CHILDREN: A SPECIAL CASE FOR PRIVACY?
WEIGHING UP THE ROLE OF DATA PROTECTION
By Sonia Livingstone
The IIC

Communications Policy & Regulation Week 2018

8-11 OCTOBER 2018, MEXICO CITY

Communications Policy & Regulation Week provides an unhurried collegiate environment in which senior international players involved in regulation, policy-making and industry come together to inform the policy agenda for the foreseeable future.

<table>
<thead>
<tr>
<th>International Regulators' Forum</th>
<th>8-9 October 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>The only independent international forum that brings together statutory national regulators in a closed, collegiate environment to debate policy issues.</td>
<td></td>
</tr>
<tr>
<td>IRF meetings are closed and carried out under the Chatham House Rule, enabling open and honest dialogue between senior regulators.</td>
<td></td>
</tr>
<tr>
<td>Free to members.</td>
<td></td>
</tr>
<tr>
<td>Participants come together to discuss the issues which affect them, to share best practice, and to build relationships with their peers.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>49th Annual Conference</th>
<th>10-11 October 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Around 250 senior executives and public policy-makers in the TMT sphere come together from across the globe to discuss big picture themes affecting the communications community.</td>
<td></td>
</tr>
<tr>
<td>Participation enables them to share knowledge, discuss the issues, and learn about technological advancements and the regulatory challenges that these present.</td>
<td></td>
</tr>
<tr>
<td>In addition to debating the issues, participants build and strengthen relationships with their peers.</td>
<td></td>
</tr>
</tbody>
</table>

Plus, workshops, networking events and private meetings throughout the week

REGISTRATION IS NOW OPEN

To register now, scan the QR code or visit iicom.org/events

Early bird rates available until 4 September 2018

TO DISCUSS MEMBERSHIP OPTIONS...

CALL: +44 (0) 208 544 8076
EMAIL: a.millwood-hargrave@iicom.org

INFORMING THE POLICY AGENDA iicom.org
The topics that are continuing to dominate the digital world are the power of the big internet platforms and a raft of issues that are surfacing in almost all walks of life, including fake news, online hate speech, political interference, privacy and algorithms. As Terry Flew keenly observes in this edition, there is a crisis of trust. He highlights platforms against the backdrop of two major intersecting themes: the digital economy and society at large. The former concerns largely unregulated market monopolies; the latter the media, data and privacy issues that are leading to a lack of trust in public institutions and media. Both Flew, and Vicki Nash and Mark Bunting in a complementary article, consider what regulatory steps could be taken, particularly with multistakeholder and accountability approaches. Underpinning the digital economy and platforms though is also the competition regime, which is eruditely taken to task by IIC board member Tim Cowen and a colleague (see news item, page 2). They say that, “Current competition law is not fit for purpose; regulators follow pro-monopoly standards.” So are we at a fundamental crossroads in reform? I’m thinking that in the short term we’ll see a lot more regulatory tinkering but, beyond that, pressure could build for competition reform on a tectonic scale... maybe the breaking up of some of these monopolies.

Chris Chapman, president, IIC
COMPETITION
LAW IS ‘NOT FIT FOR PURPOSE’

A British thinktank has issued proposals for a radical overhaul of regulation of the technology sector, which it argues is “unfit for purpose, incentivises bad behaviour and has failed to address ethical questions about big data and its use”. In the report, “Technopoly” and what to do about it: Reform, redress and regulation, ResPublica considers that “something has gone wrong with our markets and our competition law” and uses colourful language in saying that “monopolies are an evil that restrict ownership and trade... It is not too extreme to say that we increasingly risk re-feudalising society, where ownership in any substantial degree has become an unrealisable dream for too many. This rentier society has created a new digital road to serfdom and unless or until we chart a different path, we risk recreating the market dynamics of the middle rather than the modern age.”

The two authors, who include IIC board member Tim Cowen, make their case with the technology and media markets but highlight higher levels of concentration across a range of industries. Among their arguments:

- Current competition law is not fit for purpose; regulators follow pro-monopoly standards
- Consumer choice and innovation should be the new norm, not just consumer welfare
- Competition law needs to stop privileging big business and focus on the benefits of small businesses and market structure
- Social media is media, and should be regulated in the same way as traditional media
- Current merger controls should be changed to meet the challenges of the digital age.

The report addresses the issues from UK and European perspectives noting that concerns so far have been mainly based on data from the US. Intermedia will publish an article on the main recommendations for competition reform in due course. The report is at bit.ly/2zf9sia

NET NEUTRALITY
INDIA APPROVES RULES

India’s Department of Telecommunications (DoT) has accepted the recommendations made last year by the regulator, TRAI, to adopt tough rules on net neutrality, in what is being seen as a big victory for the open internet movement. “Any deviations and violations of the rules of net neutrality – which come into effect almost immediately – will be met with stiff penalties,” DoT secretary Aruna Sundararajan told the Times of India. There are though exceptions, which sound like the “special services” mooted by the European Commission, such as autonomous driving and telemedicine, which may require prioritised ‘fast lanes’. The government is to set up a body to monitor and enforce net neutrality, and the regime will include monitoring of mobile internet traffic. Also approved is India’s National Digital Communications Policy 2018.

TRAI and BEREC, the European regulators’ body, have signed a joint statement on preserving rules for an open internet.

CANADA
BROADCAST PROTECTION

The Canadian Radio-television and Telecommunications Commission (CRTC) has published a report on the future of broadcasting in Canada. The report proposes tools and regulatory approaches to support the production and promotion of audio and video content made by and for Canadians that is discoverable by audiences in Canada and abroad. It says that there are social and cultural responsibilities associated with operating in Canada and that all players benefiting from the Canadian broadcasting system should participate in an appropriate and equitable manner.

ITU
BEST PRACTICE GUIDANCE

The ITU has issued best practice guidelines on “new regulatory frontiers to achieve digital transformation”. The document calls for frameworks that foster the potential of emerging technologies and business and investment models that support digital transformation, while more specific steps are put forward for policy approaches, including regulatory sandboxes for companies wanting to test an emerging technology or innovative service without being bound by usual regulations, and 5G pilot projects. Also put forward is “regulation by data” for public participation in the regulatory process, based on information from stakeholders and users; and mechanisms for cooperation across sectors such as banking and health. See bit.ly/2zyH5bi

NOT JUST FOR CITIES: This is Guttannen, Switzerland, a remote mountain village of only 300 people and the location for a 5G test site by operator Swisscom. Although an upgrade to fibre to the curb is planned for 2021, it won’t reach all premises so Swisscom is trying out 5G fixed wireless access in the 3.5 GHz band to a small number of customers. For details see bit.ly/2ztFxia

Not just for cities: This is Guttannen, Switzerland, a remote mountain village of only 300 people and the location for a 5G test site by operator Swisscom. Although an upgrade to fibre to the curb is planned for 2021, it won’t reach all premises so Swisscom is trying out 5G fixed wireless access in the 3.5 GHz band to a small number of customers. For details see bit.ly/2ztFxia
REGULATION
OFCOM TAKES AIM AT SOCIAL MEDIA

The chief executive of UK regulator Ofcom, Sharon White, has warned regulatory action may be on its way for social media sites that publish news, in a move that brings the platform or publisher debate to the fore. She says that “online companies need to be much more accountable when it comes to curating and policing the content on their platforms, where this risks harm to the public”, but while welcoming actions by the major online players, “we consider that the argument for independent regulatory oversight of their activities has never been stronger.”

White continued: “Such a regime would need to be based on transparency and a set of clear underpinning principles. In practice, this would place much greater scrutiny on how effectively the online platforms respond to harmful content to protect consumers, with powers for a regulator to enforce standards, and act if these are not met.”

As part of the evidence base that will shape Ofcom’s regulatory proposals, which should come this autumn, it has published two qualitative research reports on what people think and feel about news, and how they consume it. The findings include:

● Online news is playing an increasing role – almost two-thirds of people use the internet for news
● Social media has blurred the boundaries between news and other content
● People often engage with news in passive and shallow ways
● People are aware of concerns about online news but can’t articulate what these mean in practice. Some try to counteract these concerns by relying on shortcuts and intuition to assess the reliability of news – but these mechanisms have limited effect. These challenges sit within a broader context of distrust in media and other institutions, says Ofcom. The research is at bit.ly/2JooJJc

PLATTFORMS
THE PROBLEMS OF POWER DEFINED

Digital Dominance, a book edited by Martin Moore and Damian Tambini, names “the power of Google, Amazon Facebook and Apple” in presenting the evidence behind the rising tide of criticism of the tech giants. Tambini says Digital Dominance is a “problem-definition” book rather than a “solutions” book, taking an interdisciplinary approach to questions such as the implications of the effect of tech giants’ market and social power on media pluralism, freedom of expression and electoral legitimacy. At a launch event the panel brought three main themes to the table: the inadequacy of current competition regulation; the extent to which self-regulation of tech giants is desirable; and the viability of hastily constructed regulation, without considering wider implications. See amzn.to/2uBAZQY for book details.

TERRESTRIAL TV
FRANCE PLANS NOT TO REGULATE DTT

Arcep, France’s regulator, has issued market analysis on the state of competition in the wholesale market for terrestrial broadcasting services, saying it does not plan on continuing to regulate this market. Arcep says digital terrestrial television’s (DTT) share of TV viewing continues to decrease steadily, as broadcasting over broadband gains in popularity. In France, IPTV broadcasting was widely adopted thanks to triple play bundles, and DTT’s replacement is expected to continue as content providers are gaining access to a growing number of alternative outlets, so it is no longer relevant to regulate only DTT competition. Arcep does say that DTT remains a significant TV access system and its analysis “in no way predicts its future”. See: bit.ly/2yB6S1m

IIC EVENTS
8-11 October, Mexico City
IIC Communications Policy and Regulation Week, comprising the International Regulators Forum and IIC Annual Conference
4-5 December, Washington
IIC Telecommunications and Media Forum
18-20 February 2019, Kuala Lumpur
IIC Regional Regulators Forum and Telecommunications and Media Forum

IN BRIEF
SMART CITIES REPORT
McKinsey has published a report, “Smart cities: Digital solutions for a more livable future”, which analyses applications and finds that cities could use them to improve some quality-of-life indicators by 10–30%. But even the most cutting-edge smart cities are still at the beginning of their journey, the report notes. Download at mkt.co/2jish1c

MERGER STUDY
Mergers reducing the number of mobile operators from four to three may push prices up in the short to medium term, even with remedies such as MVNO access, according to a study published by EU regulator body, BEREC. See bit.ly/2kgawzg

ASIA-PAC AND 5G
Asia Pacific is on track to become the world’s largest 5G region by 2025, led by pioneering 5G markets such as Australia, China, Japan and South Korea, according to the latest GSMA Mobile Economy report.

CALIFORNIA PRIVACY
California has passed a consumer privacy act that includes provisions similar to the EU’s GDPR. It will give residents of the state the right to request what personal information businesses collect about them, who the information is shared with or sold to, and the ability to opt out of such sales. It will be in force in 2020.

POLE VAULT
The US FCC has announced model agreements for small cell and 5G deployment for the city of San José, under which carriers will access city owned poles and help close the digital divide in San José, where more than 95,000 residents still lack access to broadband internet.

www.iicom.org

July 2018 Vol 46 Issue 2 | InterMEDIA 3
SMART POLICY

At the IIC’s TMF in Brussels, artificial intelligence and data privacy were dominant issues for single market thinkers, as CRISTINA MURRONI reports.

"A key challenge will be accountability: should an algorithm developer be accountable for the input, throughput, or the ultimate outcome?"

The IIC’s Spring Telecommunications and Media Forum (TMF) held in Brussels, hosted by Belgium regulator BIPT, explored the theme of artificial intelligence (AI) from several perspectives. The recent events surrounding Cambridge Analytica and Facebook have dramatically brought to the fore the complexities of dealing with data-rich services, and the need for a comprehensive debate on the ethics of the digital world.

With an inspirational peek into the future, Rohit Talwar (Fast Future Research) set the ball rolling. He stressed the importance of increasing our understanding of AI inside businesses before committing to investments, as nearly half of $800bn of IT investment is wasted because of people not understanding technology. When we start to think about dealing with the impacts of AI, he continued, we are no longer just talking about data or security, but also about social impact. Since this is state of the art technology, those who develop it are either being educated inside a business, or they’re going to be self-taught. “In which case, they’ll learn a lot about how to do machine learning, they’ll learn a lot about data science, they’ll learn a lot about the mechanics of deep neural networks. But they won’t learn about the ethics issues, they won’t learn about the social impact issues” – and that is something that we need to work on.

Skills development and large scale research are the two areas that Europe needs to urgently address, according to Andreas Tegge (head of global government relations at SAP). The biggest hurdle, however, may well be social acceptance: we need to start building it now, as the biggest impact of AI is to come. Lenard Koschwitz (Allied for Startups) brought the voice of new companies into the discussion. He called for clear policies that help data flows and innovation if we want to increase the number of AI startups in Europe, because these new companies are both platforms and users of data-driven systems.

Antonio Nicita (AGCOM, Italy) reported on a novel joint effort by Italy’s competition and privacy regulators on a first assessment of an AI strategy from a regulatory–competition point of view. Juha Heikkilä (DG Connect, European Commission) provided the perspective of the European Union. While the B2B side of AI is quite strong in Europe, the B2C and the platform side is where the weaknesses are. He argued for a European approach to drive growth in AI applications in Europe’s key industries, because of the critical mass required. Europe has to boost industrial and research capacity in AI and promote the uptake of this technology on a really wide scale: its benefits can only be really reaped if they can be spread broadly across the economy. The Commission is setting up a European AI alliance to anticipate the social impacts of AI, which is expected to come up with ethical guidelines early next year.

**ARTIFICIALLY INTELLIGENT ETHICS?**

Ethics and safety were the focus of another TMF panel: Krisztina Rozgonyi (University of Vienna) claimed that 2018 will be remembered as a watershed moment when online media platforms are finally considered as editors whose ethical and professional standards should be monitored. Andrea Renda (CEPS) proposed that regulators should play with experimental regulation, regulating through browser extensions, through specific apps, through third party certification, forms of auditing and so on. He claimed that one of the key challenges will be accountability: should an algorithm developer be accountable for the input, for throughput, or for the ultimate outcome?

For Estelle Massé (Access Now) the Convention on Human Rights already provides the ethical framework that applies to all technologies. But what outcome do we want from AI? Is it productivity? Is it fairness? We need to be clear about this: an algorithm may deliver on productivity but completely fail on social values. Whether AI delivers benefit for society depends very much on the result of the discussions we’re having now, she said.

Ondrej Sočučka (Google) explained that fairness is one of the focuses for Google, not only because of ethics, but also because it makes business sense. Google’s multi-pronged approach to fairness includes a tool that allows users to visualise their data composition and whether there may be some bias. Also, the company looks at how algorithms are working, striving to solve and correct them if there is an undesired effect. Another approach to fairness is the release of a number of free online courses to promote wider societal expertise.

Finally, Shamus Rae (KPMG) brought to the fore the possibility of inequalities of opportunity.
brought about by AI destroying jobs. Research shows that in the US 25% of the working population is underemployed, meaning that they’re trained for jobs which are more sophisticated than the ones they’re doing today, and the figure rises to 40% for people under 30. This means that we urgently need a conversation about the employment, skills and capabilities that we need.

**INDUSTRY APPROACHES**

The industry perspective on AI was provided by a panel opened by Ieva Martinkenaite (Telenor-NTNU AI-Lab/Start IoT), who explained that the first step in Telenor’s strategy is about building skills, and the second is to look for pools of available data that the big internet companies have not tapped yet, like on IoT. In Europe, a promising AI strategy would need four elements: data sharing, skills building, ethics by design (where Europe could lead) and innovation systems, where the companies of the future can thrive. Claudia Selli (AT&T) pointed at the large AI investments made by companies and venture capitalists: $26–39bn in 2016. Often these investments use open platforms for all companies to share some of the advances, because lowering barriers to access to AI is a key issue for adoption.

George Wright (BBC) illustrated how the BBC uses AI to search 90 years’ worth of archives, where the key challenge is to find both traditional video skills and the new, big data kind of skills. The BBC is further looking at what AI can offer, and is engaging the European Broadcasting Union to come up with innovative ways to use AI in production or audience research. Cate Nymann (Cisco) stressed the importance of AI to reduce cost and optimise network use in the telecoms sector, particularly as video traffic increases and a more heterogeneous set of services, devices and data flows for IoT start to take off. AI allows companies to write the policy – what the networks should do – and then see this automatically deployed over the network, using predictive approaches.

