Inter MEDIA

International Institute of Communications

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

DECEMBER 2022 | VOLUME 50 | ISSUE 2

THE INTERNET OF GEOPOLITICAL THINGS

How ideology is influencing the regulatory environment

International Institute of Communications

Insight • Exchange • Impact

If the digital and social economy is important to you, why not join its most influential policy network?

Become part of the growing network of members that is committed to finding regulatory frameworks for the widest societal and economic benefit.

The top five benefits IIC Members enjoy

1. International, regional and local events, including exclusive online events
2. Private networking for regulators and industry peers
3. Informal access to leading policy thinkers
4. Speaking and chairing opportunities
5. InterMedia, event reports and annual review

With thanks to our Industry Partners, regulators and other members

AT&T · BT · Cisco · Ericsson · Meta · Google · amazon · Liberty Global · Microsoft · Netflix · Nokia · ooredoo · sky · acma Australian Communications and Media Authority · Millicom The Digital Lifestyle · Telefónica · verizon · vodafone · The Walt Disney Company

Contact us about joining today

+44 020 8544 8076 enquiries@iicom.org www.iicom.org/become-a-member

TELECOMMUNICATIONS • MEDIA • TECHNOLOGY

DECEMBER 2022 | VOLUME 50 | ISSUE 2

CONTENTS

Inter MEDIA

International Institute of Communications

DIGITAL SOVEREIGNTY ISN'T GOING AWAY

The age of internet connectivity, supercharged by the COVID-19 pandemic is posing a challenge to governments and regulators around the world and, frankly to governance itself. Because, as it has evolved, the issues and dynamics around the internet have become as much about values as they were initially about value. As our cover author Vladimir Radunovic opines, it has shifted from the functional to the political, with real-world consequences in areas like routing, chip manufacture and the rise of the techno-security state. From differences in values and culture emerge different visions of the future architecture of the internet and with them, demands for digital sovereignty. Spreading the benefits of technology depends on the free flow of data and information. Yet states accountable to their citizens – as well as those that aren't – will continue to expect their perspectives and demands to be taken into account: all understandable, especially for the good actors. Navigating a path between such national interests and those of the wider global community will be very difficult, but it is essential. The future of the internet depends on it.

Chris Chapman, President, IIC

P.S. I recently became a director of ICANN, whose mission is to help ensure a stable, secure, and unified global internet. The commentary above is made solely in my capacity as the President of the IIC, which is a non-partisan, non-policy-making organisation dedicated to debate among policymakers, industry and academia. These comments should not in any way be construed as a view expressed on behalf of ICANN or as an ICANN director.

www.iicom.org

The International Institute of Communications is the world's leading independent, non-profit, membership forum engaged with digital media policy and regulatory affairs. It is the policy platform for the digital ecosystem.

Intermedia editorial enquiries:
enquiries@iicom.org

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

Follow us:

LinkedIn

@The_IIC

Watch speakers at IIC events on:

YouTube

www.youtube.com/user/TheIICom

Further content and details are available on the IIC website:
www.iicom.org

NEWS
FROM AROUND THE GLOBE

Above: Delegates to the G20 summit in Bali dedicated a session to digital transformation. Earlier, the meeting had been addressed by UN Secretary-General António Guterres, who said that 'bridges across digital divides' were needed to boost development. He proposed a 'Global Digital Compact', to be discussed at the UN Summit of the Future in September 2024.

DIGITAL TRANSFORMATION

A GLOBAL DIGITAL COMPACT

With the right national policies, digital technology can give 'an unprecedented boost to sustainable development', particularly for the poorest countries, UN Secretary-General António Guterres told the G20 Summit in Bali, Indonesia. 'This calls for more connectivity and less digital fragmentation' he said. 'More bridges across digital divides and fewer barriers. Greater autonomy for ordinary people; less abuse and disinformation'. However he went on to emphasise that 'without guidance and guardrails', digital technology has 'a huge potential for harm', citing the suppression of free speech, malicious interference across borders and the online targeting of women as examples. To counter this, he proposed that during the UN Summit of the Future, in September 2024, governments should endorse a Global Digital Compact for an 'open, free, inclusive and secure digital future for all' – with input from technology companies, civil society, academia and others. The compact should be 'firmly anchored in human rights' as 'the only coherent approach for a technology that affects every aspect of our lives'. The secretary-general elaborated on the three areas outlined in the Digital Compact:

