.[2] Similarly, service support jobs such as telemarketing or editorial work have been moving first out-of-house and then offshore. And major industries have been squeezed by the internet, including newspapers, publishing, travel agencies, stock brokerages and universities. Middle management levels have been cut as remote supervision and information exchange has become easier, thus reducing the need for intermediate levels of management.

Of course, new jobs are also created due to the internet. But those who get the new jobs are not the same people who have lost them, or who fear for them. To them the fact that the economy as a whole may become more efficient and dynamic is small comfort.

2 THE EQUALITY PROBLEMS OF THE INTERNET

The problem is not just the extent of job loss but that the losses have not been distributed equally. In the US, half the 7.5 million jobs lost during the Great Recession were in industries that pay middle-class wages. But only a tiny percentage of the jobs gained since the recession ended were in mid-pay industries. Nearly 70% of the new jobs were in low-pay industries, and only 29% in industries that pay well.[3] This 'hollowing out' of the middle-class workforce has a lot of implications. It means that the job mobility from lower to middle class, which had been the historic way to individual and generational progress, is becoming more difficult. It also means job opportunities at the low end, which are less attractive to Americans and create an opportunity for immigrants. Which, in turn, leads to backlash.

A second inequality accelerated by the internet is generational. The rapid change in knowledge and technologies means that the learning curve is shortened and that there is less value to experience. Now, the old become expensive, out of date and expendable. The same technological progress that enables society to keep old folks' bodies alive longer is also shortening the value of their minds.[4] And this is just at the time when life expectancies rise, when retirement systems become unaffordable to societies, and when companies find ways to avoid paying taxes to contribute to the pot by relocating offshore.

Paradoxically, a similar problem happens at the other end of the age spectrum. One would assume that, symmetrically, the internet is a great improvement in the opportunities of young people. If so, how come their standard of living today is lower than those of the preceding generation, and how come there is such huge youth unemployment in many advanced countries?[5] If the internet has done all these great things for the digitally native generation, and if it has made distance obsolete, how come they live more than ever with mum and dad?

There is a great illusion that since the internet has been creating young multi-billionaries such as Mark Zuckerberg, Sergei Brin and Larry Page, it must be good for an entire generation. But this does not prove anything for the average opportunities of the young generation. Here, another dynamic of inequality comes into play, that of the 'winner-takes-all' economy. Only a few firms make it to the top, and only a few people get to cash in on that success. Many of the others live off temporary freelancing jobs. Economic volatility is high.

Given such a high-risk, low-probability distribution of success one must compensate the players by a higher jackpot,[6] in contrast to 'safe' industries such as civil service or a Japanese lifetime employment company.

Why are internet companies risky? There is the technology risk of course, with innovation proceeding rapidly. But there are also strictly economic factors at work. These fundamental characteristics of the digital sector are high fixed costs, low marginal costs, and thus particularly high economies of scale, plus the network effects of being connected to many other people, and all this leads to highly concentrated markets with only a few dominant firms. They also led to a transformation of firms into 'networked companies' that outsource components and services to many other firms rather than produce them themselves. For many such companies, employees are temps and freelancers.

> **For many companies, employees are temps and freelancers.**

Thus, the emerging unequal and unstable employment system is not the result of economic failure but of fundamental economics that restructure economies fundamentally. And because they are fundamental they are very hard to deal with through government policy. These characteristics are inherent to the digital economy. They lead to the loss of jobs by many people and to greater uncertainty for most others. It is natural that they feel threatened. And it is equally natural that they will favour candidates who promote a stabilisation and rollback of the negative effects of the digital revolution, and who seem sensitive to their fears.

3 THE IMPACT OF THE INTERNET ON GOVERNMENTAL GRIDLOCK

Again, how is that possible? Isn't the internet supposed to help deliver tele-medicine, e-learning, and m-government? All are useful but the problem is much deeper than the digitisation of service delivery and back offices. Technology does not operate in a vacuum. A truly fundamental technology progresses far beyond the abilities of society to absorb its impacts, and a growing disconnect occurs. No governmental institution or policy can change and progress at the exponential rate of Moore's Law, close to 50% a year. While stability and tradition are important, if the gap becomes too great it leads to blowups.

When in the 19th century technology proceeded at a rapid pace while societal institutions did not, the results were upheavals and revolutions. Today, again, the key elements of the information economy are progressing at a scorching rate, while public institutions and processes are not keeping up. Complexity rises but solutions lag.

It is actually even worse than that. The internet contributes to political gridlock and to a slowing down of the political process. Of course, the internet makes some political activity easier and cheaper. The early users of the internet experienced a gain in their effectiveness, and messianically extrapolated this to society at large. But this is a classic error of composition. The internet has made it easier for everyone to organise.

Soon, just about every group in society adopted the new ways to link and communicate, and many new groups formed, too. Mobilisation became easier and faster. As a result, it became easier for various single-issue stakeholder groups to resist, block and delay anything that affected them negatively. Civil society groups, similarly, found it easier to organise and get their message out, but they often have a purist's built-in problem with compromises and log-rolling that are part of the political process. The classic smoked-filled backroom of politics may be objectionable on various grounds but it is a relatively efficient way to strike deals.

The overall result has been a slowing down of the decision-making process of government while the issues raised by technological, economic and social change have been accelerating. This leads to a widespread disenchantment with the political system. It leads to a favouring of 'can-do' candidates from the outside who are not associated with the gridlocked system, and who offer hope to cut through its Gordian knot, such as by abolishing parts of the restrictions and institutions.

4 THE IMPACT OF THE INTERNET ON SOCIETAL FRAGMENTATION

Sure, the internet makes it easier to connect with people from all around the world. But there is a flip side to this. As one connects in new ways, one also disconnects the old ways. As the internet links with new and far-away people, it also reduces relations with neighbours and neighbourhoods. Democracy has historically been based on community. Traditionally, such communities have been territorial – electoral districts, states and towns. 'Community' and 'to communicate' – the terms are related: community is shaped by the ability of its members to communicate with each other. If the underlying communications system changes, the communities are affected.

Thus, the internet facilitates and creates electronically linked new types of community. But these are different from traditional communities. They have less of the averaging that characterises physical communities, that throw together the butcher, the baker, the candlestick maker. Instead, these new communities are more stratified along some common dimension, such as business, politics or hobbies. These groups therefore tend to be issue-driven, narrow, narrow-minded, ideological, and sometimes more extreme, as like-minded people reinforce each other's views.

Liberals link up with other liberals and read liberal information.

> **"How do societies handle cultural acceleration? Badly, if the past is a guide."**

Conservatives, tea-party adherents, and 'alt-rights' do the same with their peers. In their respective echo chambers they receive less non-conforming and more confirming information. In addition to being parochial this can also be self-defeating. Liberals thus largely missed or dismissed the extent of populist dissatisfaction, because they largely spoke to each other only, read the same narrow news analyses of the same newspapers, and congregated in enclaves that benefited from the digital economy.

Thus, there is less of a shared culture than before. The old mass media system was accused of aiming at the 'lowest common denominator', but at least it was common. Now, the individualisation of information, the ability to target recipients, to select favourite push content, and to share with others, do create increasingly disparate sub-cultures inhabiting the same country.

What makes these disagreements harsher than in the past is a 'cultural acceleration' that is driven by the exponential technological trends. More content creation, more content innovation, shorter life-cycles. How do societies handle this? Badly, if the past is a guide. Cultural conservatism is deeply ingrained. Most individuals like the foods we grew up with, the music we courted to, and the ideas we encountered at home or in college. Societies are even more conservative, extolling its classic heroes of literature, poetry, arts and music. Cultural change was accepted but it had to be gradual rather than jarring.

But now the pace is accelerating, this creates inevitably cultural conflicts. In the 1960s we encountered similar cultural dissonances when 'youth culture' broke out of the somnambulant culture of the 1950s, creating conflicts that are still reverberating 50 years later. Then, the change was precipitated by the emerging broadcast TV medium with which that generation had grown up with, and with the music that broke out of the parental styles.

Today we observe the culture wars accelerated by the internet, with moral traditionalists on one side and young people comfortable with gay marriage, abortion, multi-racial friendships, feminism, atheism, environmentalism, and legalised drugs. With cultural acceleration these culture wars will intensify. This is even a greater problem in traditional societies and countries where the forces of traditionalism had a stronger hold and the change is more abrupt and disruptive. And it is reflected in electoral behaviour.

5 THE INTERNET'S WEAKENING OF INTERMEDIATING MEDIA INSTITUTIONS

One of the characteristics of the internet is disintermediation. For politics, disintermediation of information is a mixed bag. True, gatekeeping by 'mainstream media' is bad, but so is disinformation. When information comes unfiltered, it leads to the creation of stories with a weak factual base, with

mistakes, outright distortions, fabrications, rumours, and last minute political ambush. It enables the intervention from the outside in the political process. In this particular election it might have been Russia. But there is no reason why other countries or domestic interest groups and vigilantes could not do the same. This kind of intervention starts with high-minded appeals to 'transparency' by making confidential information public, and soon moves to manipulation and sabotage.

The weakening of trusted central news institutions means a weakening of the curating function of media, which includes the evaluation of credibility of information and exposing false information. Once that function is weakened, anything goes. Reality is always a subjective cultural construct, as postmodernism argues, and political extremists on both sides have embraced this notion with a vengeance. News then moves from being fact-based, at least in concept, to one of opinion, then to wishful thinking, and soon to manufactured information – fake news, 'truthiness', 'post-fact' information.

A 'long tail' of content also means a long tail of truthfulness, all the way from careful journalistic standards to pure fabrications aimed to generate profitable clicks. Accuracy is as incidental as in a docudrama. Before we mount a high horse, though, consider that mainstream media, too, favour a coverage of candidates and issues that generate high ratings and click rates. The result is that the internet lowers the credibility of information. Access to information is indeed helpful, which is why the internet undermines totalitarianism. But it undermines pretty much everything else, too, including political parties and stability.

Perhaps, the value of information to peace and harmony is overrated. Civil war situations are not typically based on a lack of information. The problems of Germany's Weimar Republic were not the lack of media information. Instead, the internet provides an avalanche of information, and for any of it to receive attention it must be structured with a 'marketing' approach. Thus, the information abundance provided by the internet leads to disinformation clutter. It becomes necessary for any message to get louder.

Political information, therefore, will inevitably become distorted, shrill and simplistic. And that is what has been happening in recent elections. Even more than before, it favours candidates who are able to distil their message – and their personalities – into several simple but galvanising concepts.

6 THE IMPACT OF THE INTERNET ON DIRECT COMMUNICATION OF A CANDIDATE WITH THE ELECTORATE

The weakening of the intermediating function of trusted media leads to their leapfrogging by candidates themselves. Donald Trump was highly effective in doing so. His use of social media, in particular of Twitter, created a rapid channel for direct reach to voters. It invariably became amplified by being picked up as a news story and dutifully reported by other media. This form of communication proved much more effective in punching through the clutter of information, and its headline message format was vastly more effective than Hillary Clinton's sober position papers and policy proposals. It also proved more effective than the Clinton campaign's elaborate individualised and targeted messaging because it seemed much more genuine.

The direct and rapid link with the electorate made it possible for the candidate to be hard-hitting without the delay and editing by news media and even of campaign staff. For example, Trump took on Pope Francis's criticism of a proposed wall to Mexico with: "For a religious leader to question a person's faith is disgraceful." Not surprisingly, this dominated the news. Even people who disagreed with Trump felt this kind of response was more candid and gutsy than one vetted through focus groups.

The internet as a platform for relentless marketing has made voters leery of overly slick campaigns. It was a major accomplishment of the Trump campaign that it seemed authentic at the same time that it used a sophisticated data analysis and campaign operation. The internet makes it possible to run an active campaign below the radar to keep the opposition complacent and the snoopy press off scent. An advanced, campaign back-office data operation was quietly built up by son-in-law Jared Kushner in San Antonio, Texas, with a staff of over 100. it became an effective machine for message tailoring, fundraising with machine learning, prioritisation of campaign efforts, data mining, and operational planning.