**SAVING PRIVATE COMMUNICATIONS**

A panel on privacy and data protection was introduced with a keynote by Christian D’Cunha on behalf of the European Data Protection Supervisor. He described the EU approach, enshrined in the GDPR and forthcoming e-privacy regulation. The EU approach emphasises the principle of accountability, requiring that if you derive value from processing personal information, then you must give an account to the people affected, as well as to the regulators, whose job is to oversee compliance. That is why the obligations of the controller are at the centre of the GDPR, along with provisions such as codes of conduct, and certification for demonstrating compliance.

Communications are meant to be, by default, confidential: that’s what people expect and that’s what the EU requires in Article 7 of its Charter of Fundamental Rights. EU privacy must now cover services beyond traditional telecoms and network providers, halting constant snooping on people’s communications via services and apps, and stopping companies forcing people to accept being monitored in exchange for accessing content online.

Rosa Barcelo (DG Connect, European Commission) expanded on the e-privacy regulation proposal: it provides overall protection of confidentiality of communications, no matter who carries the messages, no matter whether the message is a text, or an email, or a WhatsApp message: the proposal is agnostic as to who does it, or what is done.

Compared to existing regulation, however, it enables more to be done with data, for purposes of network security and to offer services that are targeted and do not impinge on the privacy of the individual. Cornelia Kutterer (Microsoft) observed that perhaps confidentiality should have been approached not merely from a data protection perspective but from the wider private sphere, relating it to the expansion to the cloud. In this perspective, it is good news that the European Data Protection Supervisor is fostering dialogue across agencies and regulators, because the wider the scope, the better the outcome.

Nick Wallace (Center for Data Innovation/ITIF) expanded on AI applications for industry rather than consumers, arguing that this is the area where the EU currently has a competitive advantage. He warned though that if the GDPR’s articles on the
right to meaningful information are taken to mean that there is a right to explanation, then this could lead to adoption of less efficient algorithms because they may be easier to explain to non-scientists.

Fiona Taylor (Verizon) sketched an ideal regulatory environment: it would have horizontal rather than sector specific regulation, and be principle-based rather than technology specific. Futureproof regulation is absolutely essential, as is harmonisation, and especially international conversations because compliance with varied rules has an impact on the business case for international services, has costs and may lead to services not being offered.

The discussion that followed highlighted, however, that the current drive is more towards facilitating and growing the AI paradigm than it is about regulation: how to create the right conditions for innovation, how to reskill the workforce.

**SOMEBODY BETWEEN EX-ANTE AND EX-POST**

Much of the discussion on the competition panel focused on practical ways to provide some remedy while anti-trust investigations take their course: reaching a settlement, issuing warning letters, threatening interim measures were some of the examples mentioned. The length of time needed to reach a decision when dealing with these complex new industries topped the list of concerns for all speakers.

Mette Alfter (Frontier Economics) explained that the concern with algorithms is that they might mean more tacit collusion in more markets. Opinions are polarised, with one view insisting that nothing will change and the other fearing that current competition tools will not work and collusion will spread. The negative view holds that the speed and amount of information available will make collusion more likely and, especially, the predictability of algorithms means that pricing software may create collusion across companies.

Francesco Liberatore (Squire Patton Boggs) added the issue of liability: who is liable for decisions or actions taken by self-learning machines? Is it the programmers, the users, the owners or the beneficiaries? Antitrust liability can only arise if the conduct has been committed intentionally or negligently. Therefore, the competition authority would have to demonstrate that the illegal action was anticipated or pre-determined, for example through programming instructions to AI, or that it could be reasonably foreseen.

Ben Wreschner (Vodafone) suggested that pricing for customers-specific services may be the area where AI use is more problematic, because it tends to reduce transparency, making it difficult for regulators to monitor markets. AI may just speed up the process of the markets reaching equilibrium: in imperfect markets, monopoly may be reached much faster.

Emily O’Reilly (EFTA Surveillance Authority) proposed that in the same way that anti-competitive conduct by an employee is attributable to an employer, even if they are acting contrary to the instructions of their employers, companies cannot distance themselves from their algorithms, even if their outcome is contrary to the original instructions that were given to such programmes. So it would seem prudent for algorithm developers and their owners to maintain some sort of tracking system or clear audit trail for the development and use of these algorithms.

**REGULATORS’ RESPONSE TO AI**

Sébastien Soriano (head of Arcep, France’s regulator), floated the idea that AI means that value in the sector is shifting from networks to devices. Today most internet experiences happen on a mobile device, and when enforcing net neutrality rules, these apply to ISPs and very little to the duopoly of Android and iOS. And this despite the fact that, in the future, we are likely to simply ask our phone assistants, which are bundled in the device, to purchase something for us, and they will do the selection. The key worry is that control of the operating system comes with vertical integration and exclusive deals, which threaten the idea of open networks.

On the other hand, as was emphasised in the panel discussion, we should remember that there needs to be evidence of harm to competitors or consumers before we act. Indeed, the objective is to extend freedom of choice for users, and to ensure that the innovation environment remains as open and permissionless as it was when the digital economy started. Stephen Unger (Ofcom, UK) suggested that while network effects may not be an issue as long as there is a threat of entry, the acquisition of large amounts of data can be the way in which companies extend a transitory competitor advantage to a permanent one. AI, particularly machine learning rather than algorithms more generally, exacerbates that concern because of the importance of large datasets in machine learning.

Monica Ariño (BT Group) emphasised that companies are asking questions about ethics as they expand their AI capabilities, and they need a framework of clear and predictable rules. Recognising from the start that the data companies have is incomplete and biased, needs to be a factor when designing AI solutions that are based on it. Jean-Jacques Sahel (ICANN) reiterated the importance of dialogue across regulators (data protection authorities, media and telecoms), across businesses and across research, especially as the idea of an all-encompassing regulator may be unrealistic, and the international dimension is likely to be very important. Regulators need to maintain a “constant dialogue”, a form of “distributed collaboration” with stakeholders and the technical community.

**Companies are asking questions about AI ethics and need a framework of clear and predictable rules.**

**CRISTINA MURRINI** is a telecoms and media analyst.
LATIN LESSONS

The IIC’s second TMF of the year took place as usual in Miami, focusing on Latin America. Connectivity and disaster recovery were themes. By CRISTINA MURRONI

The IIC’s Miami Telecommunications and Media Forum (TMF) has a special focus on the Americas and Caribbean, and this year was no exception, with Nievia Ramsundar (Telecommunications Authority of Trinidad and Tobago) kicking off the first panel on competition and investment. He held that keeping consumers happy is the main goal of regulation, as consumer take up ultimately feeds all the layers of the market. Lindsey Fussell (Ofcom, UK) focused on cost containing measures to spur adoption of ultra-fast broadband, which in the UK is taken up by only 3% of households. Adolfo Cuevas Teja (commissioner at Mexico’s regulator, IFT) highlighted the importance of creating a truly independent regulator, and setting realistic objectives based on data and observation to attract investment. Mexico has seen rewards for this strategy: 4G coverage has jumped from 25% to 80% in a few years, with better speeds than the US.

Ernesto Orozco (National Television Authority of Colombia, ANTV) echoed that view, reporting that despite industry disruption by over the top (OTT) players, the television sector has overall benefited from competition, growing by 40% with the new entrants. As competition brings prices down, regulation should provide incentives to investment, and adopt a lighter and simpler approach.

ROADMAP FOR THE DIGITAL ECONOMY
Colombia is one of the few countries equipped with a plan to take the country to its digital future, reported Juan Manuel Wilches (commissioner at regulator CRC). The roadmap identified eight main challenges, ranging from coordinating all agencies and government sectors involved, to promoting net neutrality and the adoption of state-of-the-art technology. Multisector committee meetings are held regularly and a first study into the impact of the digital economy on several industries has been launched. Giuseppina Curreli (AT&T), agreed that a vision is needed, but added that it should be supported by a regulatory framework that focuses on providing connectivity.

John Winter (Liberty Latin America), stressed how connectivity is paramount, but is not necessarily an operator’s most expensive investment: content is even more costly, so it is essential to effectively address piracy.

David Geary (Digicel Group) presented the Caribbean Regional Communications Infrastructure Program (CARGIP), a public-private partnership co-financed with World Bank loans, as an example of the transformational project that can also take place in small island states. He felt, however, that the project was a missed opportunity to design a futureproof regulatory structure for the islands involved. Caribbean Community (CARICOM) heads of government have approved a roadmap for a Caribbean “single ICT space”, reported Bernadette Lewis (Caribbean Telecommunications Union), and Caribbean governments now need to develop a completely new approach. They need to lead by example, becoming adopters of the technology and delivering services to citizens efficiently.

INVESTING FOR THE FUTURE
Latin America needs to make better use of spectrum and needs infrastructure for data centres and international connectivity, observed Enrique Iglesias Rodríguez (Inter-American Development Bank, IDB), who recommended partnering with the private sector for any network building. Eduardo Guzmán (Squire Patton Boggs) addressed the huge political problems and time delays experienced when dealing with authorisations at the local level. Perhaps the regulator should have powers to override the local authority on these matters, and certainly these issues should be addressed when planning investments.

Looking at the Mexican experience, Andrés Acedo (Acedo Santamarina) reported on the two public networks expected to provide universal connectivity: the shared 700 MHz wholesale network and the trunk network that runs through the electricity lines of the Mexican Electricity Commission. Each stage of the process has gone to plan and the first milestones have been achieved. Robert Pepper (Facebook) used the inclusive internet indicators co-developed with the Economist Intelligence Unit to show that the gender gap in Latin America is much less than other regions with similar income levels. Privacy tops every other concern when it comes to using the internet, with 91% of Latin American users listing it as their main concern, compared to 80% globally.

Melesia Sutherland (CANTO) described the challenges facing companies investing in infrastructure in the Caribbean region and called for a solution to safeguard sustainable network investments in these island states. Most states are hurricane-prone islands with 100,000 inhabitants on average: risks are high, revenues are limited, and global internet players use up to a third of network capacity and provide...
no investment. One proposal that emerged from the discussion was to give more flexibility to existing operators to make the shift towards new data-driven business models. This would enable them to reap the synergies with global platforms, benefiting from increased demand for data and often also greater economic activity.

WHAT ABOUT DATA CENTRES?
Andres Maz (Amazon Web Services) reported that the growth of cloud-based services, while fast, is undermined by the scarcity of talent (system engineers) to support it and by the lack of procurement vehicles for cloud. Bandwidth, energy, peering and quality of service are issues that need to be addressed if governments want to attract more infrastructure for the development of the cloud. Ana Carolina da Motta Kohlitz (Cullen International) looked at data localisation requirements in the region and concluded that there are no general data localisation requirements in data protection laws, but rather specific provisions in several sectors, like banking or the public sector, in several countries.

Joshua Forman (GlobeNet Telecom) focused on the CLOUD Act, which clarifies that US service providers are required to disclose all data in their possession, custody and control, regardless of the location of the data. The EU’s GDPR applies to any company that is located in the EU, or collects information on EU citizens, or offers goods or services in the EU.

Robert Pepper reported on Facebook’s investments to connect data centres, mostly in partnership with operators, with several submarine cables and in edge points of presence and other technology co-located with operators.

When discussing policy to attract investment in data centres, many felt that good intentions often clash with other government policies: for example, high taxes and duties on IT equipment, or specific requirements that raise the cost of building and operating large high-tech facilities.

USING SPECTRUM TO FUEL NEW INNOVATION OPPORTUNITIES
Spectrum discussions began with an overview of the EU’s strategy for 5G by Marjoinein Geus (Bird & Bird). Europe has allocated three bi-linear bands, and work is advancing on freeing up the frequencies and establishing the standards. The goal is to increase harmonisation and minimise uncertainties, but with many of the 28 national regulators resisting the European Commission’s effort to harmonise, it is difficult to achieve.

Thomas Sullivan (FCC) added the US perspective, where the FCC is favouring flexible use of frequencies, and supporting 5G development by freeing up as much spectrum as possible and developing secondary markets. Gabriel Solomon (Ericsson) reiterated the usefulness of a pro-innovation approach such as the FCC’s. Considering that connectivity gaps still persist, and public funding is very limited, spectrum could be used to get operators to commit to filling those gaps, either by ringfencing auction proceeds or by offering licence extensions in exchange for a commitment to invest in given areas, as pioneered by France.

The Q&A session looked at the policy of reserving spectrum in auctions to enable a new entrant: the general perception from experience is that this does not work well, especially when trying to make space for a fourth or fifth entrant, and that conditions placed on how spectrum is made available actually make efficient use of spectrum more unlikely.

PREPARING FOR THE HURRICANE SEASON
Nievia Ramsundar (Telecommunications Authority of Trinidad and Tobago, TATT), explained the rules and tools available in case of natural (or man-made) disaster. The most important stage is pre-disaster, when the task is to mitigate and prepare, and while laws do not require the networks to be resilient, the GSMA has identified this as a key consideration. Post-disaster, data sharing and cooperation are key: international cooperation helps response, while competing telecoms operators working together locally can minimise access issues and increase redundancy by using each other’s networks.

Zenji Nakazawa (FCC) reported on how the FCC response was tested by the string of hurricanes in 2017, and added that the agency is looking at ways to improve the geolocation efficiency of emergency texts sent to mobiles.

Gonzalo de Dios (Intelsat) emphasised the role of satellite communication as a critical backbone for infrastructure in the event of natural disasters. Data shows that the impact of natural disasters is getting bigger, and in 2016 alone the damages had a cost of about $154bn. This makes it all the more important to have a readiness plan, and especially to make sure these plans are implemented – which may require involving government agencies like customs, the military etc.

Melesia Sutherland (CANTO) reported on the preparedness of the Caribbean islands. Network resilience appears to be less of a problem – the equipment did not fail, but succumbed to other environmental issues, such as flooding. David Geary (Digicel) rounded off the discussion with experience from Dominica and underlined the urgent need to address which operators should contribute to the cost of restoring networks, and rebuilding them with greater resilience.

Cristina Murroni is a telecoms and media analyst.
Policymakers have been captivated by 5G as they identify enhanced mobile broadband, the internet of things (IoT), massive machine type communication, and ultra-reliable and low latency communication as enablers for the fourth industrial revolution, smart cities and smart nations.

There appears to be an international race to become the world leader in 5G and policymakers have launched initiatives towards that goal. This is exemplified by the European Commission in its statement, “5G will enable industrial transformation through wireless broadband services provided at gigabit speeds” and the launch of an action plan to make this happen. Further policy direction came from the ministerial declaration in Tallinn, “Making 5G a success for Europe”, which states in its opening paragraph, “We share a common vision for a fully connected society and the path towards the gigabit society. 5G will enable the delivery of a diverse set of applications beyond the focus of the traditional mobile broadband market.” Top of the list of commitments is: “Make more spectrum available in a timely and predictable manner”.

The 5G enthusiasm is not limited to developed markets. In emerging markets, a link is made between 5G and national development goals as typified by a statement made by the Bangladeshi telecoms and IT minister, Mustafa Jabbar: “We have missed three industrial revolutions; Bangladesh should be established as a leading country in the fourth industrial revolution. The whole world will enter into the era of 5G in 2020. The country will not be allowed to stay behind from this.” (Speech at Junior Chamber International, 19 May 2018)

This all sounds wonderful, but there is a gap between the political rhetoric and telecoms regulatory action to achieve mobile broadband and 5G policy objectives. Furthermore, since the 2018 Mobile World Congress, mobile operators and equipment vendors have started to sound rather more cautious about the business case for 5G. Without a change in government policy on spectrum availability, spectrum pricing and easing network deployment, in many countries mobile operators will not be in a position to deliver the lofty announcements made by politicians.

INVESTMENT IN MOBILE BROADBAND AND 5G
To cater for mobile broadband traffic, mobile operators are continuing to invest large sums in 4G (LTE) radio access networks and backhaul infrastructure. Some advanced markets are already past the 4G investment peak but in many emerging markets 4G deployment capex is still increasing. But there are some markets where operators have pulled back investment, often due to a cashflow squeeze caused by high spectrum fees and other regulatory fees.
Several operators have started to deploy massive MIMO (multiple-input, multiple-output) in combination with three-carrier aggregation, thus delivering gigabit speeds, and most 4G radio access network (RAN) investment currently taking place is software upgradable to 5G. In other words, investment in 5G is already underway. However, the transition to 5G requires further significant infrastructure investment. Deutsche Telekom CEO, Timotheus Höttges, estimated the cost of providing 5G networks in Europe at €300-500 billion and Sprint’s CEO Marcelo Claure stated at this year’s Mobile World Congress that in the US, operators will invest $275 billion in their networks. On top of the huge network capex, operators need to acquire new spectrum below 1 GHz, in 2 GHz to 4 GHz, and in millimetre wave bands.