- Universal connectivity means reaching the three billion people who still have no access to the internet, the majority of whom live in the Global South.
- A human-centred digital space begins with the protection of free speech, freedom of expression and the right to online autonomy and privacy, whilst recognising that 'free speech is not a free pass', and that the Digital Compact must consider the responsibility of governments, tech companies and social media platforms to 'prevent online bullying and deadly disinformation that undermines democracy, human rights and science'.
- Data has immense and unexplored potential to boost sustainable development. However, there is only half the data needed to understand progress and measure impact regarding the Sustainable Development Goals. People's personal data is being used without their knowledge and consent, 'sometimes for political control, sometimes for commercial profit'. He said the Digital Compact should focus on ways in which governments, working with technology companies and others, could foster the 'safe and responsible use of data'. 'The support of G20 countries can help ensure the digital age is safe, inclusive, and transformational'.

Full speech at bit.ly/3AQg6EK

DATA AND PRIVACY

TRANSATLANTIC DATA FLOWS

An executive order to implement the agreement on a new EU-US Data Privacy Framework has been signed by President Biden. This is the third attempt at establishing a set of principles to govern transfers of personal data from the EU to the US after both the Safe Harbor and Privacy Shield mechanisms were invalidated, following legal challenges brought by Austrian privacy activist Max Schrems. The order places limitations on surveillance by US agencies and creates a redress mechanism for individuals to resolve complaints regarding access to their data by US national security authorities. The European Commission said that the new safeguards 'provide a durable and reliable basis for transatlantic data flows', and an adequacy decision under the GDPR is expected within six months.

INFRASTRUCTURE

FRENCH DRONES

The risk of 'hybrid attacks' on telecommunications infrastructure has prompted France to obtain its first deep-sea drone and robot, sources say. Longstanding concern for the security of seabed infrastructure, especially at depths of 3,000 – 6,000 metres, has dramatically increased since the suspected sabotage of the Nord Stream gas pipeline in the Baltic in September. Currently it's thought that only the US, Russian and Chinese militaries operate autonomous underwater vehicles (AUVs) and remotely operated vehicles (ROVs), though there are some run by private companies.

SPECTRUM

5G ON PLANES

The EU will allow 5G on aircraft and Wi-Fi on the road in an updated decision on spectrum for mobile communications. Services will use designated frequencies and be connected to ground equipment via satellite, using a 'pico-cell'. The European Commission expects the plan to 'enable innovative services'. Similar plans in the US were abandoned after objections from airlines and the military. The Commission has also decided to make the 5GHz Wi-Fi bands available in road transport, to be implemented by member states as soon as possible. The decision is thought to pave the way for future metaverse applications.

SOCIAL MEDIA

DISINFORMATION PERFORMANCE WORSENS

The performance of most social media companies in dealing with hate speech has deteriorated, according to an EU report on compliance. The figures are part of an annual evaluation of online platforms' compliance with the bloc's code of conduct on disinformation, with research conducted over a 6 week period in the spring. Twitter assessed just over half of the notifications it received about illegal hate speech within 24 hours, down from 82 per cent in 2021. In comparison, the amount of flagged material Facebook reviewed within 24 hours fell to 64 per cent, Instagram slipped to 56.9 per cent, and YouTube dipped to 83.3 per cent. TikTok came in at 92 per cent, the only company to improve.

The amount of hate speech Twitter removed after it was flagged slipped to 45.4 per cent from 49.8 per cent the year before. TikTok's removal rate fell by a quarter to 60 per cent, while Facebook and Instagram saw only minor declines. Only YouTube's takedown rate increased, rising to 90 per cent.

'It's worrying to see a downward trend in reviewing notifications related to illegal hate speech by social media platforms,' European Commission Vice President Věra Jourová tweeted. 'Online hate speech is a scourge of a digital age and platforms need to live up to their commitments.' The Commission said that there had been improvements in companies' frequency and quality of feedback to users.

The factsheet can be downloaded at bit.ly/3AONEmt

INVESTMENT

PLATFORM CONTRIBUTIONS

The European Commission is currently seeking opinions on whether internet platforms should contribute to the funding of new networks given that they are heavy users of them. The idea is being pushed by the European Telecommunications Network Operators' Association (ETRO), which is asking for a debate based on 'fair contributions'. The Body of European Regulators for Electronic Communications (BEREC), a group of European telecoms regulatory bodies, has announced that it does not support the idea. BEREC said the decision followed preliminary findings from its own research into the issue. Doreen Bogdan-Martin, the ITU secretary-general, has suggested that there was interest among ITU members in getting contributions from online platforms. 'We're trying to find ways to bring the traditional operators together with the platform providers and governments and try to find ways to move the discussion forward,' she said.