The effects of this direct connection of a candidate with the electorate facilitated by the internet-based technology is not only the weakening of gatekeeper media but also of another intermediate institution, that of political parties. Trump was thus able to bypass the Republican Party and win against the party establishment in the primaries and go on to win the general election despite its tepid support. The party, too, was out of the loop.

Beyond this particular election, there is no reason to assume that this will not become a pattern for the future: an effective communicator reaching out directly to the public, personally or through a staff of hired professionals or committed volunteers. Now that this has proven possible, what is the function of major party nominations, when a candidate can go directly to the electorate, whether on the national or the state or regional level? This suggests a further weakening not only of the political parties but also of the two-party system.

CONCLUSION

It is necessary for the internet community, staunchly internationalist and multi-cultural by outlook, background and voting, to forthrightly face the question whether the changes and disruptions it has brought to America have contributed to an economy, society, politics and campaign tools that made the Trump candidacy successful. And, whether the same dynamics will be at work in other countries and lead to similar politics. The factors that enabled Donald Trump's success are inherent in an internet-based economy and society.

Therefore, this election, far from being an outlier, will be a precursor of politics to come, and a lesson to campaigns from both the right and the left.

ELI NOAM *is director of the Columbia Institute for Tele-Information. Among many projects, he is the lead author, with the International Media Concentration Collaboration, of Who Owns the World's Media? Media Concentration and Ownership around the World, published by OUP USA in 2016.*

REFERENCES **1** Atkinson R et al. (2012). Worse than the Great Depression: What experts are missing about American manufacturing decline. The Information Technology & Innovation Foundation. bit.ly/1D5DPbt **2** Wright J (2012). The demise of retail jobs? Not so fast. Emsi. bit.ly/2iNsajA **3** Condon B and Wiseman P (2013). Millions of middle-class jobs killed by machines in Great Recession's wake. Huffington Post. huff.to/1M69tP1 **4** Greenspun P (2009). Technology reduces the value of old people. Philip Greenspun's Weblog. bit.ly/2ifTaqN **5** World Employment and Social Outlook – Trends 2015. International Labour Organization, p21. bit.ly/1AHTqgX **6** Connelly BL et al. (2014). Tournament theory: Thirty years of contests and competitions. Journal of Management 40 (1): 16-47.

PLATFORM OR PUBLISHER?

The US election has brought the debate about whether social media firms such as Facebook are really media players, not technology platforms, into sharp relief, as **PHILIP M. NAPOLI** and **ROBYN CAPLAN** discuss

The outcome of the presidential election in the US has focused media and public attention on the increasingly influential role that social media platforms may be playing in how voters obtain news and information. Of particular concern has been the potential role that the circulation of fabricated news stories may have played in the election outcome. Facebook, in particular, has come under fire for being a venue for the widespread circulation of 'fake news'.

If the volume of media coverage is any indication, this issue of the circulation of false news stories on platforms such as Facebook appears to have galvanised public attention to the broader issue of the position and operation of social media platforms in the production, dissemination, and consumption of news and information in a way that previous controversies involving the intersection of social media and news did not, such as Facebook's ethically dubious emotional contagion research;[1] the construction of Twitter's trending topics list; and accusations that Facebook was suppressing the spread of conservative news.[2]

Facebook has been forced to publicly defend itself against critiques that it is failing in its responsibilities to serve its user base. At the same time, the company has initiated internal reviews of its policies and procedures and (along with Google) already has made some alterations, adding fake news sites to its list of content providers that are banned from participating in its ad network.[3] While this action does not directly affect the flow of fake news, it does affect the extent to which these sites can generate ad revenue.

What remains to be seen, however, is whether these concerns about how the dramatically changing dynamics of our media ecosystem may be affecting the democratic process will lead to any substantive consideration of whether policy responses of any type are appropriate. Do these accumulations of controversies represent a classic example of a 'policy window'?[4] Given the election outcome, and the direction in which social media are asserted to have influenced this outcome, policy initiatives of any kind in the US seem unlikely any time soon. However, other countries appear more

likely to respond proactively. Germany's Angela Merkel, for instance, has called for Facebook, Google and others to make their algorithms more transparent; and, in the flurry of concern about the US election, has vowed to regulate fake news.

It seems clear that it is time for researchers and policymakers to begin asking whether the ascendance of social media platforms to their position of potential power and influence in the news and information ecosystem represents an institutional shift in the delivery of news and information that may be on par with the rise of broadcasting in the 1930s. In the 1930s, concerns about the reach and gatekeeping power of broadcasting, and its potential as a mechanism for delivering propaganda, misinformation, and commercially-driven messages, helped give rise to a regulatory apparatus in the US designed to prevent concentration of control, assure that local news and information needs were met, and require that public service values were incorporated into the operation of broadcast licensees.[5] One could very easily make the case that there are many parallels between the ascendancy of broadcasting in the 1930s and the ascendancy of social media today.

One challenge in this regard, however, is a fundamentally different set of institutional perceptions that are being cultivated around social media platforms. Specifically, social media companies explicitly and steadfastly assert that they should not be considered media companies. Rather, they insist that they should be thought of only as technology companies. Facebook has been particularly insistent on this point. As recently as last summer, Facebook president Mark Zuckerberg maintained that "we're a tech company, not a media company", and that Facebook's focus is on providing users with "the tools to curate", a position that he and his executives have been maintaining for years.

Facebook is hardly alone in this. This rhetorical stance is widespread across the digital media sector. This position can be seen as part of a broader, ongoing effort by these companies to "discursively ... frame their services and technologies", according to Tarleton Gillespie, who also noted that these firms use terms like 'platform' strategically, "to position themselves both to pursue current and future profits, to strike a regulatory sweet spot between legislative protections that benefit them and obligations that do not, and to lay out a cultural imaginary within which their service makes sense".[6] The self-definition as technology companies rather than media companies is another key dimension of this discursive framing.

On the surface, this position may seem like a mere semantic distinction. However, this distinction has far-reaching ramifications, particularly in terms of impacting whether policymakers approach the emerging power and influence of social media platforms in a manner similar to how they responded to the potential power and influence of broadcasting when that technology first ascended to prominence; or, for that matter, whether they consider any aspect of social media's operation within the contemporary news and information ecosystem as falling within the scope of their regulatory responsibilities.

The goal of this article is to consider the policy implications associated with this question of corporate identity. Specifically, we consider the legal and regulatory advantages that accrue to social media companies if they are perceived as technology companies. We also explore the contemporary media policy concerns that would likely apply to social media companies if they were considered media companies rather than technology companies. As should be clear, this analysis begins from the assumption that the technology company label fails to adequately capture the nature and function of social media platforms as fundamental media institutions.

LANGUAGE AND CLASSIFICATION IN COMMUNICATIONS POLICY

US communications policymaking has been characterised by numerous disputes over how to appropriately classify new communications technologies and services. Such disputes are important because they affect the regulatory models applied to a technology or service, as well as the legal frameworks under which they operate. They help to illustrate how the specific words and metaphors used to describe technology, as well as the finer points of distinctions between one word and another, matter quite a bit.

The popularisation of the internet and its widespread use led to many issues related to classification. The courts and policymakers could not decide whether the internet, which was taking on many of the functions of media and communication, was something wholly new (exceptional) or whether it fitted within existing media policy regimes. In the 1990s, this became a major conundrum for the Supreme Court. In its assessment of the constitutionality of the Communications Decency Act in the late 1990s, in which Congress attempted to impose content restrictions on the internet similar to those that have long been applied to broadcasting, the court struggled with whether to treat the internet as akin to the telephone, a print newspaper, or television/radio.

> **"The self-definition as technology companies rather than media is key."**

Given the long tradition in the US of applying completely different regulatory regimes to different communication technologies based on their technological characteristics, the argument of which – if any – analogy to embrace for the internet had far-reaching legal and policy implications. In the US, the application of this approach has meant that different media industry sectors have varying levels of First Amendment protection.

A more recent example can be found in the FCC's network neutrality regulations. The regulations hinge on the classification of internet service providers (ISPs) as telecoms service providers (akin to phone companies) rather than information service providers (akin to web hosting services).

After initially classifying ISPs as information service providers back in 2002, the FCC reclassified them as telecoms service providers in 2015. This was done because the FCC's regulatory authority over telecoms service providers is much greater than its authority over information service providers (again, different technologies and services frequently operate under different regulatory models); so much so that the net neutrality regime imposed by the FCC would be impermissible if ISPs were classified as information service providers. Consequently, as one would expect, a significant dimension of the debate surrounding the network neutrality regulations revolved around the meaning of the telecoms service and information service terminologies and their applicability to the provision of internet access.[7]

This discussion highlights the importance that language plays in policymaking. In the public policy literature in general, and in the communications policy literature in particular, there is an increasing reliance on discourse analysis to understand the dynamics of the policymaking process.[8] This body of literature consistently demonstrates that 'words matter';[9] that the specific terms employed in the discourse and documents that shape and reflect policy decisions have profound consequences, and thus are employed strategically; in some cases, helping to define the contours of a policy issue; in other cases, helping to marginalise certain stakeholder groups from participating in the policymaking process.[10]

Of particular importance within the communications policy context is the extent to which the discourse has exhibited a strong technological focus, treating new technologies as autonomous agents, and/or narrowly defining the policy terrain purely in terms of complex technical issues and concerns, to the exclusion of broader social concerns. These dynamics have emerged not only within the US, but within international contexts such as internet governance as well.[11] This 'technocratisation' of communications policy discourse serves as an important backdrop for the 'tech-company-not-media-company' argument being considered here. The embracing of the media or technology company terminology could ultimately help determine the nature of the policy issues that arise and resonate – or whether any policy issues or concerns gain traction at all. Perhaps this has happened already.

LANGUAGE, CLASSIFICATION AND SOCIAL MEDIA

We can look to some recent legal proceedings to see how the rhetorical dynamics around the classification of social media platforms are playing out. As we discussed above, the way in which a company is classified can have significant legal and policy implications. Within the digital media sector, this is well illustrated by some of the challenges that have confronted Twitter. As industry observers have noted, "It has ... suited Twitter to pose as a tech company when it comes to potential regulatory and legal burdens."[12] For instance, in a response to a court order for information about a user who was arrested during an Occupy Wall Street protest, Twitter adopted the legal position that it has no ownership of individual tweets, a position that would seem to operate in conflict with the various forms of editorial discretion that Twitter has engaged in in relation to the content on its platform.[13]

"This discussion highlights the importance that language plays in policymaking."

We've seen the courts engaged in the same type of analogy-seeking in relation to Twitter as we saw in the Supreme Court's Communications Decency Act decision discussed above. In a case involving a government subpoena for information (including tweets) about an individual Twitter user, the court suggested that Twitter was analogous to "scream[ing] out the window".[14] In another subpoena made to Twitter for the IP information for some of its users (who were associated with the organisation Wikileaks), the court used a different classification, comparing Twitter, and the IP addresses used to connect to the site, to using a telephone. A fundamental implication of these classifications is the question of if, or to what extent, Twitter holds ownership and editorial authority over the content that circulates on its platform.