A 5G mobile network is also different from a traditional mobile network, which has relatively large cell sites. A 5G network looks much more like a fixed network with many small cell radio tails. The deployment of many thousands of small cells, for example on street furniture, requires an unprecedented investment in fibre and will push up network operating costs. Estimates as to the number of small cells required vary greatly, but over the next 10 years the number of outdoor cell sites in networks in advanced markets may increase by a factor of three – and more if indoor solutions such as Ericsson’s Radio Dot system are included.

These thousands of new cell sites must be connected by fibre. A calculation by the Fiber Broadband Association of the US illustrates the size of the required investment: in an urban environment it will take 8 miles of fibre cable per square mile to connect small cells. The largest 25 metro areas in the US cover 173,852 square miles, which means that to provide 5G coverage will require around 1.4 million miles of fibre cable. Validating this analysis, in April 2017 Verizon stated that it will purchase from Corning up to 20 million kilometres of optical fibre each year from 2018 to 2020, with a minimum purchase commitment of $1.05 billion.

This illustrates how the mobile networks will start to look much more like fixed networks in terms of the extent of fibre deployment and the number of end-points.

**OPEX COST CHALLENGES AND FLAT REVENUE**

So it is clear that mobile operators will need to invest huge sums into mobile broadband, be it 4G or 5G. For capex to take place there needs to be a return on investment (ROI). The ROI will come from cashflows generated by operations – in simple terms the difference between revenue and operating costs. Looking at the cost side (opex), operators will find savings as they move to virtualised networks and increase infrastructure sharing. However, operating a mobile network with a factor increase in the number of cell sites presents a network operating cost challenge.

But are there additional revenues to be had from mobile broadband? Mark Allera, CEO consumer, BT Group, commented in March 2018: “We will have to assume that consumers and businesses will be prepared to pay a little bit more for faster, higher quality access to the internet ….. getting some sort premium out of 5G as we did for 4G.” In other words there is little or no revenue upside from enhanced mobile broadband (known as eMBB) which will account for the vast majority of 5G traffic.

While mobile broadband revenues are unlikely to show much of an increase, during the next 6 years the monthly traffic per smartphone user will increase by a factor of 6 to 7. Ericsson’s Mobility Report provides insight. In North America traffic per smartphone is forecast to increase from 7.1 GB a month by the end of 2017 to 48 GB by the end of 2023. For Western Europe, traffic is estimated to grow from 4.1 GB to 28 GB and even in India data traffic may reach 18 GB in 2023.

Of course, 5G is a technology platform which opens up opportunities beyond enhanced mobile broadband, including serving “verticals” – smart cities, autonomous vehicles and robotics. Connectivity is the glue of the fourth industrial revolution. The amount of data generated by millions of sensors and other devices opens up opportunities in the application of artificial intelligence services. However, this is where the business case becomes uncertain. It is doubtful that big investments will be driven by business cases with a highly uncertain revenue potential.

While the IoT market is promising, connectivity revenue may only add around 5% to revenue, although the 5G IoT opportunity is greater if systems integration and platform revenue are added. Among operators striving to capture a slice of that revenue, three telecoms operators stand out as having a good systems integration business – Deutsche Telekom, Turkcell and Verizon. However, many operators will struggle to extract value from IoT unless they partner with other companies.

There are also some consumer market IoT revenues to be had. For example, in Germany T-Mobile offers a smart home package for €9.99 a month, but to attract customers the required hardware such as sensors is either given away with the package or heavily discounted.
CAPACITY FOR eMBB LIKELY TO BE THE KEY USE CASE

As we can see, users get vastly better value for money in terms of $ per GB of traffic. This is simply the continuation of a by now familiar trend in digital services and products to offer ever better capabilities while the cost of ownership to users does not increase. How can the mobile industry deliver the capacity to cater for the vast increase in traffic while at the same time not seeing much of a revenue increase? The answer is the combination of 5G technology with more spectrum.

Let’s look first at technology. New technology is spectrally more efficient, i.e. it allows mobile operators to create more mobile capacity per hertz of spectrum. In an urban environment, depending on the frequency band, 4G is roughly 2.75 times spectrally more efficient than 3G, and 5G New Radio (the radio interface for 5G) has spectral efficiency up to 6 times higher than 4G if the effects of massive MIMO are included.

The other essential ingredient is the quantum of spectrum available to mobile operators. In principle, the more spectrum an operator can deploy on existing sites the lower the cost of capacity. Depending on the country, today mobile operators have around 600 MHz of spectrum deployed between them. For example, in most European countries mobile operators use spectrum in the range of 800 MHz to 2.6 GHz. We are now witnessing the assignment of 2x30 MHz of 700 MHz spectrum, 400 MHz in 3.4–3.8 GHz, as well as spectrum in 1500 MHz and 2300 MHz. In the US operators have already acquired millimetre wave spectrum in 28 GHz and 39 GHz through secondary market transactions and the FCC announced auctions for spectrum in 28 GHz and 24 GHz. In Europe, post-2020 the assignment of millimetre waveband spectrum will commence, starting with Europe, post-2020 the assignment of millimetre waveband spectrum will commence, starting with

The combination of 5G New Radio and additional spectrum will make it possible to serve high traffic densities in urban areas. The ITU’s 5G design calls for the ability to serve 10 Mbps per square metre. Therefore the 5G business case may be mainly about catering for high traffic densities rather than any new business model; at least, this is the conclusion Ericsson appears to have come to. In February 2018, Fredrik Jejdling, Ericsson’s head of networks said: “We also see an enhanced mobile broadband case that may not have been considered before and could become the first use-case for 5G. If we model traffic in our existing mobile broadband networks, we think that by 2023 we’re going to see an 8x increase, and probably the best way to cost-efficiently handle that is by introducing 5G over time. We need to build networks that can deliver 8-10x lower cost per gigabyte. Evolving 4G into 5G makes sense, from a cost efficiency perspective, as traffic grows.”

THE COST OF SPECTRUM WILL WEIGH MORE HEAVILY ON INVESTMENT DECISIONS

As explained above, additional spectrum is an essential ingredient in the development of 5G. In Europe and elsewhere the near-term focus of assigning spectrum for 5G is on the 3.4–3.8 GHz band, also referred to as C-band. In its status report of February 2018, the Small Cell Forum notes: “C-Band spectrum will be the first midband spectrum to be allocated for 5G in many regions, and will be heavily used for small cells, sometimes as a separate layer to accompany an LTE coverage layer; sometimes in the same layer as 5G macro and mini-macrocells within a midband.” The 3 GHz spectrum substantially increases the amount of spectrum used by mobile operators. If operators in Europe start to use the 400 MHz in the range 3.4–3.8 GHz for mobile, this will increase their spectrum holdings from around 600 MHz to 1,000 MHz. This increase of 66% in spectrum used by the mobile industry comes against a background of stagnant revenues and network operating cost pressure. The cost of spectrum is therefore a critical issue in rolling out 5G.

There are already some benchmarks from recent auctions for 3 GHz spectrum in Europe. In Ireland, operators paid on average 0.041 $ per MHz per head of population ($/MHz/pop) and in the UK 0.167 $/MHz/pop. While in terms of $/MHz/pop, prices for 3 GHz spectrum seem low, given that the band consists of 400 MHz the investment in spectrum assets for 5G means significant sums are extracted from the mobile industry. In many markets the entire band is not immediately available and hence the cash outflow for spectrum occurs over time, but it also means operators will not have the full 100 MHz band required for efficient 5G deployment.

Spectrum acquisitions appear in operators’ accounts as “intangible” capex and of course the 5G deployment (tangible capex) has to be added to arrive at the total investment in rolling out 5G. Consequently, operators now question the logic of the desire by politicians for their countries to take a lead in 5G while at the same time extracting cash from the mobile industry. At the Deutsche Telekom shareholder meeting on 17 May 2018, CEO Timotheus Höttges summed up the situation: “5G, the next-generation network, is on the horizon, and it will truly bring the internet of things to life. For this reason, 5G is of strategic importance to an industrialised nation like Germany. The spectrum auction in Germany is due to start soon. We appeal to you to take the long view. We can only spend each euro once: either on spectrum or on network build-out. My suggestion would be on build-out.”
EXTRACTING CASH FOR SPECTRUM DOES NOT HELP THE 5G BUSINESS CASE

Germany, along with countries such as Sweden, has a history of setting low reserve prices in spectrum auctions. Others take a different view. In many markets the pattern of high reserve prices observed in previous spectrum auctions continues even in the light of a shaky business case for 5G.

Italy has a history of setting high reserve prices for spectrum and is repeating this in the spectrum assignments aimed at 5G. To the Italian government, the most important aspect in assigning 3 GHz and other so-called 5G pioneer bands appears to be how much money can be raised from the sale of spectrum rights. In a press release of 23 May 2018, AGCOM, the Italian regulator, announced: “The state expects an income from the awarding bid of at least 2.5 billion euros, half of which this year” – before even mentioning the benefits of the spectrum for 5G.

In Italy, the reserve price for 200 MHz of spectrum in 3.6-3.8 GHz has been set at €426 million which equates to 0.036 €/MHz/pop (0.040 US$/MHz/pop). This is the same as the price paid in Ireland for 3 GHz spectrum in 2017. In contrast, in Ireland the reserve price in terms of €/MHz/pop was 90% lower than in Italy. To make matters worse, in Italy the reserve for 700 MHz spectrum, the likely 5G coverage band, has been set at 0.59 €/MHz/pop which is around three times higher than prices actually paid for 700 MHz spectrum in auctions in Finland and Germany.

As a result, Italy is currently not alone in what appears to be conflicting policies. The UK extracted £1.4 billion from auctioning 150 MHz of 3 GHz spectrum and 40 MHz of 2300 MHz spectrum. And yet in a press release on 10 March 2018, the British government congratulated itself for its commitment to 5G by announcing, “On the first anniversary of its digital strategy, the government has today announced the winners of a £25 million competition to pave the way for a future rollout of 5G technology in the UK” and says this “highlights progress to date on its strategy to create a digital economy fit for the future”. But £25 million is only 1.8% of the cash extracted from the UK mobile industry for 5G suitable spectrum.

PRESSURE TO RAISE REVENUES

In middle and low income countries where government revenues are thinner the pressure to raise cash from spectrum auctions is enormous. In many emerging markets development of mobile broadband is hindered by pricing spectrum beyond the levels where a business case for 4G use is justified let alone for 5G.

A recent example from February 2018 is the spectrum auction in Bangladesh where 66% of spectrum on offer remained unsold and this despite the fact that the industry is woefully short of it. Yet, shortly after the auction, the telecoms and IT minister, Mustafa Jabbar, said: “The world will embrace 5G in 2020. So, we too will have to accept new technology and must move on to 5G. There is no option for procrastination.” The reality is that Bangladesh only introduced 4G after the February 2018 spectrum auction, making it the last country in Asia to do so.

Policymakers need to understand that mobile telecoms operators will allocate investment where there is a business case. Why would anyone invest if a better return on investment can be found in other markets? Increasingly, governments are facing a situation where they are in effect in competition with other jurisdictions for the allocation of capital by multinational mobile operators such as Vodafone, Orange, Telefonica and Deutsche Telekom, as well as regionally focused operators such as MTN, Millicom, Ooredoo, Axiata and VEON.

The demand from shareholders for regular dividends means that these operators have a finite amount of cash to invest. The boards of these companies need to decide how best to allocate cash across their portfolio of markets in order to achieve the highest level of ROI, as illustrated by the statement from Catherine Bohill, director of spectrum at Telefonica:

“Assignment conditions must allow operators the breathing room to innovate and invest. In those countries that have long licence terms and reasonable conditions, operators have lower risk and are more likely to invest. Portfolio trade-offs do exist and where spectrum assignment conditions are unrealistic, operators will endeavour to convey these shortcomings to the relevant authorities but ultimately may have to abstain from

[Tables and diagrams are not transcribed in this plain text format]
processes that place scarce capital at risk. This is a very unsatisfactory outcome and must be avoided. It is, however, an ever increasing phenomenon with high profile cases happening across the world.*

When cash is limited, that cash will be invested in the markets that offer the highest return. To attract the investment in mobile broadband and 5G to achieve connectivity policy goals, governments must adjust the cost of spectrum to a sustainable level in the context of their own market.

THE ECONOMICS OF 5G DEPLOYMENT ARE AFFECTED AT MUNICIPAL LEVEL

There is also a more local aspect to 5G investment. Given the imperative to deploy many small cells in cities, operators will prioritise investment in cities where it can be done quickly at a cost that makes business sense. Therefore, not only is there competition for investment between countries, but with 5G we are also seeing the emergence of competition for investment between cities within a country. The status update from the Small Cell Forum in February 2018 showed results from a survey among 78 mobile operators on the barriers to small cell deployment. Asked what are the top three barriers, total cost of ownership (TCO) or ROI was mentioned by 58%, site cost and availability by 47%, and site approvals by 23%

At the ministerial programme of the 2018 Mobile World Congress, Nicki Palmer, chief network officer for Verizon Wireless, pointed out that there is a great deal of divergence in how municipalities in the US support the deployment of small cells with access to municipal infrastructure such as lampposts and street furniture. Some cities look at granting access to municipal infrastructure as a way to maximise revenue. Others see it as an opportunity to encourage mobile operators to invest and place their city at the forefront of smart city development.

Operators are also concerned about getting approvals for site installations. While it may have been appropriate to go through a full planning application procedure for relatively large macro sites, applying the same procedures to several thousands of small cells would cause delays and add to costs. Given their small size, the environmental impact of small cells is minimal.

In the US this issue was recognised some time ago. Former FCC Chairman Thomas Wheeler stated in his speech before the Competitive Carriers Association in Seattle in September 2016:

“Estimates are that 5G will require a 10x growth in cell sites, and potentially significantly more. ... Which raises a key question: how can we work with siting authorities to allow the plethora of antennas that will be required quickly and at a reasonable cost? ... the nature of the technology makes the review and approval by community siting authorities, and the associated costs and fees, all the more critical. There are just over 200,000 cell towers in the US, but there may be millions of small cell sites in the 5G future. If siting for a small cell takes as long and costs as much as siting for a cell tower, few communities will ever have the benefits of 5G.”

In Europe, the site permitting issue is dealt with in the new European Electronic Communications Code where Article 56 addresses small cells and directs that permits should not be needed for cells below a certain threshold, yet to be defined. The code also addresses obstacles to fibre deployment. In June 2018, Virgin Media announced that it is taking a county council in England, Durham, to court over unreasonably high land access charges for fibre routes. Tom Mockridge, CEO of Virgin Media stated: “By demanding money for land access Durham County Council is now putting up a broadband blockade to thousands of homes and businesses across the county.” Let’s see whether the code helps to support Virgin’s case.

REGULATORY LEVERS TO ENCOURAGE 5G DEVELOPMENT

As summarised in the figure above, governments and regulators at national level and cities and municipalities at local level can pull levers to encourage investment in mobile broadband and 5G. When a government seeks to attract investment into their country or cities, for example a manufacturing facility or start-ups, they usually provide incentives. With mobile operations it seems to be other way around. Investment is taxed in the form of up-front spectrum fees or in some countries technology neutrality fees and site build restrictions hinder network deployment. It is not sufficient for governments to say wonderful things about mobile broadband and 5G. To tilt the finely balanced 5G market governments must use the levers at their disposal to achieve this.

For central government this means setting sustainable reserve prices for spectrum and releasing spectrum as soon as possible. In this context creating artificial scarcity is the worst decision governments can make. For municipalities this means cost-based access to lampposts and other municipal infrastructure and ensuring small cell deployment, below a certain size, is treated as permitted development, i.e. with no need for planning permission.

**STEFAN ZEHLE** is CEO of Coleago Consulting, which provides expertise in spectrum, network optimisation, network sharing, telecoms regulation and interconnect. Email stefan.zehle@coleago.com and visit coleago.com

www.iicom.org
Africa's new digital services sector is creating commercial, legal and regulatory challenges. Mobile operators in Sub-Saharan Africa are recasting their traditional business models to take on the new competition. But African governments and regulators – like their global counterparts – seem to be responding in contrasting ways, as I describe in this article.