INTERNET GOVERNANCE

NEW HEAD OF THE ITU

Doreen Bogdan-Martin, a former US Commerce Department expert on telecommunications, has been elected secretary-general of the International Telecommunication Union (ITU), the body responsible for global standards and interoperability on the internet. Bogdan-Martin's main competitor for the role was Rashid Ismailov from Russia. The result was seen as a victory for campaigners of the 'open internet' as Ismailov promised the rejection of 'American dominance'. But in the end he garnered only 25 votes from the 172 member states present, while 139 voted for Bogdan-Martin, the first woman to hold the post. The new secretary-general said she would spend the next four years focusing on digital skill-building and literacy, as well as making digital devices and connectivity more affordable. 'In many cases, smartphones are too expensive; the service is too expensive,' she said.

Ramping up investment in network infrastructure will also be crucial for Bogdan-Martin. The ITU estimates that it will require $428 billion (€439 billion) to meet its goal of bringing the internet by 2030 to the remaining 2.7 billion people worldwide who are still offline.

IIC EVENTS

13-14 December, Washington DC
IIC Telecommunications and Media Forum 2022

14-16 February, Phnom Penh
IIC Asia Telecommunications and Media Forum 2023

22-23 March, Brussels
IIC Telecommunications and Media Forum 2023

May, Miami
IIC LATAM and Caribbean Telecommunications and Media Forum 2023

iicom.org/events/

IN BRIEF

Spanish Prime Minister Pedro Sánchez says that about 70 per cent of all the internet traffic between the US and the EU will pass through Spain once investments planned in data centres and submarine cables have been completed.

The EU has initiated legal action against 23 member states over failures to enact copyright rules into national laws. The Commission has sent 'letters of formal notice', the first step in infringement proceedings.

In the fifth report of the ACCC's five-year Digital Platform Services Inquiry, the regulator proposes that platforms should be subject to mandatory dispute resolution processes and stronger requirements for combatting scams, harmful apps and fake reviews. *The full report can be found at bit.ly/3UahTLM*

In its latest update to the long-delayed Online Safety Bill, the UK Ministry of Justice has announced plans to criminalise the encouragement of self-harm and 'deep-fake' pornography . Requirements to define 'legal but harmful' content have been dropped.

Twitter has closed its Brussels office and the two executives responsible for the company's digital policy in Europe have left. The decision has raised concerns over the company's willingness to follow new EU rules designed to police online content.

The FCC has announced the release of its new National Broadband Map. The website will display location-level information about broadband services available throughout the US, aiming to provide users with accurate information on availability, price and speed.

15 MINUTES WITH...

TIM RINGSDORE, CEO of the Jersey Competition Regulatory Authority

Q. CONGRATULATIONS ON BECOMING THE NEW CHAIR OF THE SMALL NATIONS REGULATORS FORUM. WHAT DO YOU HOPE TO BRING TO THE ROLE?

A. I am looking forward to expanding on the great work Allyson has completed during her tenure as chair by sharing my business and regulatory experiences. My background is from the telecommunications commercial world and I'm now regulating some of the companies I used to work for. I have a very firm view on ensuring that operators are providing the most efficient, secure and reliable networks for the benefit of consumers and businesses. I think regulators have a poor reputation and I would like to raise the profile of the SNRF and the challenges small regulators face, but also the benefits that proportionate and pragmatic regulation can deliver for small nations. Hopefully together we can make sensible recommendations to our various governments regarding the support they need to provide to their regulators to ensure regulation is effective in their regions.

Q. HOW IS THE 'JERSEY ROADS CHALLENGE' GOING, AND WHO ARE YOU RAISING MONEY FOR?

A. I have just completed walking every road in Jersey in support of two charities, the Jersey Society for the Prevention of Cruelty to Animals and Autism Jersey. This involved walking over 700 miles since January at weekends and in the early mornings and evenings. It was a fantastic experience as our island is so beautiful and I managed to raise over £5,000.

Q. ALTHOUGH SMALL NATIONS HAVE MUCH IN COMMON, THERE ARE ALSO SIGNIFICANT DIFFERENCES. YOU'VE WORKED IN THE CARIBBEAN – HOW DO YOU COMPARE THE CHALLENGES FACING A DEPENDENCY LIKE JERSEY WITH THOSE CONFRONTED BY, FOR EXAMPLE, TRINIDAD AND TOBAGO?