Similar issues have arisen in regards to Facebook. Recently, it has come under intense pressure in Europe to better police extremism and hate speech on its platform. Of course, such policing represents the type of direct imposition of editorial authority that puts Facebook more squarely in the position of a publisher, and thus potentially subject to the libel laws under which publishers operate. Yet Facebook routinely engages in the enforcing of particular content standards. The most recent high profile example involved the company's removal of a post by a Norwegian author of the iconic Vietnam War photo of a naked child fleeing a napalm attack. In the wake of criticisms about censorship, the company ultimately reversed its position, on the basis of "the history and global importance of this image in documenting a particular moment in

SOCIAL RESPONSIBILITY

It is also important to note that electronic media companies such as broadcasters and cable companies have historically had a unique set of social responsibilities. These typically have been imposed internally through professional norms and codes of ethics, as well as through government regulations, which in the US have taken the form of various public interest obligations[15] that have included providing audiences with minimum levels of public, educational, and government programming; minimum levels of locally-produced programming; and providing political candidates with the ability to advertise at reduced rates. For a time, such obligations became particularly aggressive, as in the case of the Fairness Doctrine, which, through the 1970s and part of the 1980s, required broadcasters (given their significant bottleneck position) to provide equivalent amounts of coverage to differing perspectives on controversial issues of public importance. Broadcasting is currently subject to much stronger regulation on balance in countries such as the UK of course.

time". Thus, both the decision to remove the photo and the decision to reinstate it reflect the articulation of specific editorial policies and the exertion of editorial authority – activities that would seem to fit the profile of a media company rather than a technology company.

In addition to social responsibility (see panel, p28), even economically-motivated structural regulations and government oversight have historically been more aggressively imposed in the media sector than other industry sectors, given concerns about the relationship between competition in media markets and the effective functioning of the 'marketplace of ideas'. A variety of ownership regulations persist in the electronic media sector, despite the increasing competition facilitated by the internet and its lowering of the barriers to entry into various media markets.[16] Mergers in the electronic media sector undergo a separate public interest review above and beyond the standard scrutiny that all mergers undergo to assess their impact on competition.[17] This public interest standard of review is intended to look beyond economic concerns and to consider the broader political and cultural concerns raised by such mergers.

The key point here is that there is a long history of regulatory interventions in the electronic media sector on behalf of broader public interest concerns related to policy principles such as diversity, competition, and localism. The regulated industries have generally regarded adherence to these regulations as burdensome and costly; and so one can see why digital media platforms would work to establish an organisational identity that places them well outside of this regulatory framework, even if most of the traditional justifications for media regulation (use of a scarce public resource such as spectrum) don't necessarily apply to them.

Imagine, for instance, if Facebook had to operate under a fairness doctrine for social media. In many ways, one could look at the controversies that arose surrounding the alleged suppression of conservative news and the proliferation of fake news stories as just the kind of sparks that could ignite that kind of discussion. Or, one could certainly imagine a digital media platform such as Facebook, with its dominant market position, growing increasingly concerned about the possibility of a more media-oriented competition analysis being applied to its position in both the economic marketplace and the marketplace of ideas.[18]

The somewhat surprising fact that such a conversation has yet to take hold at all in US policy discourse could perhaps be attributed to the success thus far of the technology-company-not-media-company rhetoric. The point here is that being classified as media companies could potentially subject social media platforms to types of government intervention that, as technology companies, they are much better insulated against.

Facebook and other social media platforms are understandably resistant to being characterised as media companies, given the unprecedented magnitude of content for which they would bear editorial responsibility and the broader public interest norms and principles that would then apply to them from the standpoints of both professional responsibility and government oversight. The argument that these platforms are first and foremost technology companies is a key component of this resistance. The end results, however, of accepting this position, are disconnects between how a platform behaves and how it is treated under existing legal and policy regimes; and between the intended scope of existing laws and policies and the reality of their reach and applicability.

As this discussion has hopefully made clear, the question of whether platforms such as Facebook and Twitter are media companies or technology companies is not just a matter of semantics but rather part of a larger discursive contest. The outcome of this contest has significant policy legal and policy implications, and is one in which the economic, legal and political motivations for social media platforms to be (mis)perceived as technology companies rather than media companies are quite compelling.

SOCIAL MEDIA INTERSECTIONS WITH CONTEMPORARY COMMUNICATIONS POLICY

The evolving position and function of social media platforms in the contemporary media ecosystem intersect with recent and long-standing communications policy priorities. From this standpoint, treating these platforms as technology rather than media companies has the potential to undermine the effective pursuit of these policy objectives. The goal here, therefore, is to illustrate how the evolving role and function of social media platforms exhibits some strong points of continuity and intersection with established media policy concerns, and to consider whether some of the types of intervention associated with these concerns may have applicability to the social media context.

SOCIAL MEDIA PLATFORMS AND JOURNALISM.

The FCC, which for many years congratulated itself for not wading into internet regulation, has now, though its intervention in issues such as network neutrality, begun to consider the internet within the broader normative framework that it has developed for other communications services under its regulatory authority. In addition, the survival of journalism has become, in and of itself, a basic communications policy issue, with Congress, the Federal Trade Commission, and the FCC all conducting proceedings to explore if and how policymakers should take action to protect and preserve the institution of journalism.[19]

This confluence of circumstances suggests that policymakers need to concern themselves with understanding exactly how these social media platforms function in the contemporary journalism ecosystem; how they are interacting with those organisations that actually produce journalism; and if, or to what extent, they are undermining its viability. Organisations/platforms that don't see themselves as media companies – let alone as news media companies – could displace or undermine the viability of legitimate producers of journalism, which operate under news values that have at least some connection to the role that news and information serve in the effective functioning of a democracy. This exacerbates an existing policy problem and therefore requires attention. Further, the increasing centrality of social media platforms to news distribution and consumption is affecting how news organisations behave.

The key point is that, to the extent that the operation of a social media platform like Facebook is becoming inextricably intertwined with the economics and strategy of news organisations, policymakers concerned with the future of journalism need to take into consideration how these platforms are affecting the economics and journalistic output of these organisations. From this standpoint, it may be time for policymakers to start thinking about the interaction between social media platforms and news organisations in the same way that they thought about the interaction between broadcast television and cable, and the potential (though, in this case, ultimately unfounded) threat that cable television and its

FACEBOOK'S MOVES

Facebook's centralised position within the news ecosystem has led to repeated changes within the industry as news organisations have adapted to Facebook's algorithm, and as it has changed its algorithms to adapt to the behaviours of these organisations.

In an effort to combat the 'click-bait' strategies of news organisations, Facebook altered its news feed algorithms in late 2013 to identify 'high-quality' news content. High-quality was defined as whether users were continuing to interact with an article after-the-fact, which meant that some publishers saw older articles begin to re-emerge on the network, with traffic driven to this older content.[20]

In August 2014, Facebook released another change to its news feed to address click-baiting headlines. In this modification, Facebook used variables like how long people spend reading an article away from Facebook as a way to calculate how users determine content that is valuable to them. Some outlets were dramatically affected by this change, and thus re-evaluated their own news values to make them more in line with Facebook's criteria.

Over the course of 2015 and 2016, several other changes Facebook made to its news feed have affected news organisations. As status updates and personal sharing among users began to decline over 2015, Facebook began to invest more resources in products geared towards news media distribution. This included a new emphasis on 'native videos' embedded in the news feed, which was communicated to news publishers directly.

It also included, in May of 2015, the launch of Instant Articles, a platform developed exclusively for the hosting of content from recognised news media publishers that would reduce load time for users clicking on news stories. This new platform was also the first step in a new (albeit limited) revenue-sharing model between Facebook and news publishers.

bottleneck position posed to the viability of broadcast television and the free national and local news that broadcast television provided.

These concerns ultimately led to the must-carry rules, which required cable systems to carry all local broadcast stations. With such regulations, the FCC extended its regulatory authority to the cable television industry in part by classifying cable as ancillary to broadcasting.[21] Might, similarly, digital media content curators like social media platforms be similarly ancillary to the ISPs that now fall under the FCC's regulatory purview due to the reclassification that took place in connection with the network neutrality regulations?

Reflecting this perspective, some analysts have asserted that social media platforms function as utilities,[22] just as ISPs, under the telecoms service designation, are considered utilities in line with traditional phone services, but this argument has yet to gain much traction in the policy sphere. However, the more social media platforms essentially function as the gateway (or portal, to resurrect that term) to the broader web, the more it may be time to revisit this perspective.

What is perhaps most disturbing about this situation is that, despite serving as bona fide news outlets, these social media platforms seem genuinely averse to serving this function. This would seem to be a primary takeaway, for instance, from the controversy about the accusations of the suppression of conservative news stories on Facebook's trending topics list. In what seems to have been a direct response to this controversy, Facebook modified its news feed algorithm to increase the prioritisation of posts from friends and family over those by media outlets (though with apparently limited effect).[23] The company also eliminated the editorial positions associated with the curation of its trending list, relying instead purely on algorithms; a change that, as a harbinger of things to come, seemed to immediately lead to the increased prominence of fake news stories in Facebook's trending topics list.

It would seem that the more Facebook is perceived as a news source, the more the social media platform works to appear otherwise. However, in Facebook's case, no sooner did the company announce these changes than the platform found itself front and centre as the most important news source in the country, when Diamond Reynolds used the platform to livestream the aftermath of the shooting of Philando Castile by a Minnesota police officer. And, of course, not long after that, Facebook was widely discussed as perhaps the most significant, influential, and potentially corruptible, news source in the 2016 US presidential election.[24]

These developments help to highlight the significance of recent data indicating that the functionality of platforms such as Facebook and Twitter is migrating away from their initial functionality as a means of individual and small group communication. That is, less of the content on these platforms is composed of the personal news and status updates that were the initial driver of these platforms' diffusion. Today, more of what is being disseminated and consumed on these platforms is essentially institutionally produced content (i.e., professionally produced news, information and entertainment). One could argue that these platforms are evolving into broadcasters, in the most traditional sense. Perhaps it is time they start being considered – and treated – more like broadcasters from a policy standpoint.

In any case, the key point here is that as policymakers increasingly focus attention on how to preserve the institution of journalism, this objective is becoming increasingly intertwined with the role and function of these platforms in the production, distribution and consumption of news; and complicated by the demonstrated ambivalence (at best) that these platforms have shown toward their evolution into central news organisations in the contemporary media ecosystem.

VERTICAL INTEGRATION. The argument that social media platforms are technology and not media companies is premised in large part on the contention that these platforms produce no original content on their own, but rather facilitate the distribution of content produced by others. The irony in this position is that the history of media is one of companies that start out on the periphery of the media sector remaking themselves to be media companies in the fullest sense of the word. If we look historically at 'platforms' that, like social media platforms such as Facebook and Twitter, began primarily as distributors of content and not producers, we see a recurring pattern of integration into content creation. The cable industry is a prime example. An industry that began as an 'antenna service' for broadcast television gradually evolved into offering alternatives to broadcast television. The history of most cable networks is one of migrating from distributing content produced by others to creating original content.

And so it goes with companies like Amazon, Netflix, YouTube and Hulu, all of which began purely as content curators/intermediaries, only to integrate into content creation as well. Developments such as Facebook's Instant Articles (in which Facebook hosts, rather than links to, the content produced by various news organisations), and Twitter's live streaming of professional sporting events, political conventions, and Bloomberg television programming, represent the kind of initial steps toward the full-fledged vertical integration into content creation for these companies that history tells us is inevitable. Additional steps have recently followed, with Facebook announcing its intention to license original video programming, produced specifically for distribution on its platform.[25]

These developments also suggest the potential resurrection of the 'walled garden' strategy employed by AOL during the first tech bubble, which was a significant cause for concern among policymakers at the time. While concerns about AOL-Time Warner leveraging its vertically integrated position in a way that was harmful to the economic market or the marketplace of ideas proved unfounded, it's questionable whether Facebook or Twitter's position in the media ecosystem is comparable to AOL-Time Warner's position, given that their reach is global, rather than limited to those who subscribe to a certain broadband service.

And so, as dominant social media platforms like Facebook and Twitter inevitably head down the vertical integration path, perhaps it is a good time to remember that policymakers have, at various points in the past, found the public interest to be well served by limiting the extent to which companies with a prominent bottleneck role in content distribution can simultaneously produce and own content. The financial interest and syndication rules, which applied for roughly two decades to the 'big three' national television broadcast networks in the US (ABC, NBC, CBS), limited the extent to which these networks could own their primetime programming.