**MARKET SIZE**
The digital services sector in Sub-Saharan Africa is growing but is less visible than its telecoms and internet counterparts. For example, Jumia, an e-commerce player in 23 countries, has 4.2 million customers for its ecommerce business. MTN, the operator, has a mobile games business that turns over $100 million. In the mobile money field, there are an estimated 2 million plus mobile money agents.

While there is considerable excitement about some of the African start-ups involved in the new digital services sector, it tends not to be seen as a new and vital area of business activity. However, the companies involved in it – whether African or international – are beginning to attract investment into the continent. The sums may be smaller than those invested in telecoms infrastructure but they do bring investment and jobs. Mobile news platform Opera announced at the beginning of the year that it will invest $100 million to develop its African services.1 Over $25 million has been invested in iROKOtv. A third of all venture capital invested in African start-ups in 2017 – $65 million – was invested in fintech services.2

There is even infrastructure investment from the over the top (OTT) providers: after creating two metronets (in Uganda and Ghana), Google and its partners have committed $100 million to develop infrastructure. Facebook has partnered with Airtel and BCS to lay 800 km of fibre in north west Uganda.

**VOICE AND DATA UNDER THREAT**
The foundations of the old mobile business model – voice revenues – are under threat and data produces low margins and requires higher levels of capital investment. Until recently, mobile operators in Africa have struggled to produce internally consistent business strategies that explain how they will dig themselves out of this hole.

It has also meant that the OTT players have been blamed by the mobile operators and many regulators for creating this set of circumstances by slowly bleeding away voice revenues through data voice apps like WhatsApp, Skype and Viber, as I wrote in Intermedia in 2017.3

However, voice is only part of the digital services economy and there are wider and more profound consequences. In a talk at the Apps Africa Innovation Awards in November last year, Herman Singh, MTN’s chief digital officer, explained that users used to go on their phones and mostly use telecoms-provided services. Now they use only 20%
of services (and falling) that are telecoms-provided and are going elsewhere on their phone to get what they want. “Voice, data and text will decline. Do we just hand over to the OTTs? We need to become OTTs ourselves. The opportunities in the space are awesome.”

So at the heart of MTN’s fight-back against OTT is copying the business strategy of the OTT players: “The trick is building a platform that will gain user attention and revenues. Also, like Safaricom and the M-Pesa money platform, it wants to build the volume of financial transactions on its platform and in doing so build a significant revenue stream from servicing these transactions. Part of this will be done through building partnerships with digital content providers; TV services are a simple way to monetise networks, it says. It has also invested in Bizao, which facilitates easier access to application programming interfaces (APIs) for both mobile companies and digital services operators.”

On the increased capex for new data networks that is needed to achieve all this, Orange says: “Globally, Africa is the continent that needs most [infrastructure]. We are interested in both passive and active infrastructure sharing and will accelerate discussions with partners. We want to build a stronger agenda in this area.”

Vodacom – the third of the large African operators – is also taking a leaf out of the OTT operators’ playbook. According to Zunaid Mahomed, digital and fixed services officer: “We have embraced a version of our digital service operating model where we are able to provide services, not just to traditional Vodacom telco service customers, but to all customers. Most of our Vodacom-branded digital service portfolio is available to all digital audiences. While the service is telco agnostic, there will be instances where Vodacom SIM users get a better experience.” This same “Anyone-can-use-it”, platform agnostic approach is also echoed in the music streaming platform of Safaricom, Songa, which is Vodafone-owned.

It is focusing on Vodacom branded services (like Vodacom Soccer, All Out Rugby) and in some instances working with existing brands like Deezer: “This is dependent on where we are able to scale, where partners have a real advantage as well as our ability to link our network, which creates the unique ability to reach new audiences (e.g. our VideoPlay service provides a network award download feature to download videos when there is spare capacity). It’s a partner model that means we don’t necessarily want to own content or services.”

Again there is a strong emphasis on video (“with users and usage growing significantly on a monthly basis”); music (growing but hard to get paying subscribers); and games (a dedicated portal and free data promotions). Also, like MTN, it is investing in harvesting more advertising revenues from having large numbers of users on its platforms.

So, the growth of digital services is upending previously solid industry sectors. In early 2017, Senegalese mobile money transaction company Wari announced it wanted to buy the Senegalese subsidiary of Millicom, branded as Tigo. The matter is currently in arbitration, but as CEO Kabirou Mbodje told me at the Afrobytes meeting in Paris: “It could be another telco (if we don’t get Tigo). We’ve acquired a bank and we need to become almost bank-like again.”

The changes in Africa mobile operator business strategy are summarised in the table.

These business strategies mean that some operators have shifted from being strategically opposed to the OTT players to a much more tactical opposition. In the past some of them seemed to believe that if they could only resist the incursion of data-enabled services (particularly for voice), things would return to the way they were before. But you can hardly claim that you want OTT voice services completely closed down in a particular country if you are seeking to use OTT approaches in other business areas to develop your own revenues. Indeed, in the case of Orange, its venture capital company Orange Digital Ventures has announced that it will partner with
Google on investment. The futures of mobile and OTT operators are increasingly becoming intertwined and co-dependent.

While it must be reassuring to those who run these mobile operators to have a digital strategy, the central regulatory problem raised by OTT operators remains. The major OTT platforms have benefited from network effects: the more people are on Facebook, the more people will want to join (which in turn attracts more people to the platform. There is a tendency common to several of the major digital platforms where size leads to monopoly. So, what happens in regulatory terms if in the long term Jumia One becomes the equivalent of Facebook for Sub-Saharan Africa? However, in the short-term the more pressing regulatory issue is the collapse of telecoms and internet competition in many African markets: there is a steady shrinkage in the number of mobile operators with only the larger operators in a number one or two market position continuing to make profits.

The example of Uganda’s bankrupt former incumbent UTL illustrates the depth of the problem. Formerly owned by Libyan investment vehicle Lap Green, the ministry of finance has a cabinet-approved package of incentives for potential buyers that include a 20 year licence extension (against network investment); being the preferred provider of internet services to all ministries, departments and agencies of government (at lower than current prices); giving it more spectrum (against coverage targets); and unlimited access to and use of the national backbone infrastructure (and to increase government’s shareholding to between 32-45%).

The requirement for this kind of package of anti-competitive incentives to sell UTL illustrates how the market is undergoing some fundamental changes that are not encouraging competition. Even some of the more ambitious internet service provider (ISP) challengers (like Afrimax) have faltered and fallen in this changing business climate.

**REGULATORY RESPONSE**

Faced with these dual pressures of rising digital platform monopolies and collapsing competition, African regulators have been slow to respond but the first wave of policy development is now becoming visible. Some of these policy or regulatory initiatives seem to be chasing the wrong issues, while others seem to have grasped that the loss of voice revenues might be outweighed by the growth of the new digital services sector in the longer-term.

The Council of African Regulators (CAR) which has been working on these issues under the Smart Africa initiative, has outlined three broad approaches to tackling issues raised by OTTs:

- Blocking international OTT services, as China has done
- Bundling and partnering (e.g. Free Basics with Facebook where the operator gets data revenues)
- Operators developing their own OTT services, exemplified by the mobile operator digital strategies described above.

CAR notes the following issues that have not been addressed in regulatory terms in relation to OTT:

- Lack of protection of personal data
- Lack of ability to identify the entity responsible for quality of service
- Impossibility for states to identify users without referring to OTT players that may or may not communicate the requested information
- Lack of knowledge of personal data use rules
- Lack of a protection framework for vulnerable people (children, disabled, women, etc.)
- Inability to make emergency calls
- Difficulty in enforcing security injunctions, especially for listening (tapping) and traceability
- Impossibility of determining a tax base or levying royalties.

A presentation of the report earlier in 2018 said CAR should recommend the way forward on the best approach for Africa to reduce the negative impact of OTT and increase revenues of the telecoms sector. But some African (and indeed global) telecoms regulators seem obsessed with chasing voice revenues for an industry that has fundamentally changed and show no awareness of how to encourage the nascent African digital services industry that will grow and replace some of those lost revenues.

Unlike the more progressive regulators at the beginning of the mobile revolution that encouraged investment and competition, some of Africa’s regulators and governments seem not to have realised that the digital services sector will be a big growth area over the next 5–10 years. The result is that the former emphasis on a “level playing field” means the incentive to invest and ensure competition seems to be missing. Whatever its formal rhetoric, some policy and regulation seems more concerned with controlling and taxing than in providing incentives for this burgeoning new sector. This is particularly true of efforts to tax incoming calls to the continent through single gateways. A number of African countries have implemented taxes on incoming international calls, which has driven the transition to digital voice services such as Skype, Viber and WhatsApp.

**RETROGRESSIVE STEPS**

Two examples of this more retrogressive regulation come from Uganda and Tanzania and illustrate the kind of regulation that will hold back the digital sector. The Ugandan parliament has imposed a 200 Ugandan Shilling (0.5 US cents) daily tax on people using social media platforms such as Facebook, WhatsApp, Viber and Twitter. The law was meant to come into effect on 1 July 2018 but it is unclear how it will be implemented. In addition the new Excise Duty (Amendment) Bill will impose among other things a 1% tax on the total value of mobile money transactions.

Access to social media platforms was shut during the presidential election in 2016 and President Museveni said it was done to “stop spreading lies”.

"Some seem not to have realised that the digital services sector will be a big growth area."
According to a BBC report, Museveni pushed for the social media law in March 2018. He wrote a letter to finance minister Matia Kasaija insisting that the revenue collected by the social media tax would help the country “cope with consequences of oligambo [gossiping].”

A second explanation came from state minister for finance, David Bahati, who told parliament that the tax increases were needed to help Uganda pay off its growing national debt. A third explanation was offered by minister of ICT and national guidance, Frank Tumwebaze, who said it is a measure aimed at discouraging consumption of external content and promoting local content. He said that contrary to what was being said, the president’s proposal was long overdue and would not affect the internet or information access as insinuated by some.

“WhatsApp and Facebook are external products. Ugandans who are gladly using it are only consumers and are indirectly making the developers of these applications very rich. These applications are more of a luxury than a need, so we are going to be taxing your consumption of the application,” Tumwebaze said.10 He clearly does not are going to be taxing your consumption of the consumers and are indirectly making the Ugandans who are gladly using it are only information access as insinuated by some.

“A third explanation was growing national debt. A third explanation was tax increases were needed to help Uganda pay off its finance, David Bahati, who told parliament that the tax increases were needed to help Uganda pay off its growing national debt. A third explanation was offered by minister of ICT and national guidance, Frank Tumwebaze, who said it is a measure aimed at discouraging consumption of external content and promoting local content. He said that contrary to what was being said, the president’s proposal was long overdue and would not affect the internet or information access as insinuated by some.

“WhatsApp and Facebook are external products. Ugandans who are gladly using it are only consumers and are indirectly making the developers of these applications very rich. These applications are more of a luxury than a need, so we are going to be taxing your consumption of the application,” Tumwebaze said.10 He clearly does not understand that these products are now in everyday use and not luxury products: 2.6 million people use Facebook in Uganda.

He dismissed concerns it could limit people’s use of the internet. “We’re looking for money to tax increases the security of the country and extend electricity so that you people can enjoy more of social media, more often, more frequently,” he said. It is unclear how taxing people’s use of social media will increase their use as placing a charge on a previously “free at the point of delivery” service will almost inevitably lead to a decline. (There was more confusion about Uganda’s position as we went to press – Ed.)

Meanwhile in Tanzania, the Electronic and Postal Communications (Online Content) Regulations 2017, were published by the Tanzania Communications Regulatory Authority (TCRA) and came into effect during March 2018.

Against a wide range of objections, Harrison Mwakyembe, Tanzania’s minister for information, culture, arts and sports, has signed the regulations into law. The government has said that the regulation will help to put a stop to the “moral decadence” caused by social media and the internet in the country. It has also said that it sees social media as a threat to the country’s national security.

Online content publishers (blogs, podcasts, videos) will apply for a licence at a fee of 100,000 Tanzanian shillings, and pay an initial and annual licence fee of 1 million shillings. This means to run something as simple as a personal blog if you live in Tanzania, you’d have to spend an initial (approximately) $900 in licence fees. Again, payment of this level of taxes is an attempt to curb free speech that will fundamentally damage the development of Africa’s digital services sector.

PROGRESSIVE MOVES

By contrast, the government of Benin has published a progressive piece of legislation known as Code Numérique.11 Included are:

- Article 13: Open access to the internet – “Users have the right to access and disseminate the information and legal content of their choice, and to use and provide the applications, services and terminal equipment of their choice...”
- Article 15: Equality of treatment and non-discrimination – “Operators providing access to the internet treat all traffic equally and without discrimination, restriction or interference...”
- Article 19: Technology neutrality – “The principle of technological neutrality is understood as the general obligation of Legal, regulatory, institutional or other non-discrimination of technologies with regard to the services provided.”
- Consumer rights are defined in Article 25: User rights, as follows – “No operator may limit the right of the user to choose a content service provider; connect to the network any radio apparatus or electronic communications terminal equipment approved for that purpose; and to connect to an electronic communications network open to the public any internal communications network that meets the relevant standards and requirements.”
- Chapter IV tackles in some detail the personal data of users, including Article 33: “Operators and providers of online public communication services shall delete or anonymise traffic data, subject to Articles 34 to 37...” The balance of the chapter lays out the terms and conditions under which personal data may be held.

Another country with a more finely tuned sense of the future shape of the market is Nigeria. In 2016 the NCC, the regulator, published a report, “An overview of provision of over the top (OTT) services”.12 Using material drawn from reports by US and European consultancy firms, it argued that mobile operators need to innovate to meet the challenge of OTT. In terms of recommendations, it calls for a stakeholder forum “to determine if regulation is required for such services and its impact on the growth of the Nigerian telecoms industry”, including a review of guidelines on the provision of international gateway and voice over IP services and also an appropriate framework to regulate OTT players. It notes that the NCC “must ensure that it does not stifle innovation since internet penetration is still evolving, access speeds are still low and there is limited coverage of high speed broadband.”

CONCLUSION

The African digital services sector has the potential to make the lives of citizens easier; make services more accessible; allow people to take part in a conversation about what they want; increase efficiencies in the public, private and development sectors; and generate new jobs and investment. So whatever happens in regulatory terms has to ensure that these positive social and economic impacts are maximised.

African governments and regulators have a clear choice: they can either attempt to hold back the future by taxing new digital services or they can craft a response that encourages the digital services sector to play a central role in the social and economic transformation of their countries.

RUSSELL SOUTHWOOD is CEO of Balancing Act, a consultancy and research organisation specialising in telecoms, internet and media in Africa. This article expresses his personal views. See balancingact-africa.com

REFERENCES

1 Open News Clock 1 million downloads in Africa. IT News Africa, 1 February 2018. bit.ly/2vQy0gO
2 Facebook’s market share in Africa is nearly a third of all African venture funding in 2017. Quartz, 31 January 2018. bit.ly/2JQYsQK
3 BBC, 31 May 2018. bbc.in/2M1usHm
4 Another country with a more finely tuned sense of the future shape of the market is Nigeria. In 2016 the NCC, the regulator, published a report, “An overview of provision of over the top (OTT) services”.12 Using material drawn from reports by US and European consultancy firms, it argued that mobile operators need to innovate to meet the challenge of OTT. In terms of recommendations, it calls for a stakeholder forum “to determine if regulation is required for such services and its impact on the growth of the Nigerian telecoms industry”, including a review of guidelines on the provision of international gateway and voice over IP services and also an appropriate framework to regulate OTT players. It notes that the NCC “must ensure that it does not stifle innovation since internet penetration is still evolving, access speeds are still low and there is limited coverage of high speed broadband.”

5 Fintech startups took nearly a third of all African venture funding in 2017. Quartz, 31 January 2018. bit.ly/2JQYsQK
6 Africa’s social media backlash – politicians starting to find ways to control what seemed uncontrollable. Digital content Africa, 15 April 2018. bit.ly/2Kpq4no
7 BBC, 31 May 2018. bbc.in/2M1usHm
8 Fintech startups took nearly a third of all African venture funding in 2017. Quartz, 31 January 2018. bit.ly/2JQYsQK
9 Africa’s social media backlash – politicians starting to find ways to control what seemed uncontrollable. Digital content Africa, 15 April 2018. bit.ly/2Kpq4no
10 INTERMEDIA Vol 46 Issue 2 | InterMEDIA
High-profile data breaches, some involving children’s personal data, resulting from insufficient protections built into the emerging generation of smart devices, have raised urgent questions about whether children’s privacy is sufficiently valued in personal data regulation. The rapid growth in technologies and services whose business model is based on personal data collection and analysis – from social network services and personalised marketing to learning analytics, wearables and home assistants – raises yet further concerns. While it is likely that the technology industry will get better at preventing hacks, it is equally likely to get better at harnessing the value – mainly for commercial but sometimes public benefit – of the “datafication” of seemingly every dimension of people’s lives.