A. I think all small nations have similar issues, especially dealing with international companies. These companies can have tough business cases and may attempt to intimidate and influence regulatory decisions to their benefit, so having clear government policies, independence, laws, licence conditions and the powers to investigate and penalise organisations is essential for effective regulation. If the foundations of your organisation are not sufficient then you are better off spending considerable time acquiring the right arrangements that best suit your needs. It took us two years to find the right balance but it has paid dividends as we are now a well-respected and effective organisation. To support our aims we must all develop high quality internal resources, but this is not easy, so to complement this I have always developed a combination of external expert support and close relationships with other similar organisations to help with specific challenges. Keeping very close stakeholder relationships is essential no matter where you are and this is vital to ensure everyone understands your roles and responsibilities, your strategy and how regulation will benefit everyone. Being in a small jurisdiction provides us with this crucial advantage and can raise brand awareness and help develop your reputation.

Q. WHAT INSIGHTS DOES EXPERIENCE IN THE INDUSTRY GIVE YOU AS A REGULATOR? HAS IT MADE YOU MORE OR LESS SYMPATHETIC TO THE PROBLEMS FACING THE TELECOMS SECTOR?

A. I spent 15 years as MD of various telecoms companies so my knowledge of the challenges and opportunities in the commercial world is strong. This has provided me with a huge advantage when there are service incidents or commercial disputes between operators. I do understand what is technically and commercially possible so they cannot brush issues under the carpet and I know the questions to ask which makes operators consider how they approach regulatory issues the next time we engage. I have empathy with the challenges operators face especially with future investment, so I am always looking for pragmatic ways of finding solutions that benefit citizens and the Island economy. However I have limited sympathy where there have been issues involving negligence, reckless behaviour or collusion that could have been avoided. I have no hesitation in using our powers to penalise organisations if required.

Quickfire:

WHAT WAS THE LAST BOOK YOU READ?

Six volumes of Winston Churchill's diaries, inspirational!

WHAT'S YOUR FAVOURITE HOLIDAY DESTINATION?

Nashville, where our daughter lives, and the Caribbean

DOGS OR CATS?

Love them both, but dogs are a man's best friend

WHAT WOULD BE THE FIRST OBJECT YOU'D SAVE IF YOUR HOUSE WAS ON FIRE?

Family photos. We lost too many in the Caribbean during Hurricane Irma

WHAT SONG WOULD YOU LIKE PLAYED AT YOUR FUNERAL?

Kylie Minogue, Lucky Lucky Lucky. I remind my wife of this most days (a 40+ year joke)

ITALIAN, FRENCH OR CURRY?

French, it's less than 13 miles from our shore so we love it

DEBATING DIGITAL ACCELERATION

Bahrain was host to the second in-person IIC event of the year, with developments in the Middle East and North Africa on the agenda. **CRISTINA MURRONI** reports

In mid-September regulators from the Middle East gathered in Bahrain with their peers from further afield and with policy-makers from industry and civil society to discuss some of the IIC's core themes, with a regional emphasis. They debated priorities, experiences, best practice and collaboration at the first in-person meeting in the region since the pandemic. Kindly hosted by the Telecommunications Regulatory Authority, the TMF was sponsored by Frontier Economics.

SELLING THE BENEFITS OF DIGITISATION

The forum opened with a discussion on the objectives and priorities for regulators. The consensus was that the initial focus on connectivity needs to be followed by extensive capacity building and education programmes. In areas where connectivity is difficult regulators have offered incentives to network operators, such as discounted and extended spectrum licences or a temporary suspension of regulatory fees. The forum also highlighted the importance of engaging all parts of society and communicating the benefits of technology, particularly as governments switch to digital services for their citizens. Many, especially older citizens, struggle to use e-government services. For this reason traditional channels will continue to be used, but community digital initiatives and skills training are a key part of the engagement strategy.

A SUCCESSFUL COMPETITION MODEL IN BAHRAIN

The spotlight was on digital transformation in Bahrain in the second session. The country adopted a service competition model, creating BTNET, an open access network provider. The incumbent was required to separate its network and retail operations, subsequently transforming itself into a strong digital service company providing financial services for consumers and digital identity solutions, consulting and cyber services for businesses. There is considerable, successful cooperation within the industry. It's believed that once high-speed connectivity targets are met, innovation will follow.