The logic of these regulations rested on the notion that the proportion of audience attention controlled by these networks was so large that the public interest in diversity and competition was served by requiring the networks to allow other content creators to have access to this massive accumulation of audience attention – and to the accompanying revenues.

The cable industry, which essentially replaced the broadcast industry as the primary media bottleneck, found itself operating under must-carry rules (which required cable systems to carry local broadcast stations), as well as limits on the extent to which cable systems could populate their channel line-ups with networks in which they had an ownership stake. And, forgotten in the implosion of AOL-Time Warner is that conditions of the merger included the requirement that the company allow consumers to have access to unaffiliated ISPs, allow these unaffiliated ISPs to control the content of customers' first screen, to assure interoperability of its instant messaging service (in some ways a precursor to social media) with competing providers, and to open up its network to other interactive television service providers.

The point here is that, historically, media platforms that have obtained significant bottleneck positions as content distributors have sought to leverage that position for content creation as well; and that, historically, policymakers have instituted safeguards to protect competition and diversity under such conditions. As is often the case in communications policy, the question becomes whether it is preferable to be proactive (and potentially discourage innovation) or reactive (and be confronted by the inability to 'put the horse back in the barn'). History tells us that we're likely moving down a similar path in relation to a select few social media platforms, so it is important that these conversations begin sooner rather than later.

CONCLUSION

The fundamental problem is that social media platforms that are playing an increasingly central role in the production, dissemination, and consumption of news and information are – if we accept the technology company identity – essentially independent and distinct from the news and information ecosystem that they mediate. Accepting this argument means that these important platforms for news and information will exist outside of the bounds of regulatory authority that have, since the dawn of the age of electronic media, been able to exert at least some influence over the structure and behaviour of the key participants in the news and information ecosystem. In which case, we have a "discourse [that] serves to shape an institution that it fails to describe".[26]

When we consider social media platforms through the lens of prominent communications policy concerns, there are a number of points of intersection that would suggest that policymakers need to take social media into consideration. To consider these platforms purely as technology companies ultimately forecloses the application of any public interest principles to what are arguably becoming the most important mechanisms for the flow of news and information that serves the democratic process. Continuing down this path could have dramatic repercussions for how citizens meet their critical information needs and, thus, for how democracy functions.

PHILIP M. NAPOLI *is James R. Shepley Professor of Public Policy, Sanford School of Public Policy, Duke University, US.* ***ROBYN CAPLAN*** *is a research associate at the Data & Society Research Institute, New York.* *This article is based on a paper presented at TPRC, 'When media companies insist they're not media companies; and why it matters for communications policy'.*

REFERENCES **1** McNeal GS (2014). Controversy over Facebook emotional manipulation study grows and timeline becomes more clear. Forbes. bit.ly/2i3ya3s **2** Nunez M (2016). Facebook's fight against fake news was undercut by fear of conservative backlash. Gizmodo. bit.ly/2fs8yPE **3** Wong JI (2016). Facebook is banning fake news publishers from its ad network. QZ. bit.ly/2hxvsWZ **4** Kingdon J (2010). Agendas, alternatives, and public policies (2nd ed.). Longman. **5** Napoli PM (2001). Foundations of communications policy: Principles and process in the regulation of electronic media. Hampton Press. **6** Gillespie T (2010). The politics of 'platforms'. New Media & Society, 12 (3): 347-64. **7** Rinehart W (2015). A semantic network analysis of the network neutrality debate. Paper presented at TPRC. bit.ly/2gPpvR2 **8** Lentz B (2011). Regulation as linguistic engineering. In: R. Mansell and M. Raboy (Eds.) The handbook of global media and communication policy. Blackwell. **9** Lentz B (2013). Excavating historicity in the U.S. network neutrality debate: An interpretive perspective on policy change. Communication, Culture, & Critique 6: 568-97. **10** See for example: Streeter T (1987). The cable fable revisited: Discourse, policy, and the making of cable television. Critical Studies in Mass Communication 4:174-200. **11** Napoli PM (2009). Public interest media advocacy and activism as a social movement. Communication Yearbook 33: 385-429. **12** Rana S (2012). Is Twitter a technology platform, a media company – or both? Tech2. bit.ly/2gPkyaK **13** Guynn J (2016). Twitter suspends alt right accounts. USA Today. usat.ly/2gZoitK **14** See New York vs Harris, 2012. **15** Napoli PM (2015). Social media and the public interest: Governance of news platforms in the realm of individual and algorithmic gatekeepers. Telecommunications Policy, 39 (9): 751-60. **16** FCC Communications Commission (2016). Fact sheet: Updating media ownership rules in the public interest. bit.ly/2hfMk1d **17** Sallet J (2014). FCC transaction review: Competition and the public interest. fcc.us/2hfFGrH **18** See: Thompson D (2016). Facebook and fear. The Atlantic. theatln.tc/1NpErVR **19** See: Waldman S (2011). The information needs of communities: The changing media landscape in a broadband age. FCC. fcc.gov/infoneedsreport **20** Meyer R (2013). Why are upworthy headlines suddenly everywhere? The Atlantic. theatln.tc/2h08hWg **21** See US vs Southwestern Cable Co., 1968. **22** Andrejevic M (2013). Public service media utilities: Rethinking search engines and social networking as public goods. Media International Australia 146: 123-32. **23** Washington-Harmon T (2016). The friends-and-family Facebook algorithm change doesn't seem to be hurting traffic to news sites. Nieman Lab. bit.ly/2i3C8c6 **24** Ohlheiser A (2016). Mark Zuckerberg denies that fake news on Facebook influenced elections. Washington Post. wapo.st/2hNYMWF **25** Kafka P (2016). Facebook says it's in talks to buy its own video shows. Recode. on.recode.net/2hxkAGf **26** As ref 10, p176.

UNDERSTANDING AI

Applications of artificial intelligence have profound implications for societies. The US government and academics have been taking a close look

One of the last topics to be addressed by the Office of Science and Technology Policy (OSTP) in the US under President Barack Obama is a big one – artificial intelligence (AI) – and prescient given how big the impact of the modern world and globalisation have been in the election of Donald Trump. There are two reports on AI that the OSTP managed to publish by December 2016. The first, 'Preparing for the future of artificial intelligence',[1] looks at existing and potential applications, and questions raised for society and public policy. The second report, 'Artificial intelligence, automation, and the economy'[2] is a rapid follow-up and looks mostly at economic impacts of AI-driven automation.

The first report has a good overview of the various definitions of AI and its current state of development. Remarkable progress has been made on what is known as 'narrow AI', which addresses applications such as playing strategic games, language translation, self-driving vehicles, and image recognition. 'General AI' refers to a notional future AI system that exhibits apparently intelligent behaviour at least as advanced as a person across the full range of cognitive tasks, and is the stuff of dystopian visions of the future, but currently there is little here to trouble policymakers.

Meanwhile, the narrow AI apps have great promise in areas such as medicine, transport, criminal justice and even helping to solve major social problems such as homelessness and poverty. Many uses of AI for public good rely on the availability of data that can be used to train machine learning models and test the performance of AI systems, so underpinning these apps will probably be more questions about the regulation of data, which are raised later in the report. First though there is a recommendation to release datasets to address social challenges, even proposing an 'open data for AI' initiative.

Inevitably though, the report does turn to regulation, but initially about the specific risks that AI systems may introduce such as ensuring the safety of autonomous vehicles and aircraft. In the US, there is new regulation that authorises non-recreational drones, and also a new federal automated vehicles policy. These are really adaptations of existing regulation, and it is noted that airspace management is likely to be a major use for AI. In general, the report says that "broad regulation of AI research or practice would be inadvisable at this time", but agencies will need appropriate technical expertise at a senior level. It is recognised that safety engineering is problematic and a barrier to deployment.

I, Robot – a public view of artificial intelligence

More pressing perhaps is good governance of data (and 'big data') that is used to drive AI systems, such as in criminal justice applications (risk prediction tools for sentencing are mentioned that could generate racially biased results). There is discussion of how to ensure transparency of how such systems work and why they can be subject to intentional or unintentional bias in the underlying algorithms. Cybersecurity is also a major area for narrow AI – "There are many opportunities for AI and machine learning systems to help cope with the sheer complexity of cyberspace and support human decision making in response to cyberattacks."

Briefly, the second report, on automation and the economy, says that responding to the economic effects of AI-driven automation will be a significant policy challenge. It shows just how wide the impact of this new wave of automation will be as there are questions for the fundamental operation of economies and societies, ranging from reforming welfare and taxation, to new education and training strategies, to impacts on productivity. As it says: "Technology is not destiny – institutions and policies are critical."

> **"Inappropriate regulatory activity would be a tragic mistake."**

Finally, there's the 'Artificial intelligence and life in 2030',[3] the first report in an ongoing study that was launched in 2014 by Stanford University, and which has now published. The study panel picked eight domains likely to affect a typical American city – transportation, service robots, healthcare, education, low-resource communities, public safety and security, employment and workplace, and entertainment – and looks at the past 15 years and then 15 years ahead. They find no imminent threat to humankind, and "inappropriate regulatory activity would be a tragic mistake", but: "Fortunately, principles that guide successful regulation of current digital technologies provide a starting point," such as privacy regulation.

However, as the first OSTP report comments, experience shows that it's mostly hopeless trying to predict what will happen with any technology beyond 10 years – you might just as well flip a coin.

Marc Beishon

1 Office of Science and Technology Policy (2016). Preparing for the future of artificial intelligence. bit.ly/2j3XA4k
2 Office of Science and Technology Policy (2016). Artificial Intelligence, automation, and the economy. bit.ly/2jsebMI
3 Artificial Intelligence and life in 2030. One hundred year study on artificial intelligence. stanford.io/2e0yB07

VIRTUAL NETWORKS

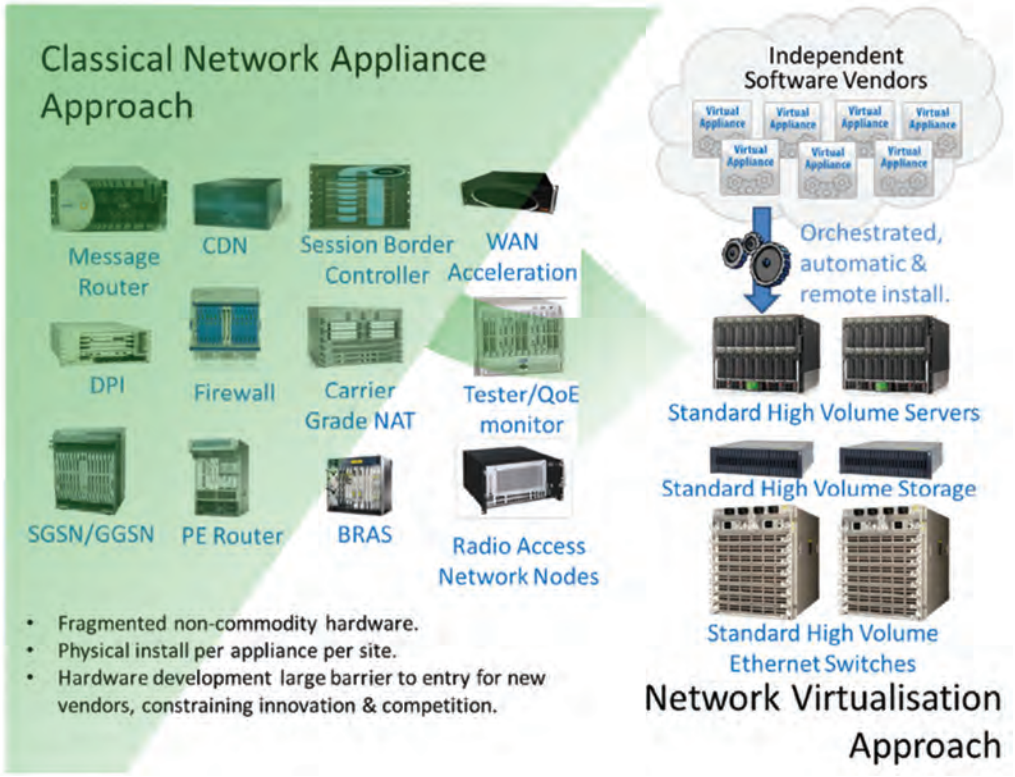
Telecoms operators have missed the platforms boat but hope to regain ground with network virtualisation. **RICHARD FEASEY** discusses the technology and regulatory implications of a powerful but potentially double-edged movement

In the traditional telecoms industry, technology and business strategy often occupy different worlds. Telecoms operators give their technologists and engineers remarkable freedom to pursue their dreams, only to find that the reality is different and less inviting. This was the case with the IP (internet protocol) revolution of the past 15 years, which left operators with lower costs and more flexible networks, but also without any control over the services environment, weaker relationships with their customers, and challenges in monetising their investments. Is the same thing about to happen again? I think it is.