In Europe, the General Data Protection Regulation (GDPR) became applicable on 25 May 2018. Several years in the making, it has been designed as a concerted, holistic and unifying effort to regulate personal data at a time when data has rapidly become “the new oil” for public, private and third sector organisations. As European commissioner for justice, consumers and gender equality, Věra Jourová, put it: “Privacy is much more than just a luxury. It is a necessity.” And so, therefore, is its protection for all citizens, since “personal data protection is a fundamental right in the EU”.

Until recently, talk of the GDPR was rather esoteric, confined to deliberations among legal, regulatory and technical experts. But spring 2018 saw the public in Europe and beyond bombarded with demands to update social media privacy settings and respond to a flood of (sometimes inappropriate) email requests to re-consent to marketing and mailing lists, all the while hearing in the mass media about scandals about political microtargeting (especially based on personal data illegally collected via Facebook by Cambridge Analytica) or fights over the so-called “digital age of consent”, as contested across Europe, most notably in Ireland and France. All this has brought a heightened awareness (and uncertainty), including among many parents and children, though doubtless unequally distributed, of the new privacy regulation and, relatedly, the ways in which personal data may be used or misused.

Public awareness matters, not just because of its potential to trigger action by policymakers but because the public is a key stakeholder in the regulation of personal data. Aggregated together, public actions and choices in the digital environment have significant consequences for politics, markets, regulatory effectiveness, equity and the direction of socio-technical change.

But ordinary people’s voices are too little heard in multistakeholder deliberations, notwithstanding the legitimacy of their interests. Children’s voices are particularly absent, being rarely consulted or included in national or international deliberations, notwithstanding that they constitute a valued and valuable segment of internet users, being often pioneering in their adoption of new services and experimental in their digital practices, yet not easily incorporated into considerations of the “population” or the “public” or “users” as a generality. This is a problematic omission, because child welfare advocates believe it is crucial to take steps to ensure that children benefit from the wealth of opportunities enabled by the internet, now and in the future, without being simultaneously exploited, surveilled or “monetised”. Already there is a host of uncertainties regarding interpretation and implementation of the GDPR, with stakeholders responding in diverse and sometimes misguided ways as they seek to comply.1

As Britain’s information commissioner observed, while “the proper use of personal data can achieve..."
remarkable things”, it is not before but after 25 May that “the real journey begins”, with “a lot of work to be done along the way”.2

In this article, I identify some problematic actions, unresolved challenges and unintended consequences of the GDPR, focusing on children’s privacy. I conclude that while the new regulation is likely to improve children’s data protection insofar as children are treated like other internet users, it may make matters worse insofar as they are singled out for special treatment as children.

HOW DOES THE GDPR SET OUT TO IMPROVE THE PROTECTION OF CHILDREN’S PRIVACY?

Widely billed as a far-ranging, even radical effort to give European citizens greater control and choice over the uses of their personal data, through privacy-by-design, privacy-by-default and governance mechanisms, the whole GDPR is too complex to summarise here (see instead the guide from the UK Information Commissioner’s Office, ICO).3 Suffice to say that, as regards the information relating to identifiable persons, the legislation obliges data controllers and processors:

- To process personal data lawfully, securely and fairly, in ways that are transparent to and comprehensible by data subjects
- To collect and process data and, if they engage in profiling, to do so in ways which are limited to specific, explicit and legitimate purposes, taking account of special provisions for the treatment of “sensitive” data (e.g. political views, sexual orientation, medical records or biometric data)
- To facilitate individuals’ rights to access, rectify, erase and retrieve their personal data under specific circumstances
- To meet a host of governance requirements to ensure compliance, informed by the conduct of risk-related impact assessments.

These obligations are designed to benefit individuals and organisations alike. They will surely, therefore, benefit children also. However, the GDPR makes some additional requirements in respect of children’s data, for reasons set out in Recital 38:

“Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.”

This rationale contains much of merit, not least as it is the first time that the EU has considered children’s data as specifically worthy of protection. Yet it raises some conceptual and practical issues that should, ideally, be grounded in a stronger empirical basis than exists at present. These concern, first, children’s media literacy (what is their awareness of the risks associated with personal data processing and of their rights in this regard?), second, the harm that the regulation seeks to avoid (especially that relating to commercial profiling), and third the implied nature of family relations (parental responsibility, parental media literacy, children’s need for privacy from parents, and the readiness of families to act as assumed by the regulation).
The messy world of real families – who may lack time, share devices, have secrets or conflict with each other – fits ill with the GDPR’s implied world of conscientious parents and dutiful children. This has proved particularly fraught in relation to privacy, since it may be critical for a child’s wellbeing that their access to preventive or counselling services does not depend on parental consent; yet such a protection is only mentioned in Recital 38, and not included in an article (though in the UK’s Data Protection Act, a specific clause was added to address this).

Although (just) a recital rather than an actual article in the GDPR, Recital 38 informs the “higher threshold of protection for the processing of children’s data” specified in Article 8, which states that:

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member states may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

In a recent Media Policy Project roundtable at the London School of Economics and Political Science, it emerged that Article 8 leaves scope for interpretation, indeed confusion, regarding the requirement of parental consent.1 Also contested in the GDPR more generally are the rules on profiling children, how decisions are to be made regarding the legal basis for processing (including, crucially, when it should be based on consent), how parental consent is to be verified, and when and how risk-based impact assessments should be conducted (including how they should attend to intended or actual users). Further, it is not clear how, in practice, children can claim their rights or seek redress when their privacy is infringed unless, perhaps, the mechanisms specified in the UN Convention on the Rights of the Child (UNCRC Articles 43-54) will be made available to them in this context or, alternatively, national data protection authorities will resource specialised channels both to enhance children’s data literacy and to find solutions to problems children encounter.

CONTESTATION AND CONFUSION OVER THE “DIGITAL AGE OF CONSENT”

During 2017/18, Article 8 of the GDPR attracted considerable attention among the child rights, safety and welfare community, sometimes spilling over into the public domain, regarding children’s rights to protection and privacy online, on the one hand, but also to participation, information and expression online, on the other (all these being rights established in the UNCRC). Since a higher age of consent (if not routinely flouted) would favour protection rights and a lower age would favour participation rights, the stakeholder community has been divided in trying to determine where and how to strike the optimal balance.

Adding to the heated nature of this debate is the fact that, although the GDPR was designed to protect users’ personal data and privacy, personal data mediates not only commercial but also interpersonal interactions online and, thus, the potential harms at issue are not only commercial but also interpersonal (such as bullying, harassment, hate, grooming); hence the efforts of those on the protectionist side of the debate to raise the age at which children can use online services. Hence, too, the interest of the child safety community in whether and how it will now be the GDPR rather than safety specific regulation that, for instance, specifies the age at which children can access services, the conditions under which children can request removal of problematic content (“the right to be forgotten”) or the requirement for parental oversight (via consent mechanisms) as well as, more broadly, the requirement on platforms to conduct risk impact assessments.

This debate played out differently across European member states, resulting in all possible
ages between 13 and 16 being chosen as the “digital age of consent” (see figure, page 20). It appears that these national decisions made little reference either to research evidence regarding children’s developing media literacy during adolescence or to direct consultation with children or child advocates regarding their best interests (UNCRC Article 3), although internationally all countries apart from the US have ratified the UNCRC in which Article 12 states that the child has a right to be heard “in all matters affecting them”.

So why such different decisions about the age of consent? Do we imagine that children mature at different rates across Europe? There is little evidence for this. It seems more likely that European countries vary culturally and politically in how they weigh children’s rights to protection and participation. The result is a notable lack of harmonisation across Europe, affecting both children and businesses, along with some unresolved cross-border issues.

In the UK, a hard-fought debate over the Data Protection Bill (now, Act) in the House of Lords and a tacit government defeat resulted in an interesting compromise – namely, agreeing the age of 13 (to support teenagers’ participation rights) for Article 8 but additionally requiring an “age-appropriate design code” for online providers for all children – as is consistent with the UNCRC Article 1 definition of a “child” as all those under 18 years old. Just how privacy-by-design, itself a principle promoted by the GDPR, can be implemented by a service provider who may not know whether a user is a child or whether they are below a certain age threshold, remains to be seen.

The UK ICO will now produce and enforce a code with distinct provisions for children according to their age, to ensure that providers fulfill the GDPR’s requirements for transparency and interpretability (or legibility) of terms and conditions, use of risk impact assessments, mechanisms for the right to withdraw consent and erase data, and for support and redress. Since there is a group able to use online services without parental consent (being 13+) yet are still in need of child protection (being under 18), this places a particular responsibility on service providers (and on enforcement of the ICO’s code).

Matters should be simpler for the under 13s, insofar as both providers and parents are responsible for their internet use. But since many children use services underage (51% of UK children have a social media profile by the age of 12, despite most platforms setting a minimum age of 13), and since many providers simply require a self-declaration of age, the unintended consequence of the regulation is that under 13s may appear to providers as adults, so missing out on child- (or teen-) specific protections.

The Article 29 Data Protection Working Party says: “Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.” This raises some interesting questions about those services – including the most popular social media companies – that assume the self-declared age is valid, especially when the evidence suggests that underage users experience harm online.

During April 2018, it became apparent that much of the fuss regarding Article 8 was due to a widespread misapprehension that this specifies a “digital age of consent” relevant to children’s access to all online services, rather than only those where an information society service is being directly offered to a child and where the processing of personal data is based on consent. In other words, the prefatory phrase, “Where point (a) of Article 6(1) applies”, was widely missed. GDPR Article 6(1) states the six lawful bases for processing personal data (of which consent, point (a), is but one, with relevant others including what is necessary for the performance of a contract, point (b), and the legitimate interests of the data controller, point (f)).

Such a confusion can be traced to the two meanings of consent – first, the requirement on the data subject to consent to a service (as when ticking “I agree” to terms and conditions) and, second, the data controller’s decision to rely on consent as the lawful basis for processing personal data. This confusion will surely extend to users who are unlikely to distinguish consenting to a service to gain access to it (for instance, when signing up to Facebook) from the lawful basis on which their data is processed.

In the run up to 25 May 2018, as users were required to update their privacy settings, it became apparent that not only have different member states adopted different approaches as regards children, but so too have different providers:

- Facebook appears to be keeping the age of 13 as the minimum to use the service (as long required by COPPA – the US Children’s Online Privacy Protection Act 1998) by processing personal data on the lawful basis of contract (for adults and teenagers if permitted legally to make a contract in their country), and on the basis of legitimate interest (for teens 13+ not permitted to make a contract). Additionally, it processes sensitive data and profiles users (as defined by GDPR Article 9) on the basis of consent (thus applying EU member states’ different ages of consent for Article 8 only in relation to sensitive data and targeted advertising).
- WhatsApp (owned by Facebook but taking a different approach) announced that it would henceforth restrict its services in Europe to those aged 16+ (based on a simple self-declaration of age), thus obviating the need to collect information about age and so enabling data minimisation.
- Instagram (also owned by Facebook) began asking its users if they were 18+, stating this affects the use of their data for targeting adverts (i.e. profiling), though it also has implications for the safety provisions applied for 13-17 year olds.
- Twitter invited users (at least in the UK) to agree that they’re over 13 years of age, also removing some users believed to have been under 13 when they first signed up to the service.

The implications for children now deemed underage – in the UK, 55% of 12-15 year olds use

www.icom.org
Facebook, 43% use Instagram and 24% use WhatsApp – are only now emerging. It would be problematic if children were to be faced with the decision either to lose access to a service they value or to lie about their age to retain access (and, thereby, find themselves treated as an adult rather than benefiting from the protections due to them as a child). The position for their parents is also problematic, for they would surely wish their child could engage honestly online while in receipt of appropriate protections but, instead, are likely to find themselves complicit in various workarounds so their child can access services.

The legal implications are also unclear. For instance, whether Facebook's decision to process personal data partially on the basis of legitimate interests, itself unexpected to many, may prove unsustainable given the upcoming revision of the EU’s e-privacy directive, in which legitimate interest is currently not foreseen as a ground for tracking or profiling. Then there are the legal challenges, such as that brought by Austrian privacy activist Max Schrems11 – on the grounds that the all-or-nothing as that brought by Austrian privacy activist Max Schrems11 – on the grounds that the all-or-nothing consent required by key companies constitutes illegal “ bundling” and “ forced consent”,12 contra the consent required by key companies constitutes illegal “ bundling” and “ forced consent”,12 contra the general and privacy in particular. Here I select just the complex and changing digital environment in understanding of children's rights.13

There are many questions that have been – and should yet be – researched regarding the views and understandings of children and parents as regards the complex and changing digital environment in general and privacy in particular. Here I select just two indicative sources of evidence regarding children's developing competence, both of which suggest the inadequacy of a regulatory approach that seeks to protect children’s data via implementation of a rigid age threshold.

Ofcom, the UK regulator, asked a nationally representative sample of UK children to respond to the statement, “When you use Google to look for something online, you are given a list of websites in the Google results page”, and to choose from the answer options shown in the figure below, with the top green line being the “right” answer.14 The results suggest that with increasing age, children gain the commercial literacy to realise that some but not all search engine results can be trusted. However, there is no strong increase in understanding through the early teens, the main gain being among younger children.

One might conclude that 13 year olds are almost as literate as 16 year olds (it being younger internet users who lack commercial literacy). Development in understanding thereafter (ages 16-21 and, using other indicators, for older ages also) is variable, offering little evidence of a magic switch in maturity when children turn 13 (or 16) and so hardly justifying setting an age threshold as a “bright line rule”15 by which those in need of greater protection can be identified.

The Parenting for a Digital Future project asked a nationally representative sample of UK parents to answer the question, “At what age do you think your child will be or was old enough to make their own decisions about the websites or apps they use?” This is a view of their child’s “age of independence”, as they were asked to assess their child’s maturity rather than to consider the legal question of consent. The average age chosen by parents of children aged 0-17 was 13, although the most common answer (the mode) was 16. But as shown in the figure on page 23, what was more striking was that parents’ views vary greatly according to the age of their child.16

So, while parents of young children consider 13 a reasonable age, parents of teenagers take a different view, clearly thinking that they should stay involved in their children's decisions about internet use. Parents of teenagers aged 13 to 17, therefore, think that the UK government’s chosen age of consent of 13 is too young: 79% of this group think their child should be at least 14 before making decisions about whether to consent to online services, with the ideal age of consent averaging 15. Also interesting was the finding that more digitally skilled parents such as those able to create their own websites or videos and parents who have had negative online experiences also favoured an older age of consent.

**ADVANCING CHILDREN’S RIGHTS IN THE DIGITAL AGE**

In a digital age in which children’s every communication and action is tracked and recorded, it is becoming clear that privacy (UNCRC Article 16) is vital to children’s “best interests” (UNCRC Article 3) and their opportunity to develop to their full potential (Article 29). Increasingly, digital privacy mediates children’s negative rights – the avoidance...
of harm, insofar as infringements of privacy place a child at risk, and also their positive rights, “insofar as it is part and parcel of individual autonomy, a necessary precondition of participation”. With the ink not yet dry on the GDPR nor on the policies of public and private sector organisations designed to implement it, it is too soon to be sure whether children’s rights will be fulfilled or, at worst, undermined by a regulation that only partially takes account of their specific needs and circumstances.

At present, the lack of harmonisation across countries and services (itself counter to the EU’s goal of easing the regulatory burden on businesses while improving clarity and accountability for users) combined with the practical ease of circumventing protections provided for those of different ages and continued legal uncertainties over implementation, is creating an unsatisfactory regulatory context.

In the future, it is possible that the public may make different choices in managing their privacy online as they gain what we might call “data literacy”. This term has been variously defined by different disciplines18 but should now capture not only a knowledge of data processing but also a critical understanding of data flows and the data lifecycle. But data literacy, like media literacy and other literacies, always depends on legibility: people cannot “read” or understand or responsibly engage with that which is illegible.

Hence the GDPR, and the “datafication” of society more generally, is accompanied not only by insistent calls for the mainstreaming of media literacy education and awareness-raising, but also for policymakers to enhance data controllers’ public-facing mechanisms, including transparency, accountability and redress. Some of these requirements are built into the GDPR, but some must be engineered by the state, business or wider society to support, complement or enforce the implementation effectively.