Regional players in the country also highlighted industry developments and collaboration. 5G is now available everywhere and this will speed up ICT development, while mobile operators offer a digital service platform with many partners enhancing the proposition. Gaming is one of a number of sectors expected to grow and a new data centre is in line to attract foreign investment. The panel of speakers agreed that the guidance offered by national telecommunications plans and the engagement of all parties are a major incentive for the industry to develop. Ambitious policies

on connection speed and sustainability were welcomed. The focus now was on international connectivity, with a new submarine cable due to be operational shortly.

MORE CAPACITY NEEDED

The third session explored national and international connectivity issues. Speakers observed that the digital economy is adding prosperity to the world but the contribution of the digital industry to the economy in the region is still low when compared to the USA and EU. For that potential to increase more capacity is needed, including subsea cables and regional connectivity, neutral co-location facilities for interconnectivity, open access to capacity and affordable prices. More local content would drive greater uptake of digital services and a wider digital transformation. The panel agreed that one challenge in the region is the over-taxation of the telecommunications industry, which is still being treated more as a source of income than as an enabler. Regulators are working alongside the industry in several countries to change this. It was argued that a distinction should be made between access and accessibility. 3G is available to 90 per cent of the population in the region and 4G to 65 per cent, but take-up is much lower. Other factors such as price, local content and education are at play and need to be addressed before the arrival of 5G. Finally, as the trend is towards more video-hungry services, the question is how the burden of investment should be shared between infrastructure providers and the hyperscalers.

DATA GOVERNANCE

The panel discussion clarified that any data framework will need to enable both cross-sector data sharing and cross-country data flows. Speakers argued that a common framework can be built in steps and there may be an advantage in learning from other country's mistakes. GDPR, for example, has shown the difficulty of enforcing the rules. It restricts the use of personal information while users want more personalised services. Achieving this is problematic if written consent is required. Adequacy assessments could be the first step towards determining that another country's safeguards are sufficient. Cost cutting becomes more difficult when the burden of compliance has increased. Future-proof policies can be the solution. This means keeping flexible definitions, tech-neutrality, and legal review processes included in law. Mechanisms to bring stakeholders together are a key element of the process and dialogue must continue when legislation is in place. Regulatory sandboxes were also discussed as a way of extending a domestic experiment to a bilateral or multi-country pilot.

DATA LOCALISATION

Data is now at the core of all transactions, but, on its own, raw data has no value – it needs to be processed and put into context. Today's technology can help make sense of that data. In a significant development for Africa, Nokia is building the largest submarine cable in the continent. There are reasons to be optimistic, as many countries are waking up to data-driven policies, but there is also a risk that some will diverge from principles-based rules and make a push for localisation, running counter to the global data flow. Some also want to look at data flows as an issue primarily of trade. Countries' push for localisation were universally condemned by the industry. As one panellist said, data localisation is not an enabler; it restricts a company's ability to scale and creates fragmentation.

> **"Data localisation is not an enabler; it restricts a company's ability to scale."**

CONTENT SERVICES

Data policy is also key for effective content, as discussed in the fifth session focussed on content issues. Data helps establish the best way to deliver information, and is key to successful content. Regulation has a role in adapting imports to the region's sensitivities, as well as protecting consumers from harmful or illegal content, including misinformation. Here too,

open and transparent collaboration between stakeholders is critical.

As people are spending more and more time online and platforms are used for an increasingly wide range of services, the idea that the risks from online content exceed its benefits is beginning to gain traction in some countries. Part of the solution is the emergence of more Arabic content, with local platforms generating new creators.

PLATFORM REGULATION

The session reported on the pressure for platforms to do more to protect consumers, with the debate shifting to how, rather than whether, to regulate. One panellist said that his body will not regulate for the sake of regulating, but will do so when an issue arises and there is a clear understanding of the problem. The large platforms have the data to create services that other players cannot match. Agile frameworks and rules will help different authorities within a country talk to each other. There also needs to be further cross-country harmonisation.

Collaboration towards a stated objective may be the best way to work together. It helps to stimulate positive action instead of sanctions – because the industry is often looking to achieve the same objectives – and may present options that work without raising compliance costs for everyone. There are a range of tools short of regulation that can be used to achieve the desired outcomes and there is a drive in the region to engage the industry and be open about governments' plans. A panellist from a telecoms company observed that over half of the total industry value is created by six companies globally, while very little of it goes to the sector providing the connectivity. He pointed at the regulatory asymmetry, which sees telecoms heavily regulated while the online giants have much greater freedom.