This time the driver of change is not IP, but the network virtualisation movement or what Korea Telecom refers to as the 'transition to IT'. Once again, the technologists and engineers within the operators are enthusiasts.

Network virtualisation promises to reduce costs, both capital and operating, still further, to allow operators to run multiple logical or virtual networks over a single physical infrastructure, and to create opportunities for greater innovation and more competition among their suppliers. It does not require 5G to be realised, but key elements of whatever 5G vision you happen to subscribe to assume that network virtualisation will be adopted.

The logic is deceptively simple: split out the network intelligence from the underlying hardware, commoditise the latter and open source the former. In short, turn the traditional 'network' into a platform business. Traditional telecoms operators have mostly missed the boat on platform businesses so far, so perhaps this is their chance. If they succeed, operators would dump their traditional, vertical supply chain and replace it with two-sided ecosystem, with coders on one side and



SOURCE: ETSI WHITE PAPER ON NFV (2012)

producers of standard IT hardware on the other. AT&T is clear that this is its aim:[1]

"AT&T expects to develop key software resources in a way that they can be openly used, and cannot be lost through the acquisition or insolvency of a vendor partner. This pivot will enable AT&T to do business with start-ups and small businesses that we might have deemed too risky in the past. While they may not always endure, small businesses demonstrate the large fraction of innovation and agile development in the marketplace and enabling the company to do business better with these small companies is a key element of Domain 2.0."

This is a transition in which the software that orchestrates the functions performed by what we refer to today as 'the network' and the underlying physical hardware of that network are decoupled into two sides of a platform, just as services and networks were decoupled with IP. The underlying architectural principles are generally known as software defined networking (SDN) and network functions virtualisation (NFV).

TECHNOLOGIES EXPLAINED

SDN refers to the decoupling of the control plane from the packet forwarding functions (or 'data plane'). These functions are today integrated within the same network components, such as routers, in which communication between the control and data planes is undertaken using propriety code written by the vendor. With SDN, the aim is to use standardised hardware that could be supplied by many different vendors that is then controlled by software, which anyone could write, through a standardised interface.

Just as IP enables us to combine traffic from different sources into a single multiplex rather than running a series of discrete networks, so SDN would enable a wide range of logical 'networks' over common physical resources. The common physical resources of the network, including the radio spectrum, could then be dynamically allocated and reallocated between the different network slices without any changes to the underlying hardware.

This capacity to create different 'slices' over a common network substrate is a key feature of the 5G vision and would allow internet of things (IoT) applications that need only narrowband, low power, delay tolerant conditions to run alongside gigabit wireless fibre applications over the same physical network.

NFV envisages virtualising network equipment as software so as to run a wide variety of applications on virtual machines hosted on standardised IT hardware. Many functions that are currently performed by dedicated components in the traditional network – firewalls, load balancing, intrusion detection – could be virtualised. In each case the idea is that the proprietary hardware is replaced by a 'virtual machine' which is hosted on a generic IT or cloud infrastructure. SDN can be deployed without NFV, and vice versa, but most operators envisage deploying both and the concepts appear highly complementary.[2]

There are many benefits from SDN and NFV, most of which are common to both. Shared network assets, including spectrum, can be managed more holistically and efficiently. Routing decisions that are taken by an omnipotent network controller will ensure more optimal utilisation of the network as a whole, as well as allowing for different service policies to be applied for different flows or sequences of packets. This architecture also allows for cloud computing and IT capabilities to be hosted at the very edge of the network – a concept often known as 'mobile edge computing' – which is a prerequisite for some of the very low latency applications envisaged for 5G.

> **"Shared network assets, including spectrum, can be managed more efficiently."**

Orchestrating networks in this way improves efficiency and lowers costs. SDNs ought to be easier and faster to upgrade in order to support new services, since there is less dependency on hardware

that is difficult, expensive and slow to replace, and more dependency on software, which is easy, cheap(er) and quick. When hardware does need to be replaced or augmented, standard IT hardware and open interfaces ought to increase competition and reduce dependency on particular vendors, driving costs down: Google claims 95% utilisation on its 'virtualised' backbone (compared with industry norms of 30-50%), while AT&T has announced plans to 'virtualise' 75% of its network by 2020 and predicts that it will reduce hardware costs by 30-40% and operating costs by 50%.

Operators such as AT&T, China Mobile and Korea Telecom are announcing ambitious plans to virtualise their networks. But challenges and uncertainties remain. There is a huge amount of proprietary network equipment to be replaced or to be integrated into the new architecture. Operators need staff to develop software, but many traditional telecoms engineers lack these skills and those who have them are in short supply. There are security concerns and other technical risks of the kind associated with any massive IT project.

WHO WILL BENEFIT?

But the question is surely not if but when the virtualisation of networks will happen. The virtualisation movement has powerful backers, and we have seen that the potential benefits are huge. The more interesting question is who will reap the benefits when it does. Of course, the telecoms operators assume that they will sit at the heart of the platform.

One clue might be provided by looking at who is driving the technical work required to make virtualisation happen. Existing platform businesses such as Facebook and Google are the key movers behind various industry initiatives which are seeking to reduce hardware costs (which means reducing energy consumption in data centres)[3] but also efforts to virtualise functions currently performed by switches in telecoms networks so that they can instead be hosted in data centres,[4] as well as promoting the standardisation of software interfaces between applications and network operating systems and between these systems and hardware.[5] These firms have a long-standing interest in driving down the costs of internet access, which network virtualisation promises to do. But they also have skills in coding and in building platform businesses, and it may be these skills which matter most in determining who controls the platform in future.

All this needs to be seen in the context of other trends that are changing our view of what it means to operate a telecoms network or to be a telecoms operator in the future:

- **Infrastructure outsourcing.** Mobile operators have been divesting towers to tower companies ('the towerco') for many years. In the US, 80% of mobile towers are already owned by an independent towerco rather than by the operators. In Europe, Middle East and Africa it is closer to 20%, but the trend is in the same direction. Operators are also outsourcing significant parts of their active networks (to traditional vendors such as Ericsson and Nokia) in order, they hope, to benefit from economies of scale, reduce the operational complexity of their businesses, and perhaps for financial engineering reasons as well. Whether virtualisation will exacerbate this trend or reverse it is unclear to me. There is a clear potential for tension between the efforts of traditional vendors to extend their control over network assets, and the aims of the virtualisation movement and of operators like AT&T, seeking to reduce their dependency on such vendors.
- **Sales channels.** Trends in retailing and distribution in the telecoms industry are changing too. Many operators have long relied on third parties for retail distribution, particularly in mobile and particularly for prepay services. On the other hand, there has also been a trend in some markets towards reintegration, with network operators buying out third party distributors to obtain more control over their sales channels. Some have long speculated about whether online distribution of mobile devices will replace traditional retailing, as it has for other consumer electronics, but the long queues outside Apple stores suggest otherwise. We are some way off that today.

> **"Virtualisation will happen – the more interesting question is who will reap the benefits when it does."**

- **Spectrum.** Ownership of radio spectrum has traditionally been a core function and exclusive asset for mobile operators. But this appears likely to change as software enables the sharing of spectrum. 5G envisages the availability of significant tranches of unlicensed or shared spectrum: in the FCC's Spectrum Frontiers proposal for millimetric spectrum (above 24 GHz), almost twice as much spectrum (7 GHz) is being made available for unlicensed purposes as for traditional licenced applications.

We also know that the transition to IP meant an increase in services competition, the globalisation of the market and the disintermediation of the network operators. If those trends are also a feature of the 'transition to IT' then the 'network' will become increasingly fragmented, ownership and control dispersed, and boundaries redefined. AT&T accepts that some element of control might pass from the operators to customers and to third parties, although it still assumes that it (AT&T) will retain control of the 'platform':

"NFV can readily be applied to the control and management plane in addition to the data plane. This allows virtual networks to be created and managed by end users and third parties using the tools and capabilities heretofore reserved only for native network operators. Domain 2.0 comprises more than simply a network or service architecture. It requires appropriate business practices, a supplier and software ecosystem, a software-savvy planning and operations organisation, and management willing to try alternatives and fail fast."

Some of today's telecoms operators – those with the resources of AT&T or China Mobile – may be

better placed to beat the software giants at their own game than they were 20 years ago when the IP transition began. But it is difficult to avoid the suspicion that virtualisation plays to the strengths of existing platform businesses rather than to those of the telecoms operators. The key question may be whether the control of the software sits better with the owner of hardware or with the provider of the applications (or the user of the applications).

If the project to turn central offices into data centres[4] is taken literally, then large corporates and those involved in IoT may literally buy a 'network as a service' from a data centre provider. This is a market where the internet and IT companies such as Amazon, Microsoft and Google, not the telecoms operators, dominate.

If this is right, there are several lessons for policymakers and regulators to be drawn from the history of the IP transition which are likely to be relevant to the IT transition and network virtualisation:

- Policymakers will want to ensure that incumbent players, both traditional telecoms equipment vendors and traditional network operators, do not try to erect barriers to virtualisation. Such barriers might involve insisting on proprietary code and standards rather than open interfaces and open source software. Bundling hardware and software, or hardware and hardware, or software and software together, could also be barriers. The standards bodies for NFV and SDN – most of which sit outside the traditional telecoms groups such as the European Telecommunications Standards Institute (ETSI) – could play an important role in avoiding this.
- Although the incumbent players may attempt to move from hardware into software, the internet companies may also attempt to gain from moving from applications into network software. Application providers might, for example, design their services so they would only run properly over their own virtual network and not over those of rivals. This would be a complex area to police and would necessitate a serious re-examination of existing net neutrality assumptions to recognise that the decoupling process means that today's internet access provider may no longer control the network in future. (These are the terms used in today's European net neutrality rules. I assume net neutrality rules in the US may be revised for other reasons following the election of President Donald Trump.)
- The virtualisation of networks and decoupling of software from hardware may also lead regulators to worry much less, or not at all, about competition in hardware. The imperatives – better asset utilisation and cost reduction – that are already driving the formation of the towerco, network consolidation and spectrum sharing, might end with a reversion to a single physical network over which competing virtual networks are then deployed. In a decoupled world, duplication of physical network assets would yield few benefits and lots of costs, while consolidation of these assets should not mean any loss of competition in the virtual realm. Networks could then be hosted in enormous data centres, with their location determined by energy costs or the regulatory environment, rather than the location of the customers they serve or the physical assets or hardware over which they run.
- Regulators will face the same issues of supervising and regulating networks as they now have with regulating IP services that are provided by firms which operate remotely and on a global basis. They have already lost a significant degree of control over IP services, but would now face the prospect of losing control over the virtual networks as well (including being unable to shut them down). Being able to regulate the towers and hardware that remain within a country will not count for much if control of the network sits elsewhere and there is no exclusive rights to spectrum which a government could withdraw.