As with the canary in the coal mine, children often find themselves in the vanguard of digital innovation and their problematic experiences of privacy online turn out to indicate problems also significant for the wider population. After all, it is not only children who do not read or understand terms and conditions, not only children who are prepared to trade their personal data for free services, and not only children who struggle in practice to exercise their right to protect or retrieve or delete their data.

As I argued recently, one problem with the problem of treating children as a special subgroup is that this conjures a problematic normative vision of all other users as somehow invulnerable and invincible.19 Not only is this wrong (for user vulnerabilities extend far beyond childhood) but, once provision has been made for some, further calls for special protection are likely.

In future, it may work better for data controllers to protect the rights (and limit the commercial exploitation) of all users than to try to identify children (and other vulnerable users) so as to treat them differently (not least because the very process of identifying children may undermine the principle of data minimisation which protects their privacy). Designing systems for the minority of users who are white, educated, middle-aged, able-bodied and resilient may prove unwise and expensive in the long run, as well as counter to many people’s rights.

In other words, it may be that a governance regime that treats children fairly will be one that works for everyone, and it may also prove more efficient and effective than one that addresses (some) adults’ needs first and then tacks on children’s as an afterthought.

SONIA LIVINGSTONE is a professor in the Department of Media and Communications at the London School of Economics and Political Science. She is the author of 20 books on children’s online opportunities and risks, advises on children’s rights in digital environments, directs the projects Global Kids Online and Parenting for a Digital Future, and founded the EU Kids Online research network. See www.soniaalivingstone.net

Thanks to John Carr, Jeff Chester, Stephan Dreyer, Eva Lievens and Mariya Stoilova for comments on this article.


July 2018 Vol 46 Issue 2 | InterMEDIA 23
These are tough times for digital platforms. The revelations in March 2018 that the political consultancy firm Cambridge Analytica managed to access the personal data of as many as 87 million Facebook users on the basis of an online quiz, and that this data was on-sold to third parties including Donald Trump’s 2016 US presidential election campaign, threw into sharp relief questions of trust in digital platforms. The Cambridge Analytica data breaches, carried by the Guardian based on the revelations of whistleblower Christopher Wylie, was the latest of many issues to arise for companies such as Facebook, Google, Twitter and other major social media companies over the past three years. For Facebook in particular, it marked the 15th occasion in the company’s history where its practices with regards to personal data have come into question, an issue strongly raised in Mark Zuckerberg’s two-day testimony in April before the US Congress.

Concerns about the circulation of fake news, the ability to manipulate algorithms for political campaigning, alleged privacy breaches and the misuse of personal data, online abuse and harassment of women and minorities, and alleged Russian government manipulation of the 2016 US presidential election through social media platforms, have been features of the political landscape worldwide. Collectively, they constitute part of what the Economist has termed a “global techlash” against the once-feted corporate titans of Silicon Valley.

The broader political environment has also become a more difficult one for the digital platforms. Whereas the relationship between Silicon Valley and the Obama administration was a generally positive one, and the policy glow of innovation, enterprise and start-ups saw the “disruptive” platforms being championed worldwide, there is a growing political backlash against these companies. Decisions as otherwise diverse as the EU’s decision to fine Google €2.4bn for alleged anti-competitive practices around consumer search in June 2017, the US FCC’s repeal of net neutrality rules in December 2017, the many concerns being raised about online hate speech and proposed crackdowns on fake news, and the revoking of Uber’s licence to operate ride-hailing services in London in September 2017 flag a growing preparedness on the part of governments and regulators to reassert their powers. They also mark a reassertion of the power and influence of incumbent service providers – be they US cable companies or London taxi drivers – and their preparedness to draw upon leverage points within national political systems to rein in the digital platforms.

This has fed into calls for greater regulation of these platforms, with public enquiries and parliamentary hearings now taking place in several nations. These include the European Commission’s communication on online platforms and the digital single market, the Australian Competition and Consumer Commission (ACCC)’s digital platforms inquiry that commenced in 2018, the US Senate Commerce and Judiciary Committees’ investigation into alleged Russian interference in the 2016 presidential election, and the UK House of Lords Select Committee on Communications inquiry into internet regulation.

When Google, Facebook and Twitter sent their lawyers to the US Senate Commerce and Judiciary Committee hearings in 2017, Senator Dianne Feinstein noted the failure of their CEOs to attend the hearings, and observed at the Senate Select Committee on Intelligence:

“I must say, I don’t think you get it. What we’re talking about is a cataclysmic change ... You created these platforms, and they are being misused. And you have to be the ones to do something about it – or we will.”

The US Senate Committees did secure the attendance of Facebook CEO Mark Zuckerberg to give testimony on 10–11 April 2018. Much has been made of the degree to which the 33-year-old Zuckerberg rhetorically outmanoeuvred the senators who questioned him. Writing in the New Statesman, Nicky Woolf’s story was headlined, “Man makes $4bn in two days explaining Facebook to old people”, referring to Facebook’s share market recovery as the hearings took place. It is also fair to say that the likelihood of more substantive regulatory or anti-trust action towards Facebook or
other digital platforms in the US would appear slim under the Trump administration.

But the warning signs are clear. Companies such as Facebook, Google, Apple and Amazon are now subject to the scrutiny of politicians and regulators, and the possibility of new regulations needs to be factored into their decisions. In his response to Senator Lindsey Graham, Zuckerberg acknowledged as much when observing that “the real question, as the internet becomes more important in people’s lives, is what is the right regulation, not whether there should be or not”. Graham himself later noted on his own Facebook page:

“I expect the regulatory regime for a company like Facebook will be challenging and difficult. The regulatory tools available to us today may or may not work with Facebook. It could possibly take the creation of new laws and regulations to deal with this platform. But I do believe this. Continued self-regulation is not the right answer when it comes to dealing with the abuses we have seen on Facebook.”

Other parliamentarians are making similar observations. Vince Cable, the leader of the Liberal Democrats in the UK, has called for the break-up of companies such as Google, Amazon and Facebook, arguing that we “must revive the trust-busting spirit of previous generations”, while Andrea Nahles, the new leader of Germany’s Social Democratic Party, has called for rules to govern “digital capitalism”, stating that “we don’t accept that more and more internet platforms are becoming monopolists that don’t take responsibility for society”.

THE PLATFORM-BASED INTERNET AND THE CRISIS OF TRUST

Calls for greater regulation of the internet have been around for as long as the internet itself. The Communications Decency Act, which would have made the distribution of pornography online illegal, was passed by the US Congress and signed into law by President Clinton, before being struck down by the US Supreme Court. The LICRA vs Yahoo case, where the French court found it illegal under French law for Yahoo US to auction Nazi memorabilia online, was originally heard in 2000. The Australian government’s plans to introduce mandatory internet filtering of obscene or offensive content were first mooted in 2006 before being abandoned in 2011.

Many comparable instances of state or judicial regulation of online content can be identified. Lauren Edwards observed that the idea of the internet as a pure free speech medium had been in retreat since the early 2000s, as the platformisation of the internet meant that use had come to be increasingly associated with particular search engines or communication platforms, meaning that “there is a difficult balance to be struck between allowing these private companies the right to run their own business affairs and remain profitable, and the almost-public function that [digital platform companies] now perform.”

The calls for greater regulation of digital platforms comes at the intersection of two major developments, in the digital economy and society at large. The first is the platformisation of the internet, as digital platform companies have become increasingly central to both the economy and societies more generally. Vincent Mosco has observed that, in 2016, Apple, Alphabet (Google), Microsoft, Amazon and Facebook became the world’s five largest companies by market capitalisation. It has also been estimated that 70% of web traffic is now directed by Google and Facebook, and that Google now controls nearly 90% of search advertising, Facebook almost 80% of mobile social traffic, and Amazon about 75% of e-book sales.

“Their rise is connected to the rise of platform-based companies more generally, including Airbnb, Uber and Airtasker, and questions around the lack of regulation of such platforms, which typically present themselves as enablers of interactions...”
trust attitudes towards government, business, the media and non-governmental organisations (NGOs) in 28 countries and over 15 years, has found general levels of trust in these institutions to have been declining throughout the 2010s, with the sharpest declines in liberal democracies. It has also consistently found that levels of trust among the general population in these institutions are considerably lower than those of tertiary educated people in elite occupations, who constitute 25% of those surveyed in each country.

The larger societal context for concerns about the “black box” of algorithmic content distribution and data management is the crisis of trust in social institutions, including those of the media. The Edelman Trust Barometer, which has surveyed trust attitudes towards the media, found that trust in media can be differentiated into two elements: trust in journalists, and hence in traditional media, and trust in digital platforms. In the majority of countries, there are now more people who distrust news media than trust it, with 70% of those surveyed across the 28 countries fearing the use of fake news as a form of information warfare. But there was also evidence of rising trust in journalism (59% in 2018 trusting journalists, as compared to 54% in 2017), and a decline in trust in platforms (from 53% in 2017 to 51% in 2018). This was associated with a sharp rebound in trust in the credibility of journalists, from 27% in 2017 to 39% in 2018, which was part of a more general increase in the preparedness to trust expert opinion, and to distrust “people like yourself” as sources of reliable opinion. Journalists were more trusted than digital platforms in 21 of the 28 countries surveyed.

An important element of the platformisation of the internet has been the rise in social news. The Reuters Institute for the Study of Journalism found, in its Digital News Report 2017, that the percentage of support by a minor senate party then led by Nick Xenophon for the Liberal-National coalition’s media reform legislation, passed in the latter part of 2016. Proposals for digital platform regulation can be understood as operating across four dimensions:

- Focus on state or non-state actors
- Focus on exit (enabling greater competition and transparency)
- Formal regulation or “soft law”
- National or supranational domain of application.

The likelihood of a particular path being pursued is contingent to some degree on the institutional culture and regulatory histories of nation-states. In the US, it is difficult to extend the remit of the Federal Communications Commission (FCC) beyond broadcasting to digital content in the absence of a strong Congressional will to do so, which is patently not in existence at present, so there tends to be a stronger focus on legal remedies and the role of non-state actors and grassroots campaigning for change. By contrast, the European Union has tended to take a more interventionist approach towards digital platforms, particularly in recent years.
The risks associated with misuse of platforms are potentially highly significant given their pervasiveness.

represent stakeholders to have a role in particular governance processes within the organisation. In the immediate aftermath of the Cambridge Analytica revelations, Facebook announced its participation in a joint programme with the Social Science Research Council in the US, Harvard and Stanford universities, and seven philanthropic foundations to support industry-academic collaborations, and will make data available to social science researchers via an independent, transparent, peer-review process to research the responsible use of social data. This would be an example of selective stakeholder engagement around who can access Facebook data for research purposes, and it has been criticised by other scholars in the field. See the box below for probably the best example.

EXIT AND VOICE OPTIONS

It is useful to understand the calls for greater regulation of digital platforms in terms of the framework of exit, voice and loyalty first proposed by Albert Hirschman26 and adapted by Nick Couldry.21 Arguments for exit look at market-based solutions to the power of digital platforms, such as competition measures or the promotion of alternative digital platforms. The Economist has flagged the issue of competition actions being pursued against Facebook and Google, which could lead to the structural separation of Instagram and WhatsApp from Facebook, and YouTube from Google.2 Others have advocated the development of alternative platforms.

Timothy Wu has argued that the challenge is not to “fix” Facebook, as data harvesting is too deeply embedded in its business model, but rather to promote alternatives.22 This could be an alternative social media platform that trades a modest subscription for guaranteed data protection – the example of Lyft being a competitor to Uber comes to mind – or some form of non-profit entity, with Wikipedia perhaps providing one model for a potentially more cost-effective and civically-minded social media platform. The issue is not simply one of an alternative platform, but an alternative business model that is less reliant on providing personal data as the condition for accessing free services. Ello has had some success in this regard in the US, although its user base is a small fraction of that of Facebook.

One challenge is that alternative platforms could turn out to be worse than the established platforms: leaving Twitter for Gab (the ad-free social network for those who “cherish liberty”) would seem

TRUST AND SAFETY COUNCIL

The best known example of a more formal arrangement is the Trust and Safety Council established by Twitter in 2016, which brought together 40 NGOs to advise on issues relating to online abuse, harassment, mental health, bullying, media literacy and digital citizenship. Not a lot is known about how the council interacts with Twitter about decisions that involve suspending accounts, tackling online abuse, and balancing its strongly held commitment to free speech with its reputation as a platform given a disproportionately high amount of abusive behaviour among its user base. One of the major criticisms of Twitter has been its inability to maintain a clear line as to what constitutes unacceptable behaviour on its platform, which in turn points to the limitations of a corporate self-regulatory approach that selectively includes stakeholders from the NGO sector.27
an odd move if one wants to get away from abusive behaviour and poorly argued conspiracy theories. There is also no guarantee that alternative digital platforms will be more accountable or transparent than the established ones. Companies such as Apple and Google, for instance, were once poster children for a more ethical and responsive corporate culture than those whom they challenged.

Much of the concern about digital platforms stems from the wish for something more like a partnership, where the inevitable trade-off of various forms of freely available access (to search, community, news, opinion, entertainment etc.) for personal data comes with some form of accountability, transparency and capacity to control one’s own digital rights. Writing in pre-internet times, Albert Hirschman referred to this as the demand for voice, which he defined as “any attempt at all to change, rather than to escape from, an objectionable state of affairs”. He viewed the capacity to exercise voice as essential to meaningful citizenship in democratic societies, where “it has long been an article of faith … that the proper functioning of democracy requires a maximally alert, active, and vocal public.”

Whereas debates about social media in the late 2000s and early 2010s tended to be about the capacity of social media to enable new voices to be heard in the public sphere, the contemporary debate is about the capacity to exercise voice over the digital platforms themselves, particularly around their uses of personal data. Couldry saw this as the difference between the capacity to speak, and the right to have one’s voice meaningfully responded to by powerful social institutions, with the associated need for “new ways of valuing voice, of putting voice to work within processes of social cooperation”. While there is an extensive literature on how social media has been used to make demands for voice and participation in politics, there is now a growing demand for greater transparency and accountability of digital platforms themselves.

MEDIA POLICY REGULATION

The key question in this regard is whether digital platforms should be subject to media policy regulation similar to that for established publishers and broadcasters. Historically, digital platforms have benefited from the provisions of legislation such as Section 230 of the US Communications Act 1996, which identified “safe harbor” provisions for internet service providers, and has provided legal indemnity for digital platforms in two respects. The distinction between carriage and content, which was a feature of communications policy debates in the 1990s, has meant that digital platforms have been able to evade classification as publishers or broadcasters, while still having the capacity to regulate, monitor or delete user content without losing their “safe harbor” protections. This draws on the distinction made in US law between those who provide information and content, and hence can be held liable for it, and those who distribute or carry the content of others.

Several scholars have been challenging this distinction. Tarleton Gillespie has noted that interventions to manage and curate digital platforms have continued to grow, as “social media platforms have increasingly taken on the responsibility of curating the content and policing the activity of their users; not simply to meet legal requirements, or to avoid having additional policies imposed, but also to avoid losing offended or harassed users, to placate advertisers eager to associate their brands with a healthy online community, to protect their corporate image, and to honour their own personal and institutional ethics.” Robert Picard and Victor Pickard make the point that “these firms are increasingly monitoring, regulating, and deleting content, and restricting and blocking some users, functions that are very akin to editorial choices.” They acknowledge that the issue is difficult one, as “platform responsibilities might differ from those of traditional publishers”. For example, they are expected to be open to the distribution of user-generated content to a degree that would never be expected of traditional publishers or media broadcasters.

Others have observed that “the framing of social media platforms and digital content curators purely as technology companies marginalises the increasingly prominent political and cultural dimensions of their operation, which grow more pronounced as these platforms become central gatekeepers of news and information in the contemporary media ecosystem.” It is also increasingly at odds with how they are operating in practice, as they are not only strongly engaged in the curation of content on their own sites, but also increasingly commissioning original content for their digital platforms. The discourse of companies such as Google and Facebook has been shifting over time, from insisting that they are not media companies at all – they are simply technology companies – to one where they argue that they are not traditional media companies.