DATA AND NETWORK SECURITY

Players who serve many markets around the world confirmed that the weakest point everywhere is people – not controls or processes for protection. Training and engaging every company department on security issues is critical, and so is the integration between cybersecurity and operations. As cybercrime is now becoming an industry, the success of the current infrastructure cannot be taken for granted – systems need to be constantly updated and organisations should never really feel safe. For example, there is a continuing lack of understanding of the DNS landscape and how it has evolved. There are more than 1,500 possible domain names in local languages. This is not widely known and, as a result, security systems often treat new names as fake. Even in the DNS space, end users do not know their rights and responsibilities. Education and collaboration is the right approach.

SUSTAINABILITY

The last session explored the issue of sustainability. Industry players discussed a range of ongoing projects and the ways in which new technology like fibre optic networks are reducing the industry footprint. For some operators, being early champions of sustainability has strengthened the brand. Energy consumption is a big issue and several are switching to solar-powered solutions. There was a general call for policymakers to take the lead in the sustainability debate. Attention was drawn by a satellite operator to the fact that a new industry of low-orbit satellites is operating with no rules about space debris. Once again, there were calls for the constituent players in the ecosystem to work together towards sustainability objectives. A 'coalition of the willing' is ready for industry players to join.

THEMES AT THE BAHRAIN RRF

The Bahrain Regional Regulators' Forum brought together regulators from the Middle East, Asia and East Africa region to debate issues of connectivity and the digital divide, the protection of consumers and how to stimulate investment.

- On connectivity there was broad agreement on the importance of breaking down political barriers through regulatory and diplomatic engagement. It was noted that while, in some cases, the challenge was to build infrastructure, often it was engagement that was more important. Discussions explored the removal of geographical discrimination to ensure equality of service in rural and urban areas. While it may be impossible to reach all areas with fibre, alternatives should be provided at the same price since it is the affordability of the service that will enable rural businesses to grow.
- The forum considered the issues arising from consumers' misunderstanding of contracts. There was widespread support for a code of practice, providing clarity in the specifics of tariff and contract terms, download speeds and termination clauses. A COP can also set out the obligations of operators towards consumers in areas such as privacy and data usage. Online protection needs to focus on the education of children and parents, including online tutorial videos.
- There was much debate about the cultural challenge of content being produced outside the country that wouldn't be legal in traditional media, and where regulatory responsibilities fall between different bodies. Technology companies' community standards are the same across the world and don't necessarily acknowledge cultural differences. There was consensus in wanting tech companies to invest, but also for them to make more effort to respect local and regional culture.
- On innovation and investment, regulators agreed on the need to address the challenges coming from technology, such as the protection of data or privacy, but not the technology itself. Regulators need to be mindful of using tools that may limit innovation. It was agreed that guidelines are often more helpful to innovation than rules.

LEGISLATING FOR ONLINE SAFETY

Regulators around the world are wrestling with rules to protect consumers online. **ROSS ANDERSON** and **SAM GILBERT** review the UK's proposed Online Safety Bill and suggest some changes

Public opinion with respect to a small number of tech platforms, including Facebook, Instagram, WhatsApp, Google, YouTube, Twitter and TikTok, shapes the context for the UK's Online Safety Bill. Rightly or wrongly, many people believe these platforms largely constitute the web. While these major platforms were previously viewed as neutral or even benign, a series of scandals has raised questions about their responsibility for serious harms that result from the services they provide. Platform owners' responses have included revisions to terms of service, increases in moderation team staffing and (in Meta's case) the creation of an independent oversight board. These have generally been seen as insufficient.

Despite widespread credence given to the theory of 'surveillance capitalism', which posits that platforms' advertising-based business models are the root cause of such harms, laws such as the General Data Protection Regulation that target platforms' collection and use of personal data do not appear to have mitigated them. The Online Safety Bill takes a different approach, by establishing duties of care for platform owners towards their users.

The apparent simplicity of this solution is deceptive: the Bill itself is lengthy and complicated. It has had several iterations, outlasting two prime ministers and six secretaries of state for Digital, Culture, Media and Sport. Policy issues that predate the ascendancy of 'big tech' – notably the circulation of child sexual abuse material (CSAM) online and the use of digital technology to facilitate acts of violent online political extremism (VOPE) – have been brought into its scope, along with provisions intended to combat fraudulent advertising and safeguard freedom of expression.