"Policymakers may need to think more about how the value chain works in the interests of users.

EVALUATING THE VALUE CHAIN

The history of the IP transition also suggests that there are some other significant risks ahead. One will be the challenges which the participants in a long and complex value chain face in coordinating their interests and activities in order to produce what economists call complementary goods. The classic example with IP services has been the ongoing tensions between the telecoms network operators and IP service providers about the costs (in terms of additional network capacity) which those services impose on the networks and how they might best be recovered.

So far, the value chain as a whole has been able to deploy more network capacity and broadly to meet the demands that new applications have presented without the internet collapsing. However, we now seem to be moving into an ever more complex world in which the demands of applications on 'networks' will be much more heterogeneous and the degree of coordination between different entities required to satisfy them will be much more challenging.

Policymakers have so far been able to largely ignore the complaints of the different participants in the value chain, and they can probably continue to do so while the overall system continues to deliver. My sense is that they watch nervously as Comcast and Netflix argue about peering arrangements or European operators threaten to block adverts, knowing that if something really did go wrong and services were badly disrupted, then they probably have few effective tools with which to fix it. Network virtualisation might require policymakers to think more seriously in future about how to ensure the value chain works effectively in the interests of users.

Whether Google, Facebook or Amazon end up running vast global networks instead of today's telecoms operators I do not know. If they do, the current enthusiasm for network virtualisation among the engineers inside the traditional telecoms operators (as well as their traditional equipment vendors) may turn out to produce an unwelcome surprise for their colleagues in strategy, as well as a new set of challenges for policymakers.

RICHARD FEASEY *is an independent consultant and an associate at Frontier Economics, having previously worked for a variety of global telecoms operators over a period of 25 years. The views expressed in this article are personal and should not be attributed to anyone other than the author himself.*

REFERENCES **1** AT&T Domain 2.0 Vision white paper. soc.att.com/2gZSu7T **2** There are numerous introductions to SDN and NFV from vendors and industry groups. The ETSI 2012 white paper on NFV is often cited – see bit.ly/1tsRH2A – and I have found the AT&T white paper (ref 1) particularly useful. **3** The Open Compute Project is focusing on reducing data centre costs – opencompute.org; see Open Cellular on cellular network costs – bit.ly/29ioWvx; and the Telecom Infra Project on core network, backhaul and access – telecominfraproject.com. Facebook is active in all three groups. **4** The aim of the Central Office Rearchitected as a Data Centre (CORD) project is self-explanatory and has both Facebook and Google (as well as AT&T and Verizon) as participants. opencord.org **5** OpenDaylight claims to be the largest open source SDN industry player. opendaylight.org

POLITICAL PROTOCOL

The Internet Governance Forum (IGF) is much more than a UN talking shop and has the potential to be a key political networking body, reckons **WOLFGANG KLEINWÄCHTER**, who reports from the 11th IGF in Guadalajara

The Internet Governance Forum (IGF) has matured. In December 2016, about 2,000 internet experts from governments, business, civil society, academic and technical communities met offline (and another 3,000 online) at the UN sponsored 11th IGF in Guadalajara, Mexico. More than 200 plenaries, workshops, talks, forums and meetings of coalitions discussed over one week nearly everything on today's internet governance agenda: from the management of critical internet resources and the follow-up of the IANA (Internet Assigned Numbers Authority) transition, to the relationship between internet governance and international trade agreements; and from cybersecurity to the digital economy, from the internet of things to artificial intelligence; and from human rights in the digital age to sustainable development and how to get the next billion people online. How did it get here – and what are the most important issues for 2017?

THE TUNIS COMPROMISE FROM 2005

The IGF was established by the UN World Summit on the Information Society (WSIS) in Tunis in 2005. In Tunis, the 193 governments of the UN member states could not agree on an 'internet council' and how to organise oversight over so-called critical internet resources. However, they agreed on what was seen in 2005 as 'low hanging fruit': The establishment of a multi-stakeholder discussion platform, the IGF.

The idea of such a discussion platform was pushed mainly by civil society groups from the early beginning of the WSIS process in 2002. The rational behind the proposal was simple. Before decisions are taken in the unchartered waters of borderless cyberspace, they need an enhanced understanding of the numerous interdependent, complex issues which take into consideration not only governmental positions but also perspectives, arguments and interests of all non-governmental stakeholders from the private sector, civil society and the technical community.

It was difficult to argue against such an approach. And for many governments this was just the way out to avoid a failure of the Tunis summit. The green light for the IGF was a 'cheap success', as expectations for real success of the IGF were rather low. Many observers called it nothing more than another UN talking shop.

For governments the real issue was how the core of the internet – protocols, IP addresses, root servers and domain names – are managed. But in 2005, an agreement was out of reach. Back then, ICANN (Internet Corporation for Assigned Names and Numbers), which manages the internet domain name system (DNS), operated under two contracts with the US government. Many governments wanted to substitute such a unilateral oversight by the establishment of a multilateral intergovernmental oversight mechanism. Other governments disagreed. In their eyes governmental control over the internet was a bad idea. They preferred that the technical internet resources are better managed by the multi-stakeholder internet community.

Furthermore, the US government argued that its stewardship role over ICANN was not control of the internet, just a result of the internet being invented in the US. And it indicated that sooner or later it would terminate its special stewardship role. The good thing was that this disagreement did not block a compromise.

The argument, that the complexity of the internet needs the involvement of all stakeholders, including the private sector, civil society and the technical community, prevailed. The IGF was seen as the right instrument to promote such a multi-stakeholder discussion to bring more enlightenment into this complexity, to enhance communication and collaboration among all stakeholders, and to pave the way for decisions, where needed, in governmental or non-governmental bodies which have a related mandate.

Now, ten years later, the situation has changed and history has proved that the Tunis summit made the right decisions. The IGF is one of the most important annual gatherings of internet experts around the globe. In December 2015, the high level WSIS+10 meeting of the UN General Assembly extended the mandate of the IGF until 2025. For many internet related issues, the IGF is the best place to kick start a discussion or to organise pressure on decision-making bodies to find solutions for emerging issues.

A good example is ICANN: the management of critical internet resources was on the agenda since the 2nd IGF in 2007, and the IGF paved the way for the final transition of the US stewardship role that was completed in September 2016.

And the multi-stakeholder model itself – which was in 2005 a rather unclear invitation for a new political experiment – is now more accepted as the best approach to discuss and find solutions for the growing number of internet related technical and public policy issues. Documents adopted by leaders at the G7 (Ise-Shima, Japan, May 2016) and the G20 (Hangzhou, China, September 2016) include paragraphs of support for the multi-stakeholder approach to internet governance.

TRADE AND IOT IN GUADALAJARA

The 11th IGF in Guadalajara – and in particular the session on the relationship between internet governance and trade negotiations – was a good demonstration of the value of multi-stakeholder dialogue. Nobody disagrees that trade, and in particular e-trade, is a key element of the digital economy: arrangements among nations are needed. But so far, internet negotiations and trade negotiations are based on two very distinct political cultures. Internet governance discussions are based on open, transparent, bottom-up processes where all stakeholders are involved and on an equal footing. Trade negotiations take place among governments behind closed doors, with big private sector players in a strong lobbying position.

For many speakers in Guadalajara, the failure of the Anti-Counterfeiting Trade Agreement (ACTA), the Trans-Pacific Partnership (TPP) or the Trans-Atlantic Trade and Investment Partnership (TTIP) is the result of this clash of cultures. The good thing in Guadalajara was that all stakeholders – governmental trade negotiators and their opponents from consumer protection organisations, business people and technical experts – had a chance to present their views and expectations, and everybody was listening to everybody. Such openness is key to identifying areas of common interest and to find solutions which balance legitimate but conflicting interests in a way that all parties can live with. The discussion helped to broaden the understanding of such complexity.

> **“The failure of trade agreements is the result of a clash of cultures.”**

Certainly, multi-stakeholder processes are more difficult and often take more time. But among the participants in Guadalajara one could observe also a growing recognition that such an inclusive process will enhance the opportunities to find sustainable solutions in the interest of all parties, in particular in the difficult area of trade. And note that in World Trade Organization (WTO) negotiations, governments have not shown they can achieve faster results if they negotiate among themselves in a silo. The Doha trade round is without any concrete outcome after nearly 20 years.

This example is a good hint as to why the IGF is needed and why it does not need a mandate to do negotiations itself. It is obvious that there is a need for a new round on global trade negotiations. And at the end of the day, it will be governments that will have to make the final decisions on signing and ratifying treaties. But the open multi-stakeholder discussions – as those in the IGF – enable the governmental experts at the negotiation table to understand better the various perspectives of the conflicting parties. which will help them to find the right compromises to get a sustainable outcome. And it allows the non-governmental stakeholders to raise their voice and articulate special interests in a serious UN-sponsored environment.

Another example was the discussion about the internet of things (IoT). Since 2008, the multi-stakeholder IGF Dynamic Coalition on Internet of Things (DC-IoT) has been examining a number of IoT-related issues, including governance, privacy and security. When the coalition was established during the 3rd IGF in Hyderabad, India, IoT was still an emerging issue. Now it is at the centre of the global internet debate. In Guadalajara, the DC-IoT meeting presented perspectives from governments (European Commission, NTIA of the US Department of Commerce, ITU-T study group 20), from the technical community (IETF, ISOC), the private sector (ICC Basis, Google) and civil society groups which raised, among other topics, the need to understand more about the ethical implications of new IoT services and devices.

This meeting did not produce any concrete outcomes. But the questions raised in the discussion were wake-up calls for everybody in the crowded room not to remain in their stakeholder or sectoral silo, where IoT issues are discussed only in their inner circles of experts, but instead to talk to other stakeholders and sectors to exchange best practices and learn from how to benefit from new IoT opportunities by keeping the security and privacy risks under control.

A GRAND DESIGN FOR THE AGENDA

So the IGF has matured into a discussion platform which helps to formulate an agenda and which, in an internet world where the list of new and open issues is growing on a weekly basis, is value in itself. Certainly it is impossible to summarise the Guadalajara outcome in a few words. But one can put the dozens of questions raised during the six days into four big ‘baskets’ that allow a more holistic approach to the internet governance debates of the future (see panel, p39). This helps to identify areas where informal or formal agreements among stakeholders (including intergovernmental treaties) are needed and who should continue the discussion, and where and how.

LOOKING AHEAD: EVERYTHING IS LINKED TO EVERYTHING

The 11th IGF in Guadalajara has helped to structure the internet governance agenda for 2017 and beyond. But it also has helped to open our eyes to understand better that in the internet world everything is connected to everything. That means that neither cybersecurity issues

FOUR 'BASKETS' FOR INTERNET GOVERNANCE

BASKET 1: CYBERSECURITY

All the new threats to national security – the risk of cyberwars, the emergence of cyberweapons, cyberespionage, the fight against cyberterrorism and cybercrime – will dominate the internet discussion in the years ahead. The IGF will not be the place where solutions will be negotiated. But to understand all the new challenges for cybersecurity, it will not be enough if government experts alone try to agree on new intergovernmental treaties. They will need the cooperation of the technical community and the private sector, as the case between the FBI and Apple has demonstrated recently (over access to the iPhone used by a shooter in last year's San Bernardino attacks). Civil society has also to be part of the discussion.

If governments ignore the interests of billions of internet users, any intergovernmental cybersecurity agreement risks failure, as we have seen with the trade agreements.