If digital platforms are to be subject to media policy regulations, there are clearly implications for how those regulations are themselves constructed. Traditional forms of content regulation would be impossible to apply to a platform such as YouTube, which generates over 300 hours of original video content per second. Similarly, regulations to support particular forms of content production would work differently for subscriber-driven platforms such as Netflix and Amazon Prime to how they have worked for traditional broadcasters. Given the expectation that platforms such as Facebook and Twitter should remain open to their users to be the primary generators of content, and the difficulties in constructing a consensus around what constitutes “inappropriate content”, the point is made that “accountability and attendant punitive actions need to be exercised in measured ways to ensure that free expression is not unduly restricted… The most serious breaches of laws and norms should typically be handled through legal and regulatory mechanisms and less serious breaches through self-regulatory private mechanisms.”

CO-REGULATION AND ‘SOFT LAW’

It is in this context that the concepts of soft law and co-regulation become relevant. Co-regulation has been a feature of regulatory theory for some time, and is premised upon the notion that regulators can set the general rules and laws, and industry can oversee the operational dimensions of their application, subject to oversight from the government regulators and the parliament. It typically requires the existence of a third party between government and the regulated firms to set and enforce rules and standards, and can be advantageous when there is both a public interest in regulation but a need for government to have some distance from the process, whether due to the costs of regulation or the need for proximity in order to have ready access to relevant information.

For soft law (see box opposite for explanation) to have teeth, it requires the oversight of independent public agencies that are nonetheless trusted by the parties who are subject to such provisions. It also needs clear backing by state regulation and civil and criminal law (“hard law”) if required. The potential of
soft law is that it recognises the difficulties of simply applying existing laws and regulations designed for publishers or broadcasters to online media. It would enable digital platform companies to have a role in shaping the regulatory requirements they are subject to. It is also conceivable that provisions could be developed by government agencies working with digital platform industry stakeholders.

CONCLUSION

The days of unregulated or self-regulated digital platforms appear to be coming to an end, at least for the largest platforms. While the calls of various politicians, public interest groups, activists and others may at times appear poorly informed or self-interested, they are now continuous and rising in scale and volume, and are being articulated as public interest issues that necessitate some form of policy action. The generalised crisis of trust in public institutions identified by Edelman and others has taken a particularly sharp form for the leading digital platforms, and the platformisation of the internet has thrown into doubt claims that some form of regulation would be an unreasonable inhibition upon freedom of public expression. Simply going from public shock to public shock, with a retrospective promise to “do something”, is no longer sufficient.

It is the contention of this article that some form of co-regulatory arrangement, bound up with soft law approaches to enactment and enforcement, is the most likely direction that such regulation will take. For such arrangements to be effective, there will be a need to clarify what are those matters of concern that are most open to codification of rules, laws, elements of good practice, and areas of regulatory breach. Consumer and data protection, and competitive practices and the exercise of market power, political advertising, fake news and online hate speech are among the areas around which rules can be developed (although, in reality, there will be contention in all of these areas). Issues such as whether social media generates online filter bubbles, job losses in the traditional media industries, or whether users become addicted to digital platforms, are not so readily addressable through co-regulatory codes.

Independent third-party oversight is critical. Digital platforms have good reason to be suspicious of regulation by governments of online content, as do their user communities. There are too many governments reacting to social and political unrest by cracking down on social media and online content. At the same time, there needs to be a regulatory authority with credibility and teeth. It is apparent from the failures of self-regulation and co-regulation in fields such as finance that the application of rules and principles will be ineffective in the absence of both ethical change on the part of regulated entities, and “a fundamental cultural change in the way business values are seen in government, by regulators, in the courts, in the community and in business itself”.26 While an independent regulator cannot itself engineer such a change, it can use the enforcement of sanctions in response to breaches of such codes as occasions in which to broadcast the requirements of ethical practice in online spaces.

With regards to media policy, the implications of the rise of digital platforms to a position of dominance in media industries and the platformisation of the internet are two-fold. On the one hand, they point to the need for fundamental reform of media laws to recognise that the 21st century digital environments differ profoundly from those of mass broadcast media. At the very least, they imply the need to move beyond industry-based silos that focus on the platform of delivery, rather than the underlying principles, as the basis of regulation. On the other, such laws themselves need to be future-proofed. The relative incapacity of governments to regulate digital platforms in the current context arises in part from policy decisions made in the 1990s, where the carrier/content distinction was paramount, and where digital platforms were constructed primarily as online service providers, as simply facilitators of public conversation, rather than as powerful institutional entities routinely engaged in “algorithmic governance” of digital public spaces.

TERRY FLEW is professor of media and communications in the Creative Industries Faculty at the Queensland University of Technology, Australia.

REFERENCES

3. Zananton (2017). Internet firms face a global techlash. ecos321ymph4
12. Edelman Trust Barometer. edelman.com/edelman-trust-barometer
25. van der Sluijs (2018). The concept of soft law is originally derived from international law, and refers to the use of quasi-legals, including rules, norms, guidelines, codes of practice, recommendations and codes of conduct, which are typically applied at an industry level, to enforce appropriate corporate behaviour. Jessika van der Sluijs has made the point that effective applications of soft law requires:
26. An institutional framework to be in place that creates a compulsion to cooperate among regulated entities.
27. Clearly identifiable entities that are subject to the regulatory processes.
28. An apparatus to address non-compliance and to ensure that sanctions are enforced when rules are broken.
29. Clear channels of communication of the rules, breaches, responses and evidence of compliance or redress.
The role of digital platform companies in our lives is expanding rapidly. Every day, huge numbers of us are creating and sharing content with known and unknown others on social media, booking rides, and buying goods from distant sellers in online multisided marketplaces. Behind the scenes, companies, big and small, trade on platforms offering B2B services or access to casual labour who will work from a distance. Such advances have brought huge benefits of cost, efficiency and choice.

But at the same time, warning bells are ringing. Workers may be technically self-employed yet work exclusively via one platform, and consequently find themselves reliant on policies and rating systems that they may have no influence over and no means of recourse against. Consumers rely on platforms for effective exercise of their rights, which may prove hard to enforce when the seller is a small producer on the other side of the world. Such advances have brought huge benefits of cost, efficiency and choice.

But at the same time, warning bells are ringing. Workers may be technically self-employed yet work exclusively via one platform, and consequently find themselves reliant on policies and rating systems that they may have no influence over and no means of recourse against. Consumers rely on platforms for effective exercise of their rights, which may prove hard to enforce when the seller is a small producer on the other side of the world. More dramatically, we read about pop-up brothels abusing the new market for ultra-short-term lets, and extremist groups using video-sharing platforms as tools of radicalisation.

In each of these cases, it is easy to believe that the root problem is our embrace of the “platform society”. It has become fashionable to see this as little more than a fancy name for technologically enabled systems whose primary innovation is their capacity for bypassing regulation while generating economic rents. But this is to ignore the significant benefits of platforms in unlocking latent supply and demand, removing barriers to trade, opening markets and driving innovation.

The question is what kind of regulation, if any, can address growing concerns about platform impacts while preserving their benefits. There seems to be a developing political consensus, at least in the EU, US and UK, that these benefits should not be won at the expense of citizen, worker or consumer rights. Legal cases are being fought which challenge the freedom of platforms to offer services without taking sufficiently responsible steps to protect longstanding rights. Notably, legislators are moving to enact laws which might remove some of the legal protections that online service providers have thus far relied upon to avoid liability. Regulation seems inevitable – but how, and to what end?

This trend is nowhere more visible than in the domain of social media. After a tumultuous year in which Google, Facebook, Twitter and YouTube have suffered public failures on issues such as fake news, political manipulation and data protection lapses, even Tim Berners-Lee was moved to comment. In his 2018 letter marking the birth date of the web he

A POLICY PLAYBOOK FOR PLATFORMS

In the second article on platforms in this issue, VICKI NASH and MARK BUNTING take a practical look at the role for policymakers in more effective oversight
protested the ability of “a few dominant platforms... to control which ideas and opinions are seen and shared”. He called on internet users to imagine an improved digital economy where the incentives of the tech sector are better aligned to fit those of their users, and society as a whole. This may be a worthy challenge, but what exactly might it entail? And is it possible?

One of the most obvious problems is that, as many scholars have noted, there isn’t really any such thing as “the platform society”. There’s so much variation across sectors that from a regulatory perspective little is to be gained by lumping together companies simply because they share a single core design principle, namely their role as multisided markets, connecting buyers and sellers or consumers and advertisers. But it is worth reminding ourselves why this fundamental feature matters. Online platforms provide a space in which third parties can connect: buyers are exposed to sellers of goods, services or labour; sellers gain immediate access to new markets; and all hope to benefit from speedy, transparent and mutually beneficial transactions.

Certainly, this core feature of platform companies goes some way to explaining why they so often seem to sidestep existing regulatory expectations; if all the platform does is to help others transact, it is not immediately obvious that they should bear responsibility for ensuring that those transactions are lawful or respecting of individual rights. Or this at least is the argument that some platform companies have made. In practice, if we think more critically about the role of platform companies in shaping the environment in which their users transact, it is clear that their role is less that of a neutral host, and more akin to a benevolent dictator, shaping the rules of engagement. Today’s digital platforms do far more than enable users to share, communicate or transact easily. At a fundamental level, they govern the types of transactions that are possible, and the terms on which they take place.

While this goes some way to explaining why the platform model can seem to enable digital companies to fall through regulatory gaps, identifying where policy interventions might be needed, and what sort might help ameliorate the situation, is less straightforward. In the case of social media, for example, companies are rarely paid by their users for the service they provide. Instead, the data trails left by users as they traverse the network can be used to create valuable profiles that enable more accurate targeting of advertisements, meaning advertisers pay a higher price than they would if adverts were merely shown at random.

This gives social media companies an incentive to keep users actively engaging with their service, which in turn may mean showing them content that holds their attention or keeps them scrolling. The departure from social objectives arises if the content that best keeps our eyeballs on a page is more likely to be harmful to others, hateful or illegal. In this context, policymakers can urge social media companies to act responsibly by regulating content but the drive towards monetising engagement will continue to pull against this, even for those companies that strive to cooperate. If it is hard to imagine which policies might effectively and consistently align platform incentives with the public good, it is equally hard to ensure that considerations of what constitutes such a good are not swayed by the interests of incumbents threatened by platform innovation.

Copyright, for example, is a policy area where vested interests still shape the regulatory agenda. The new EU digital single market directive on copyright includes proposals for both a “link tax” that is supposed to reward rights holders for content shared, and for the monitoring of content uploads to sift out copyright-infringing content. Both aspects have raised significant concerns for champions of innovation in the digital economy who argue that such measures stifle creativity and information sharing, and introduce unnecessary surveillance of user content.

Against this backdrop, it is easy to understand why policymakers are rummaging through their regulatory toolboxes. We are seeing a direct shift away from the principle embraced in the EU e-Commerce Directive, namely that information service providers are “mere conduits” enjoying immunity from liability regarding illegal online content unless notified about it, towards more proactive obligations to detect and remove illegal content before being notified. While it is hard to argue against an expectation that companies should not make money from circulating illegal content if they have the tools to identify and remove it, what we are left with is a scenario in which governments effectively pass on the responsibility for policing speech to “private sheriffs” without requiring them also to protect lawful expression.

If the UK government proceeds to make platforms directly liable for all the content they host (as it has suggested it might do), it is hard to see how this would work without either limiting opportunities for expression and participation online, or giving unaccountable private companies unprecedented powers over information and speech. Indeed, with the introduction of measures such as Germany’s Network Enforcement Act we already see governments measuring companies’ success in removing content not by assessing the accuracy of their decisions, but the speed with which they act. It is not hard to imagine the incentive this metric creates.

A DIFFERENT KIND OF POLICYMAKING

Good policy responses must get to grips with three profoundly disruptive effects of platforms on law and regulation.

First, they raise a new kind of problem. Much existing regulation responds to problems of...
The protracted debate about intermediaries’ policies and processes, and no about technological capabilities, little visibility of technology firms, based on unproven assumptions. But often, the risk is law that is the opposite of platforms without clear mandates or accountability. Delegates legal and regulatory decision-making to sufficiently represented.

And a need to ensure all stakeholders’ interests are maximise benefits and anticipate rapid changes. Issues are often counter-productive. Law needs to be rethought alongside code, reconciling private market governance with public policy. Dialogue is called for between policymakers and platforms to increase mutual understanding, maximise benefits and anticipate challenges.

We are moving from an era of command-and-control regulation to one characterised by co-governance, forums for collaborative rule-making, and a need to ensure all stakeholders’ interests are sufficiently represented. In this world, we need to avoid vague law that delegates legal and regulatory decision-making to platforms without clear mandates or accountability. But often, the risk is law that is the opposite of careful: that throws problems over the wall to technology firms, based on unproven assumptions about technological capabilities, little visibility of intermediaries’ policies and processes, and no systematic approach to oversight, impact assessment and review. The protracted debate about the EU Copyright Directive provides an example; in the row about whether to require upload monitoring, it has lost sight of the bigger picture, which is the need for platforms to strike a fair and reasonable balance between different fundamental rights, and for regulators to ensure effective oversight of how they do that.

**NEW FORUMS, NEW REQUIREMENTS**

There have been two kinds of response to these challenges. The first is the proliferation of “multistakeholder initiatives” to tackle policy objectives online. These cover everything from extremist content online⁷ to the development of artificial intelligence for social good.⁸ They are usually nominally voluntary, although they often form under intense pressure from policymakers.

One of the earliest enduring examples is the Internet Watch Foundation. Its chair, Andrew Puddephatt, has produced a checklist of success factors: good multistakeholder models have a clear remit, a precise definition of the problem or opportunity to be addressed, and a shared goal: independent governance; the ability to make binding decisions about content or sources to be blocked or promoted; and transparency about performance relative to goals.¹¹

One advantage of the multistakeholder approach is the ability to take a global approach to global problems. But equally, this can cause problems where differences in legal frameworks and social expectations exist between jurisdictions. And these initiatives can be slow and wasteful; indeed, they can be used by participants as a means of delaying action. Most importantly, the processes themselves can lack transparency and accountability – concerns have been expressed about whether multistakeholder initiatives further the interests of the participants rather than pursue consumer and citizen benefit. It can be unclear who, if anyone, is seeking to identify and further the public interest in these initiatives.

A second response, then, is what we think of as “procedural accountability”, a collection of regulatory initiatives to oversee the processes by which platforms make rules and govern markets, rather than the services they host or the tools they use. In these approaches, regulators specify goals to be achieved (in broad terms), and standards for platform procedures to achieve them – for example, standards for goal-setting and problem definition; for assessment of impact of chosen solutions; for stakeholder engagement; for dispute resolution and appeal processes; and for transparency.

This provides a way for intermediaries to achieve legitimacy through procedural means – that is, by developing processes, policies and systems consistent with principles of good governance. Such regulatory strategies might work well where disputes about policy are inevitable, desired.

**Demands to ‘level the playing field’ may not coincide with consumer interests.**

---

³ scarcity, and the risks that emerge when a finite resource is held in too few hands. The regulation of media, supermarkets or retail banking has traditionally addressed the problem of too much power and too much concentration. Competition is part of the solution, but regulation of other kinds has always been deemed necessary to protect consumers, suppliers and workers.

Now we have a different challenge – a surfeit of openness. Anybody can reach a global market on Facebook, Amazon, peer-to-peer lenders or cryptocurrency trading sites. Platforms seek to build trust, including by working to filter out bad actors. But it is often impossible to assess how effective their rules, algorithms and automated detection technologies are at this. The range of issues is as diverse as the economy itself; we don’t know how to measure success; and we don’t have access to the data even if we did.

Second, applying old rules to platforms’ new business models is unlikely to be effective, because the costs and benefits of regulation are so different in different contexts. As Edith Ramirez, former chair of the US Federal Trade Commission, put it in 2015: “…existing regulatory schemes tend to mirror, and perhaps even entrench, traditional business models and thereby chill pro-consumer innovation.” Demand to “level the playing field” are frequent, but usually self-interested, and may not coincide with consumer interests.

Instead, policymakers need to focus on clearly defined and evidenced problems, and be cautious of unintended negative consequences, including raising entry barriers and foreclosing the benefits of competition enabled by platforms. Transparency is helpful to identify potential areas of concern, but it is important to clarify “transparency of what” as too much transparency can enable platform rules to be gamed.

Third, new ways of regulating are needed.⁴ Prescriptive rules that pre-empt platforms by enforcing particular technical solutions to complex and rapidly changing issues are often counter-productive. Law needs to be rethought alongside code, reconciling private market governance with public policy. Dialogue is called for between policymakers and platforms to increase mutual understanding, maximise benefits and anticipate challenges.