OVERVIEW OF THE ONLINE SAFETY BILL

The Bill aims to:

- Make it harder for violent online political extremists to proselytize and recruit
- Reduce the online circulation of child sexual abuse material
- Mitigate risks relating to 'legal but harmful' content (for example, content that might encourage eating disorders)
- Make it harder for children to access pornography
- Prevent fraudulent advertisements.

It targets major social media platforms, search engines and pornography websites (collectively referred to as 'service providers'), which will be subject to regulation by Ofcom.[1] The regulator will set specific codes of practice for service providers and have the power to fine them up to 10 percent of global annual turnover or £18 million (whichever is the greater) – or to block

them entirely in cases of repeated violations.

The Bill's main mechanism is the creation of duties of care for service providers. Specifically, they will be required to:

- Protect their users
- Remove illegal material (including CSAM and VOPE content)
- Create and implement more robust policies on 'legal but harmful' user behaviour and content (including harassment, disinformation, and self-harm material)
- Offer users more controls (for example, enhanced features to block and report other users)
- Prevent fraudulent adverts being posted
- Safeguard pluralism in debate.

In addition, it requires service providers to prevent children from being able to access pornography, via age verification or other means.[2] Finally, it gives Ofcom the power to mandate messaging services to scan public traffic for VOPE content and both public and private traffic for CSAM.[3]

The Bill is framework legislation and does not specify what constitutes 'legal but harmful' content, neither does it describe in detail how service providers should discharge their duties of care, or which service providers are in scope. However, Ofcom has indicated it expects to regulate 30-40 service providers in total.

CRITICISMS OF THE BILL

Despite broad agreement that online harms are a real issue and that self-regulation by service providers is not a satisfactory solution, the Online Safety Bill has many critics. They fall into one or more of three groups: those who believe the Bill goes too far, those who believe it does not go far enough and those who think some aspects of it are unworkable in practice.

Those who believe it goes too far are concerned that the Bill is illiberal, in that it limits freedom of expression, enables the expansion of the state's surveillance capabilities and distances the United Kingdom from multilateral efforts at internet regulation.[4]

The duty of care with respect to 'legal but harmful' content is said to create stronger incentives for service providers to overpolice social media posts, effectively censoring their users, and potentially producing a chilling effect on free speech online. At the same time, Ofcom's power to mandate the use of 'proactive technologies' is seen by some as a back door to the introduction of a general monitoring obligation – the blanket monitoring of users' online activity by service providers, which is prohibited under the European Convention on Human Rights.

WHAT ARE 'ONLINE HARMS'?

There is no settled definition. The Online Harms Whitepaper which preceded the Online Safety Bill specified 23 harms, but noted that its list was 'neither exhaustive nor fixed'. The term is usually understood to encompass both new forms of harm arising from the diffusion of digital technology and established forms of harm to which digital technology has added new dimensions.

Examples of new forms of harm include:

Doxxing: maliciously publishing personal information about a specific individual on the internet

Trolling: posting unsolicited comments online with the intention of causing hurt or provoking an emotional reaction from an individual or group

Cyberbullying: the use of digital messaging applications to send threatening or insulting messages to an individual

Cyberflashing: sending unsolicited sexually explicit images to another person

Revenge porn: posting sexually explicit images of a former partner online without their consent in order to cause them distress.

Examples of established harms to which digital technology has added a new dimension:

- Child sexual exploitation and abuse
- Violent political extremism
- Incitement of violence.

The Bill puts harms relating to data protection and cybersecurity out of scope, while recent comments suggest the 'legal but harmful' category may be scaled back or removed.

Those who believe the Bill does not go far enough are concerned that it leaves gaps – particularly in terms of the protections afforded to women and children, and the scope of the service providers to which it applies. Secondary legislation will be required to specify the 'legal' harms service providers will be required to mitigate, meaning issues such as the online abuse and harassment of female public figures may not actually be tackled despite the concern and undoubted harm this causes. Meanwhile, online gaming platforms, which are used by 86 per cent of 12-to-15 year olds, do not appear to count as service providers by the Bill's definition. Given that design features and aspects of gaming business models have been shown to expose children to financial harms, as well as abuse by older gamers, it is argued that they should be subject to the same duties of care as social media platforms.