The body which has emerged over the last years with the highest authority for global cybersecurity issues is the Group of Governmental Experts (GGE) which operates under the First Committee of the UN General Assembly, and which is probably the best place to produce concrete outcomes. The UN GGE is a purely intergovernmental mechanism. But it would be wise for it to listen carefully to the IGF and other multi-stakeholder discussions and to take reasonable ideas and arguments, which represents legitimate interests and perspectives from non-governmental stakeholders, on board.

BASKET 2: DIGITAL ECONOMY

The digital economy is the driver of the global economy. There is no way back into the pre-internet age. A key aspect, as mentioned above, is certainly trade. But the future of the digital economy goes beyond e-trade. It includes, as the recent OECD ministerial meeting in Cancun in June 2016 has stated, e-skills, e-jobs, 'industry 4.0' and many other aspects. At the G20 Hangzhou summit meeting in September 2016, the leaders of the 20 largest nations adopted a 'global digital economy development and cooperation initiative'. This is ill-defined and in its early stage. But as it is linked to the recommendations of the OECD Cancun conference, it has great potential to help countries to define a national digital economy strategy and to identify new areas for global digital cooperation.

Germany now has the G20 presidency for 2017. The G20 summit is planned for July 2017 in Hamburg, but in April there will be a special meeting of ministers responsible for the digital economy. And the day before the ministerial meeting, a multi-stakeholder conference is planned to involve non-governmental stakeholders in the future debate about the digital economy.

As in the cybersecurity field, the IGF will certainly not become the negotiation body for the global digital economy – the G20 and OECD are intergovernmental bodies and have legitimacy and authority to translate discussions into decisions. But as the OECD in Cancun has demonstrated, the involvement of non-governmental stakeholders, organised in the OECD's advisory committees on business (BIAC), trade unions (TUAC), the technical community (TAC) and civil society (CISAC), was very useful in formulating the Cancun declaration and to design strategies for areas such as e-skills and e-jobs. The G20 can certainly benefit from this experience and the IGF offers a great opportunity to broaden and deepen the debate.

BASKET 3: HUMAN RIGHTS

The issue of how human rights are protected in the digital age has been on the IGF agenda since 2006. A couple of years ago the IGF Dynamic Coalition on Rights and Principles produced a document that defined a number of new digital norms, and there are projects such as the Brazilian Marco Civil and the Italian Bill of Internet Rights. In Guadalajara, a German initiative for a new European Union charter of digital fundamental rights was presented (see digitalcharta.eu).

The discussion on human rights in the digital age at the IGF has helped to clarify at least two things:

- Individuals have the same rights online as they do offline
- There is no need to invent new human rights but there is a need to enhance our understanding of existing rights.

A big step forward was the adoption of the Universal Declaration of Internet Governance Principles at the Netmundial conference in São Paulo in April 2014. What is needed now is to make sure that these principles are implemented. But there are also international bodies that can translate the IGF discussion and the Netmundial principles into more concrete action. The UN Human Rights Council with its special rapporteurs on freedom of expression and privacy in the digital age, is a strong intergovernmental body which has opened itself gradually to more involvement of non-governmental stakeholders, using the IGF debate as a source of inspiration.

BASKET 4: TECHNOLOGY

The internet itself is a technical innovation. But there are so many innovative products, devices and services on top of the internet and its domain name system, such that technological development has become an issue in itself. Cloud computing, IoT and artificial intelligence have moved to the centre of today's discussion, and there will be new ones tomorrow.

To have a place where such emerging issues can be discussed in a multi-stakeholder environment is important. The IGF can function here as an early warning system where both the opportunities of new technologies and their risks and threats can be discussed.

nor issues related to the digital economy or human rights can be discussed in isolation any more. To take just one example, IoT is now a key point for the digital economy. If we move from driverless cars to driverless tanks, it is an issue in the cybersecurity debate. And IoT will also have a massive impact on our individual privacy.

We have to design global discussion and negotiations with a mechanism that reflects these linkages. But this needs innovation in policymaking. The internet, as we know, is a network of networks, connected via universal protocols. What we need in the policy field is a similar network of networks where the various bodies and platforms are interlinked by a similar 'political protocol'.

WOLFGANG KLEINWÄCHTER *is a professor emeritus at the University of Aarhus. He was a member of the ICANN board (2013-15) and was a special ambassador for the Netmundial Initiative.*

EUROPE'S NEW CODE FOR OTT

There are few issues more fraught than how to deal with over the top services. **ANDREAS GRÜNWALD** and **CHRISTOPH NÜSSING** examine Europe's draft code

In 2015, a German court classified Google's Gmail as a regulated telecoms service.[1] This court decision added to the discussion of whether and to what extent communications services that are provided 'over the top' (OTT) will be regulated under European telecoms laws. The Gmail decision also provided momentum for the call by telecoms operators for a regulatory level playing field for traditional telecoms services (voice telephony over fixed or mobile networks, or SMS) and OTT.

Google's appeal against the Gmail decision is still pending so, under current German law, this particular question will not be resolved for some time. In a similar case, BIPT, the national regulatory authority (NRA) of Belgium fined Skype last summer more than €220,000 for failure to notify it was a provider of an allegedly regulated telecoms service, SkypeOut.[2] And most recently, a Belgian court issued a further fine against Skype for failure to comply with statutory obligations addressed to providers of regulated telecoms services.[3] It can be expected that Skype will appeal this decision.

In September 2016, however, the European Commission presented its new draft directive, the European Communications Code (ECC),[4] which will enact a specific regulatory framework for OTT communications services. While under this framework many OTT services would only become subject to a limited set of new requirements, others – specifically those that allow a breakout to the public switched telephone network (PSTN) – would then be regulated at the same level as traditional telecoms services. (The ECC will replace the current EU telecoms framework which was last revised in 2009, and which consists of four directives – Access, Authorisation, Framework and Universal Service).

The discussion on the regulatory treatment of OTT demonstrates one of the major shortcomings of the current regulatory framework because its statutory definition of an electronic communications service (ECS) is rather blurred. It leaves member states with a lot of room for interpretation as to whether a specific service consists of mainly the 'conveyance of signals', as demanded by the current definition of ECS under European law and thus qualifying as a regulated service. This is especially questionable where the provider of the respective service does not control the underlying transmission infrastructure and does not at least send all traffic through a central infrastructure. The statutory definition therefore allows for strictly technical interpretations (rather favouring the non-regulation of OTT services) as well as more functional interpretations (favouring regulation of OTT).

These uncertainties result in a patchwork of deviating regulatory views on OTT services across the EU. On the one hand, in an early statement in 2004, the Commission itself suggested that VoIP (voice over IP) services would not be considered to be regulated telecoms services. On the other hand, member states (as with the German national regulator and court with respect to Gmail, or the Belgian regulator and court with respect to Skype) took a stricter approach toward regulating OTT services. Similar to the German order demanding Google to register its Gmail service as a regulated ECS, both Belgian orders were also based on the assumption that Skype and SkypeOut qualify as regulated services under Belgian law, which is also based on the current European regulatory framework. Skype argued that it does not provide a regulated service, but merely offers software allowing its users to communicate without Skype's further involvement.

> **There is a patchwork of deviating views on OTT services across the EU.**

NEW CATEGORY: INTERPERSONAL COMMUNICATIONS SERVICE

With the draft ECC, the Commission now suggests an amended ECS definition. In future, ECS shall be subdivided into three service categories, and multiple categories may apply to the same service:

- **Internet access services** as defined in the net neutrality regulation (EU/2015/2120).[5] The definition includes all services that provide access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.
- **Interpersonal communications services** is a subcategory that includes all services that allow direct interpersonal communication and therefore also most OTT services.
- **Other services** are also included but only if they mainly consist of the conveyance of signals. According to the Commission, this shall include

transmission services for machine to machine (M2M) communications or for broadcasting, both of which do not include internet access or interpersonal communications.

Services in either of these subcategories shall only be subject to regulation if they are normally provided for remuneration. This requirement was also at stake in the German Gmail case, where the relevant questions (e.g. is a service provided for remuneration if it is provided free of charge to the users, but features paid ads?) are still unresolved.

If the ECC is adopted as currently drafted, most traditional as well as OTT communications services targeted at end users will qualify as interpersonal communications services (ICS) and therefore also as regulated ECS.

The ECC defines all services as ICS to which all of the following criteria apply:

- **Services that enable direct interpersonal and interactive exchange of information via an electronic communications network.** This includes all services that allow the user to engage in live voice and/or video conversation or to exchange text, voice, video or email messages. In contrast, transmission services for M2M communications, for example, will not qualify as an ICS because these services do not entail an interpersonal exchange of information, but merely facilitate the exchange of information between individual internet of things (IoT) devices or an IoT device and its human operator.
- **Services that allow such exchange of information only between a finite number of persons as defined by initiator and/or the participants.** This includes all services that allow the exchange of information among certain individuals or a limited number of persons. In contrast, it excludes broadcast transmission services from the scope of ICS. These services allow the exchange of interpersonal information, but broadcasting always entails one-to-many communications.
- **Services that are not ancillary features of another service**. This includes interpersonal exchanges of information that must not merely be a minor feature of another service to which they are intrinsically linked. This excludes, for example, a chat feature that is part of a video game from the scope of ICS.

To allow for a graduated level of regulation, the ECC divides ICS into two further subcategories:

- **Number-based ICS** are capable of PSTN communications either via E.164 numbers assigned by the service provider, or by enabling communication with third-party E.164 numbers (without assigning such numbers to its own users). Accordingly, only services which allow for a 'breakout' to the PSTN will be subject to the regulatory requirements addressed for number-based ICS.
- All other ICS are defined as **number-independent ICS**. This subcategory also includes services that use E.164 numbers for purposes other than the actual communications process (e.g. to identify user accounts as is the case with WhatsApp or iMessage).

Email such as Google's Gmail could be captured by the move from a 'conveyance of signals' to an 'interpersonal communications service'

Compared with the current framework, the Commission has decided to set aside the approach of defining regulated ECS merely based on technical features (i.e. the conveyance of signals). Instead, the ECC suggests adopting a more functional understanding of communications services.

NEW RULES FOR OTT SERVICES

Since most OTT services would qualify as an ICS based on the suggested ECC definition, these services will generally also qualify as regulated ECS. This does not, however, mean that all OTT services will be subject to a level of regulation similar to the one currently imposed on traditional telecoms services. Rather, the Commission wanted to involve a degree of deregulation for all regulated services. At the same time, where necessary, a more limited set of communications-specific rules should be applied to all relevant traditional telecoms services and OTT services – but only if the latter are comparable to traditional telecoms services.

Therefore, under the draft ECC, only number-based ICS will be regulated on the same level as traditional telecoms services. However, some level of regulation will also apply to number-independent ICS, i.e. OTT services that do not allow a PSTN breakout. As a general approach, the Commission chose to only make providers of number-independent ICS subject to regulatory obligations where this is required by public policy interests:

- The provision of number-independent ICS will not require any individual or even general authorisation by any national regulator. However, providers of number-independent ICS may still be required to notify regulators about their service commencement. But it will be sufficient to submit such notification to BEREC (the body of European regulators) instead of having to file it with the

competent regulator in each member state where the service shall be offered.

- Providers of number-independent ICS shall not have to participate in the dispute resolution scheme prescribed for all other ICS.
- Users of number-independent ICS will generally not have to be provided with the ability to reach emergency services via the respective service.
- Most of the sector-specific consumer protection rules set forth in the ECC will only apply to number-based ICS and internet access services. In particular, this concerns the following provisions which will not apply to number-independent ICS:
  - Transparency obligations demanding the publication of general or quality-of-service-related information
  - Additional information requirements that the ECC sets out with respect to end-user contracts
  - Sector-specific restrictions on the maximum duration of end-user contracts and rights to terminate such contracts
  - Providers of number-independent ICS shall have no obligation to facilitate change of provider.