We are moving from an era of command-and-control regulation to one characterised by co-governance, forums for collaborative rule-making, and a need to ensure all stakeholders’ interests are sufficiently represented. In this world, we need to avoid vague law that delegates legal and regulatory decision-making to platforms without clear mandates or accountability. But often, the risk is law that is the opposite of careful: that throws problems over the wall to technology firms, based on unproven assumptions about technological capabilities, little visibility of intermediaries’ policies and processes, and no systematic approach to oversight, impact assessment and review. The protracted debate about the EU Copyright Directive provides an example; in
outcomes are difficult to specify, and it is hard to assess the impacts of algorithms and platform features. In such cases, following due process may be a better indicator of responsible decision-making than decision outcomes themselves.

Companies already voluntarily put in place some types of procedural accountability, for example, ethics committees and transparency reports. But as with multistakeholder forums, government usually lurks in the background. There are procedural elements in a number of current policy and legislative proposals. For example, both the EU’s draft Copyright Directive and recommendation on illegal content have procedural components, including standards for complaints and redress mechanisms, transparency undertakings, and platform notifications of decisions.

In the UK, the Code of Practice on Search and Copyright signed in 2017 by Google, Bing and rights holders, provides an example of regulators playing an active procedural role – they convened the parties and worked to agree measures of success for actions to reduce infringing material appearing in search results, and an approach to evaluation and reporting, with the Intellectual Property Office (IPO) commissioning research to track progress. However, this also illustrates the potential limits of procedural approaches; there is no requirement of redress for websites that can show they have been wrongly classed as infringing. All stakeholders need to be represented in procedural accountability initiatives, including those who will push the case for freedom of expression, consumer interests and competition.

Procedural accountability does not of course resolve the difficult issues at the heart of online content regulation: the trade-off between different interests, the difficulty of differentiating legal and illegal content and the importance of context, which mean content decisions will inevitably be contested. But by establishing due process, independently defined and ideally independently validated, intermediaries may be able to legitimise their content policies and practices without the need for regulators to specify the particular tools and specific outcomes by which they manage their communities.

**REMAKING LAWS AND PUTTING CONSUMER, CITIZEN AND WORKER INTERESTS FIRST**

Platforms provide an opportunity for the role of policymakers to evolve. They should leave specific rules and particular technical solutions to platforms, which are in the best position to implement and evaluate responses to identified problems, and assess unintended consequences. Instead, policymakers should focus on setting overall objectives, determining whether intervention is needed to achieve them and working with platforms if additional measures are considered necessary. More generally, they should encourage good governance by platforms that achieves a fair and responsible balance between fundamental rights, and thereby builds public trust, and promotes freedom of expression and open markets, while also protecting consumers and citizens from harm.

Perhaps a new policy playbook is starting to emerge that can help in this task:

- First, identify specific problems, based on robust evidence, and with reference to consumer, citizen and worker rights, not historic vested interests or incumbent lobbying.
- Second, convene all the parties who can play a role in addressing identified problems – this may include platforms and other technology firms, but also civil society, the media and various parts of government.
- Third, set measurable objectives, in consultation with all parties, and define clear remits and tasks. This may be achieved by “nudging” parties to a consensual agreement. But government has a range of carrots and sticks at its disposal – finding the right leverage to achieve the right outcome is a critical part of the new policy challenge.
- Fourth, explore ways of testing and revising policies rapidly. Lessons from technology – the use of sandboxes, test-and-iterate, trials – may help.
- Finally, put in place due process to oversee parties’ efforts to fulfil their commitments, assess the fairness and effectiveness of their actions, and iterate policies and incentives where necessary.

**CONCLUSION**

The task of modernising regulation for a platform society is not trivial, as digital will touch every part of the analogue economy, and more often than not we are likely to find the old rules are not fit for purpose. New capabilities and maybe new institutions are required. Risks – failure to achieve the intended purpose, or unintended consequences for the various sides of platform markets – are impossible to mitigate entirely.

Nonetheless, the breadth and complexity of platform challenges and opportunities make accountability more important, not less. Platforms undertake a great deal of regulatory activity, much of it in consumers’ interests, but rarely with systematic scrutiny. Policymakers must find better ways of engaging with platforms, and more effective oversight of platform activities, if we are to move from today’s counter-productive “dialogue of the deaf” to a more constructive future.

**VICKI NASH** is deputy director and policy and research fellow at the Oxford Internet Institute. **MARK BUNTING** is a partner at Communications Chambers and a visiting associate at the Oxford Internet Institute.

REFERENCES

1 For example, the FOSTA-SESTA bill, an amendment to Section 230 of the Communications Decency Act, was signed into law in the US on 4 April 2018.

www.iicom.org

July 2018 Vol 46 Issue 2 | InterMEDIA
Telecoms policymakers everywhere face similar challenges. As networked applications become ever more critical to modern life, users are demanding that broadband services meet their growing needs. How can regulators develop the institutional and industry capability for managing increasingly complex digital supply chains?

I am based in the UK, so we can take the charter of Ofcom, the UK regulator, as an exemplar of the situation. Its remit for broadband and broadcast is encoded in the Communications Act 2003 (and elsewhere in government policies). It aims to:

- Develop UK digital infrastructure, making good experiences through investment and innovation
- Ensure retail services offer choice and transparency, by articulating fitness-for-purpose, thus allowing users to make rational trade-offs of cost and service level
- Ensure fair wholesale access for competitive markets, by instigating and refereeing BT’s equivalence platform, with price regulation at boundaries
- Identify and manage economic bottlenecks as these shift, e.g. new markets for network capacity or content delivery vs old local loop monopoly
- Ensure efficient use of finite resources (spectrum, capital, labour), in particular to protect the weak (poor, disabled, remote, etc.) from exploitation.

There is much to celebrate in terms of the industry growing up to meet these essential needs. For instance in the UK, there has been a massive take-up of broadband, with widespread adoption of fibre to the curb (FTTC), and a very competitive mobile market. In many ways the UK is seen as a role model of competent and forward-looking regulation. All human endeavours are necessarily imperfect, and this is one of the better ones. But all regulators now face greater user demand from:

- Richer and more diverse applications, like IoT, telework, remote education, home healthcare, etc.
- Video moving to the internet, so you cannot any longer separate broadband from broadcast
- Increasing need for dependability, requiring a “safety case” as society comes to depend on applications working on a continued basis.

Then there are concurrent fundamental changes in the nature of the supply, which for the UK are:

- A growing requirement to move from FTTC to FTTP/H (premises, home) to improve reliability and capacity
- BT’s wholesale arm facing economy of scale issues, especially as BT’s retail arm has built its own infrastructure
- TETRA (terrestrial trunked radio) replacement with associated (and often unquantified) technical, commercial and political risks

THE ‘SUPERFIT’ REGULATOR

MARTIN GEDDES describes how regulators can shape up to meet the realities of the digital age and give users broadband services that are fit for purpose.
SG is coming for capacity and capability, with challenging backhaul requirements for coverage

- Increasing demand for security and performance isolation between users and industrial internet uses (e.g., smart cities).

I see increasing commentator concern over the broadband experience, as the promised supply doesn’t sufficiently satisfy future demand. Indeed, there is now a widespread user perception of broadband being the “unreliable utility”, in stark contrast to its peers. You won’t get many laughs at a stand-up gig talking about water or gas delivery, but broadband internet service is the target of jokes. My Australian friends tell me their unending NBN (National Broadband Network) comedy is increasingly tragic to live with.

The resulting stresses in the regulatory system exhibit themselves as symptoms like net neutrality, which is an expression of power battles between the edge and core over resource pricing and fairness. End users experience confusion over how to resolve service quality faults: is it the Wi-Fi, router setup, in-building wiring, protocol design, local access loop, ISP service, or the internet in general that’s the problem?

I myself have faced this, struggling to “debug” my own poor home broadband experience, and I am supposed to be an industry expert! It has involved at least three items from the above list interacting to manufacture “unhappiness as a service”.

As we can see, there are many facets to this challenge of digital experience quality regulation. The central problem is that there is no universally agreed framework to quantify the network, and to relate it to the user experience. The science of network performance and digital experience quality is immature.

For spectrum policy, the mathematics was all cracked in the 18th century, the science of electromagnetism in the 19th century, and the engineering (e.g., MIMO, multiple-input and multiple-output antennas) in the 20th century. Today in the 21st century we can focus on what policies to implement, not how to execute them.

Similarly, with computing, the mathematics was cracked in early 1930s, and the bulk of the science in the 1950s to 1980s. We don’t worry about different regulation for Intel vs ARM processors, because we know they are fundamentally equivalent at some level. For data transmission, we have information theory from the 1940s; there is a strong theoretical basis with widespread buy-in to foundational concepts.

**IT’S PACKET NETWORKING NOW**

Packet networking is different. Yes, the statistical theory behind shared buffers was developed in the 17th to 20th centuries. But the theory and mathematics of complete distributed systems only became public knowledge in the 2000s. The formal definition of the resource “trading space” is very recent indeed. These conceptual underpinnings aren’t yet in the textbooks or taught on university courses. I know, as I have been teaching them to the R&D labs of leading equipment vendors...

The obscurity and novelty of the core maths and science results in a diversity of metrics, measurement systems, and predictive models. They vary by network bearer technology, vendor and market. For regulators, this poses a danger of picking winners, and then regretting the choice. There is a lack of consensus in the regulatory community about both the problem and its solution.

Furthermore, there is an unclear mandate to solve this issue: regulation presumes the existence of the necessary fundamental concepts and tools. Go back to the start of the article: which of those mandates would legitimise Ofcom spending its limited resources with the Institution of Engineering and Technology to talk mathematical models of packet performance? Possibly none of them. As a result, regulators are forced to face a series of serious questions:

- How can regulators make progress at the practical level to measure and manage broadband QoE (quality of experience)?
- How can they ensure that digital infrastructure is fit for purpose?
- How can they develop the necessary human skills in digital experience quality?
- How can they redesign processes and policies to fit the maths and science?
- How can they acquire an adequate technical capability to get visibility through the end users’ eyes?
- How can they anticipate and act with respect to managing quality at key regulatory, technical or economic boundaries?
- How can they engage with a systemic capability deficit that exceeds their own scope and remit?

My suggestion is that regulators should initiate a “superfit” transformation programme, akin to the “superfast” one of the past decade. The core purpose is to upgrade institutional capability in digital supply chain quality management. Note that I am not opposing or displacing the superfast model; it just has limits to its utility that we must transcend, since quantity is not synonymous with quality.

This is an issue of both organisational capability and national policy. It requires a coordinated response from all stakeholders in the ecosystem, including consumer groups, research institutes, and standards bodies, as well as the usual list of vendors, telecoms operators and experts in law and economics.

The timing is now right, as the maths, science and tools exist, albeit being immature. High-fidelity measurements can capture network performance in a user-centric way. It is possible to identify the dynamic performance effects due to statistical multiplexing, and separate them from the static architecture and configuration ones. There is also an inevitability to the transition, as networks become ever more dynamic – think SDN...

---

There is now a widespread user perception of broadband being the ‘unreliable utility’.
A paradigm change: wherever we are at. This will engage us in an ideal, so we know which way to head from preexisting frameworks to draw on.

There are many other industries that have software engineering. The quality management programme, then we can progress from unmanaged technology trio with a sensibly designed change framework: we only change when we identify with chaos to a self-optimising system. The essential prerequisite is a language to describe the “superfit” vision, to engage with industry to define a broader framework for “superfit” services. The essential prerequisite is a language to describe the problem, and a means of defining what success might look like.

There is a necessary step for most that I term “supereconomic” on the way to “superfit” as in countries such as the UK where the emphasis is on cooperation and decoupling services from network mechanisms. Supereconomic is a transition zone from superfast to superfit. In mobile broadband, an example of superfast is 4G, supereconomic is 5G’s “enhanced mobile broadband”, and superfit is the desired (if overambitious) model for 5G’s low-latency network “slices”. Superfit then starts to deliver assured outcomes and is the regulatory end game.

REGULATORY PRIORITY: EDUCATION

The regulatory priority is to educate oneself and key supply chain stakeholders: people first, then processes, and lastly clever new technology. This means regulators have to identify the internal and external game changers, and those who will help them be effective. These are the people who must need training in the core maths and engineering, and how to apply it.

This is a safe bet, as the science isn’t going to change significantly: there’s only one plausible answer. That said, regulators need independent advice and review of the core material, because we all require social proof as well as intellectual argument. This may involve formal contracted processes, as well as informal (e.g. from the Royal Society in the UK).

The subsequent step is to perform experimental measurements of infrastructure using these new techniques and their supporting tools. The experiments should be designed to meet regulatory objectives, which may substantially differ from commercial ones or those of the end user. These findings can then be promoted internally. This creates vital institutional understanding, and gathers feedback from the regulatory coal face.

Once this basic shared understanding is developed, the main planning task begins, to build a map of the upgrade journey. The needs a necessary consultations to establish what is the right “superfit” vision, the best delivery approach, and how they can actually be delivered. Then the policy establishment can spearhead the change process.

The transformation timescale is 10+ years, but valuable results can be delivered relatively quickly. Each refactoring cycle can deliver tangible benefits tied to specific business processes. Examples might be fault isolation, retail service comparison, or service interoperability. This will create public awareness and buy-in to the “superfit” approach, resulting in a virtuous cycle of more assured outcomes and is the regulatory end game.

THE ‘SUPERECONOMIC’ STEP

- From network-centric to user-centric
- From periods to instants
- From averages to distributions
- From separate silos to complete systems
- From state (quantity with quality) to stateflow (quantity of quality).

So where to begin? The kickoff action is to define a learning project to discover how to advance towards fully managed supply chain quality. This means finding a “corner case” which can be used to try the “upgraded” way of working. Good examples might be accessibility services for the disabled, or delivery of broadband to remote areas.

From this pioneer project, we can then construct the nucleus of the new organisational capability: the game changers need a “game changeable” context. This may require a temporary virtual organisation that draws together many different functions and competencies that cut across normal organisational boundaries.

In the UK’s case, this is also an opportunity to redefine the market interfaces, and so have significant impact on BT, Openreach and the regulated equivalence of inputs. What does it mean for a wholesale service to deliver the “same” performance to different users over varying geographies and bearer technologies? How can you be sure content providers are not being discriminated against?

This in turn opens up the opportunity for a broader industry upgrade, like those from dial-up to broadband, or analogue to digital, or fixed to mobile. The enlightened regulator can perform the necessary consultations to establish what is the right “superfit” vision, the best delivery approach, and how they can actually be delivered.

Then the policy establishment can spearhead the change process.

MARTIN GEDDES is a network performance scientist and a scholar of emerging telecoms technologies and business models. His company, Martin Geddes Consulting, is at martingeddes.com

36 InterMEDIA | July 2018 Vol 46 Issue 2

www.iicom.org
The IIC

Membership

TOP REASONS TO JOIN IN 2018

We welcome members from across the converged TMT sector and current membership includes global IT giants and start up tech businesses, converged regulators from mature markets and national regulatory authorities from small nations. Other members include academics, broadcasters, content providers, lawyers and many more.

Industry players join to...
1. Form influential trust-based relationships with senior regulators
2. Get to test new ideas in a collegiate, neutral, independent environment
3. Gain valuable insights into how regulators are responding to technology and market trends
4. Gain consensus on best regulatory frameworks for commercial and wider societal benefit
5. See emerging trends from across the converging digital ecosystem

Regulators join to...
1. Gain current information and insights
2. Build supportive and strategic relationships
3. Explore the far-reaching implications of new technology
4. Showcase their regulatory work in a collegiate arena
5. Get validation and constructive feedback on ideas from international peers

Events form the backbone of the IIC. They give members and non-members the chance to meet in a neutral environment, develop informal bonds and forge solutions to policy and regulatory issues. Additionally, members receive InterMedia, the IIC’s quarterly journal, and access to post-event reports for which they are eligible.

BECOME AN IIC MEMBER IN 2018

The IIC operates on a not for profit basis solely to enable the balanced, open dialogue that informs the policy agenda.

Fees enable us to deliver a rich programme of discussion events and other benefits for our members. There are different levels of membership to suit your organisation type, size and goals.

TO DISCUSS MEMBERSHIP OPTIONS...

CALL: +44 (0) 208 544 8076
EMAIL: a.millwood-hargrave@iicom.org

INFORMING THE POLICY AGENDA

iicom.org
The IIC publishes Intermedia to provide a forum for a wide range of people and views. Intermedia does not necessarily reflect the opinions of IIC officers, trustees and members. Credit quotations as source: Intermedia, Journal of the International Institute of Communications © 2018

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