Finally – and in contrast to some demands by traditional operators – number-independent ICS will not have to be interoperable with each other. Respective obligations may, however, be imposed by a national regulator if the general access to emergency services or the general end-to-end connectivity between end users becomes endangered due to an overall lack of interoperability among ICS. From today's perspective, such a situation seems unlikely. It may, however, occur if end users start using, or providers start offering, services with end-to-end (i.e. PSTN) connectivity on a larger scale.

While all of the aforementioned rules and obligations do not apply to number-independent ICS, OTT services with a PSTN breakout that can be qualified as number-based ICS will be subject to all of these respective provisions and traditional telecoms services will be as well.

CARVE-OUTS FOR PUBLIC SECURITY REGULATION

The current draft ECC generally allows only for little member state deviation or additional regulations on the topics within its scope. Nevertheless, its implementation into member state law will likely still not provide for a consistent regulatory framework for OTT (and other ECS) services across the EU.

In particular, countries will remain relatively free to impose further obligations on the offerings of all ECS providers (including number-independent ICS) where deemed necessary to ensure the protection of national security interests, to safeguard public policy, public morality and public security, or to permit criminal prosecution.

This is already the case under the current telecoms regulatory framework and will not change under the ECC. As a consequence, OTT providers may still be facing different regulatory regimes in different countries, in particular with respect to the following regulations:

- Depending on the respective member state law, such public security obligations may require providers to disclose information about their users (e.g. names, records or addresses)
- Providers may be required to maintain records on communications activity under applicable data retention regimes and to provide access to such information for law enforcement authorities
- Providers may be obligated to allow legal interception of ongoing communications among their end users.

These changes could raise tricky questions regarding how to comply with legal developments in this area from a technical standpoint, and in a way which will be consistent with privacy and confidentiality requirements in other EU legal instruments such as the e-Privacy Directive and the General Data Protection Regulation. Therefore, OTT providers should be prepared to increasingly become targets of requests from local law enforcement authorities, as was the case for Skype in Belgium. Like the requirements set forth by the ECC itself, such obligations imposed under national security legislation may also apply to non-EU based operators because member states could make compliance with such obligations a prerequisite of allowing a provider to offer its services in their territory.

> **Many OTT services are still only regulated to a minimal extent.**

NEXT STEPS

The Commission's proposed directive will now be forwarded for deliberations to the European Parliament and the European Council. It can be expected that these discussions will lead to further amendments of the current draft:

- Traditional operators cannot be fully satisfied with the current draft. Many OTT services they were complaining about (e.g. instant messaging services which are eating up their text message revenues) are still only regulated to a minimal extent, as opposed to their own SMS offerings
- On the other side, OTT providers may fear loopholes that countries can use to introduce further regulation under the public security umbrella. With many national governments seeing a problem in not being able to extend their surveillance of telecoms to OTT services, this fear may be justified.

If the ECC is adopted by the EU, it will still not have any immediate effect because, like any EU directive, it will first need to be implemented into national law in each member state. With this timeline in mind, the full scope of future OTT regulations will only become clear after implementation into national law. Realistically, this will not happen before mid-2019.

ANDREAS GRÜNWALD *is a partner and* ***CHRISTOPH NÜSSING*** *an associate at law firm Morrison & Foerster. They are based in Berlin, Germany. This article does not constitute legal advice.*

REFERENCES

1 Grünwald A and Nüssing C (2015). German court: Google's Gmail is a regulated telecoms service. bit.ly/2iZ5oW0

2 Belgian Institute for Postal services and Telecommunications (2016). Skype fined by BIPT regarding the SkypeOut telecom service. bit.ly/2ip8ktZ

3 Martin AJ (2016). Belgian court fines Skype for failing to intercept criminals' calls in 2012. The Register. bit.ly/2d00jhc

4 Proposed Directive establishing the European Electronic Communications Code. bit.ly/2caAmrr

5 Available at: bit.ly/1UDThtC

FACILITATING INNOVATION

We shouldn't be complacent that the regulatory approaches of today will be enough to support innovators in the era of the internet of things, says **JEREMY GODFREY**

Back in the year 2000, I was interviewing prospective telecoms strategy consultants. I asked them what they thought 3G would be used for. Some said video calling. Some talked about watching TV and movies on handsets. Some said purchasing music or checking email on the move. Nobody mentioned anything like WhatsApp, Twitter, Facebook or Snapchat. Nobody mentioned anything like Pokémon Go. Nobody mentioned anything like Google Maps.

This was four years before Apple even began work on the iPhone. So it's understandable that none of the candidates predicted applications that depended on smartphones with touchscreens, cameras and GPS. But once the smartphone was invented, millions of innovative applications were developed, and some of them have made much impact on people's lives.

What has enabled this innovation to happen? First, there is a huge market opportunity – there are more than 5 billion end users with connected devices. And second, there are very low barriers for innovators to bring new applications to market – the open internet provides a ready-made global distribution platform. Innovations that create value can rapidly become highly successful and the rewards for successful innovators are high. So, many of the world's most creative people are motivated to work hard and to take entrepreneurial risks.

GOOD REGULATION HAS BEEN CRUCIAL

Well-regulated telecoms markets have been critical in creating this environment. Competition has created incentives to upgrade network technology. And spectrum assignments have provided an essential input to enable investment in high-speed mobile networks.

In addition, a variety of regulatory tools have been used to ensure competition and choice for end users, and to create and uphold user rights. Operators of access networks have been constrained from raising prices to monopolistic levels; nor have they been able to control which applications their end users are able to use. The result has been substantial improvements in the quality of the world's connectivity, enabling exponential growth in the use of innovative applications and hence in the volume of data carried. All this has been achieved without a significant increase in the amount charged for the underlying connectivity.

Between 2008 and 2013, telecoms expenditure in the OECD grew by less than 0.2% a year. Over the same period Facebook grew its revenues more than tenfold, and its user numbers eightfold. This reflects the fact that enhanced connectivity would be of little value if it were not for the innovative applications that make use of it.

But will the innovation model of a small startup developing an application, getting it hosted in the cloud, and using the internet as a delivery platform still be applicable in the era of the internet of things (IoT)? And will today's regulatory approaches suffice to enable IoT-based innovation?

Just as it was difficult in 2000 to predict the applications and the business models of 2010, it's difficult today to imagine the IoT applications of ten years from now. Commentators write about a small number of examples, such as smart thermostats and autonomous vehicles. But in all probability some of the most significant IoT applications of ten years' time will be beyond what most of us can currently imagine. But we can perhaps imagine the tools that innovators will need. Let's imagine Thingamabob, an IoT-based start-up five or ten years from now. The idea and the business model that the founders have in mind could have some or all of the following characteristics:

> **"It's difficult today to imagine the IoT applications of ten years from now."**

- Thingamabob has designed a thing called a Gizmo
- Some Gizmos will be used at fixed locations, others will be used on the move, including when the user travels across international borders
- In order to work, Gizmos will need to communicate with one another and with Thingamabob. Some of these communications will need to be guaranteed to have very low latency
- Users will typically buy a dozen or more Gizmos, and subscribe to a service run by Thingamabob
- The user experience is kept very simple, with no configuration needed by the end user or in the supply chain. Once the user has registered their Gizmos, they just work
- The end user doesn't have to arrange connectivity.

The cost of wide-area connectivity is included in the subscription to Thingamabob's service. But if the user wishes, Gizmos at fixed locations can be connected to a user-supplied wireless connection (such as WiFi) with a discount on the subscription.

What would be necessary for the founders of Thingamabob to have an easy route to market, so that their Gizmos and the associated service can compete with other innovations?

Of course, Thingamabob will need there to be low-latency wireless networks such as 5G operating in all the countries where Gizmos are to be used. There is a lot of spectrum management work needed to bring this about, but the nature of the work is well understood. The world's regulatory community knows how to go about setting standards, harmonising band allocations and assigning spectrum rights of use. There will be important decisions to be made about matters such as shared use of spectrum, coverage obligations and the timing and design of spectrum assignment processes. Difficult though some of these decisions are, it seems likely that spectrum will get assigned for the 5G networks that Thingamabob's service will require.

Current ideas about IoT applications may not be useful when predicting what is to come

5G SPECTRUM MAY NOT BE ENOUGH

But the mere existence of 5G networks may not be enough to ensure the company can deploy its service cost-effectively. Here are some of the things it may need:

- Access to computing resources that are located within the 5G network. The need for reliable low latency connections between Gizmos and the Thingamabob service means that the company may not be able to use data centres located far away from the places where Gizmos are being used. Instead it may need to run parts of its application within the 5G network – maybe at cell sites, or at aggregation nodes or at switching centres.
- An ability to easily remotely reconfigure Gizmos to work with different 5G networks. Without this, Thingamabob could not deliver the simple customer experience that it desires, find it difficult to switch its fleet of Gizmos from one 5G operator to another which would limit price competition among network suppliers, and could find itself stung with exploitative roaming charges when Gizmos move across national borders.
- Non-discriminatory commercial deals for 5G connectivity that reflect costs. If 5G operators are able to impose an excessive toll on Gizmos, or favour a Gizmo competitor for some reason, then Thingamabob's founders might not be able to sell Gizmos profitably at a low enough price to build the scale they need to be successful.
- An ability to work with a global supplier instead of cutting deals with national 5G operators – If Thingamabob had to cut deals with 5G operators in every national market, it could incur heavy costs in travel, legal fees and in employing commercial staff. The process would also significantly delay its time to market. And if the result was a multiplicity of commercial deals struck on different terms, it might also have to adapt its application to work differently in different markets, increasing costs and damaging the customer experience.

The barriers to Thingamabob's innovation would be substantially lowered if it could deal with a global service provider that could provide it with virtual computing resources, and low-latency 5G connectivity between Gizmos and those services. Such a service provider would be a combination of a cloud computing provider and a multi-country MVNO. Will such providers emerge as a result of competition, or will regulatory action be needed?

Spectrum constraints mean that today there are no more than a handful of 4G operators in each national market. But the nature of today's internet means that mobile network oligopolies have not so far been an inhibitor of innovation. In future, however, companies like Thingamabob may need more intimate access to 5G networks. Regulators will need to assess whether innovation by IoT providers is at risk of being inhibited by the market structure. And if regulatory intervention is needed, it will probably require greater international collaboration so that companies like Thingamabob can operate on a global scale.

We are still several years away from needing to make decisions. But it is not too early to have a debate about the role of regulation in enabling IoT innovation. When regulatory frameworks are being reviewed – as the EU framework is at the moment – it would be a pity if all the debate about 5G was related to spectrum management issues. It could well turn out that the main focus should be on regulatory reform that facilitates IoT innovation.

JEREMY GODFREY *is the chair of ComReg, the Irish communications regulator. The opinions expressed in this article are his own.*

The IIC

Five reasons to join...

The IIC enables the balanced open discussion that shapes the public policy agenda for the converged TMT sector...

1. The Chatham House Rule gives participants the freedom of 'off the record' expression and debate

2. Senior policy makers and regulators share their challenges and success stories

3. Members build collegiate relationships with international regulators

4. Members can attend local chapter meetings for free wherever they are in the world

5. This collaborative, supportive network helps facilitate the creation of good policy

Thank you for the very stimulating and candid discussions. I was impressed with the quality and the level of the debate

Dr Syed Ismail Shah
Chairman
Pakistan Telecoms Authority

Types of membership

- IIC Partnership
- Industry Membership
- Regulator Membership
- Associate Membership

Visit www.iicom.org
Call +44 (0) 20 8544 8076
Join the IIC's LinkedIn Community for year round debate

Shaping the Policy Agenda

INTERNATIONAL INSTITUTE OF COMMUNICATIONS

Inter MEDIA

ISSN 0309 11 8X

Annual subscription £175

Online: www.iicom.org

International Institute of Communications
Highlands House
165 The Broadway, London SW19 1NE
Tel **+44 (0)20 8544 8076** | Fax **+44 (0)20 8544 8077**