Those who think the Bill is unworkable point to its length, complexity, dependence on secondary legislation, and the operational challenges and costs of implementing its requirements – a process which is not expected to begin until mid-2024. It is argued that – in contrast to physical injury – there is no objective way of ascertaining that emotional or psychological harm has occurred, making it impossible to determine whether service

providers have discharged their duties of care.[5] At the same time, controversies of interpretation are said to be a likely consequence of relying on flexible standards and introducing categories such as 'legal but harmful' content and 'content of democratic importance'.

COMMENTARY

We are sympathetic to many of these criticisms, but nevertheless regard the Online Safety Bill as an important policy intervention. Its strength is that it clearly gives service providers responsibility for mitigating the risks of cruelty and other harms that their business activities produce. But it is a weakness of the Bill to suggest that harm mitigation can be achieved without trade-offs in terms of freedom of expression. For ideological, political, and financial reasons, service providers have typically been reluctant to remove content and suspend accounts unless the law has been broken or their own terms of service otherwise violated. 'When in doubt', Meta CEO Mark Zuckerberg has written, 'we always favor giving people the power to share more.'[6] The threat of sanctions introduced by the Bill signals the opposite: that when in doubt, service providers should err on the side of caution and remove or restrict content, accounts, and features that could cause harm to other users.

> **"It is a weakness of the Bill to suggest that harm mitigation can be achieved without trade-offs in terms of freedom of expression."**

We agree that this is highly likely to result in the overpolicing of legal expression on social media, particularly as what counts as 'harm' is not settled. There will be more instances of inconvenience and unfairness: users posting in good faith may find their access to services being shut off temporarily or permanently, or even that they have been reported to law enforcement. It is entirely predictable that features designed to facilitate reporting of abuse and blocking of abusive accounts will be used maliciously to harass opponents.

However, we believe the harms are sufficiently serious that the trade-off is worth making. If we are presented with a choice between a system that maximizes freedom of expression and one that minimizes cruelty, we should choose the one that minimizes cruelty. Limiting freedom of expression in mass-market social media is a price we may well be prepared to pay if we are serious about mitigating online harms. Note that platforms such as Facebook/Meta and YouTube already use their terms of service to take down not just illegal child sex abuse material but animal cruelty, videos of gangland killings and much else; yet there are some forms of cruelty, such as revenge porn, over which the industry drags its feet. A focus on cruelty may help clarify boundaries. Moreover, it is important to note that such limits do not amount to the removal of individuals' basic right to free speech. Even when permanently banned from one platform, users remain free to post on other platforms, or to build and publish on platforms of their own. It is providers of infrastructure services such as web hosting, payments, and cloud security which have the power to cut off altogether individuals' and organizations' ability to express themselves online – a power that is rarely exercised. As noted, these providers are outside the Bill's scope.

There is one caveat. The duty of care to users creates high compliance costs, which only large organizations can reasonably be expected to bear. If, as some have suggested, it was extended beyond the 30-40 service providers Ofcom appears to have identified there would probably be adverse consequences for competition: smaller providers might become financially unsustainable, reinforcing the market power of big tech companies. For this reason, we are in favour of a scale threshold. However, we also favour bringing major gaming platforms such as Roblox into scope.

Finally, while we recognize that the Bill creates legal uncertainty, we think there are grounds for cautious optimism about the effectiveness of flexible standards in reducing harms. Since 2006, UK financial services firms have had a duty to ensure they are 'treating customers fairly' (TCF). While it has often been criticized for being a vague standard rather than an enforceable rule, in practice TCF has led to firms giving more consideration to the meaning of 'fair' treatment and how it can be evidenced. Together with dialogue between the regulator and firms over enforcement notices, this appears to have had a positive impact on the customer-centricity of sales practices, new product development, and organizational culture.[7] What TCF has done for financial services, an Online Safety Bill with a focus on cruelty might do for digital ones.

CHILD PROTECTION

Some online services, such as Gmail and Facebook, already scan communications for images that are already known to be illegal, including images of sexual abuse. US firms are required by US law to report such material to the US National Center for Missing and Exploited Children (NCMEC) and cannot report them anywhere else, which will cause a problem if Ofcom wants them reported directly to a UK agency. NCMEC currently reports about 100,000 such images to the National Crime Agency every year resulting in several hundred

prosecutions per month for indecent image offences.

Recently, some services have also started using AI to scan for new images that might be illegal. This has a much higher error rate; there are both false negatives (abuse images that escape detection) and false positives (legal images that are wrongly flagged as abusive). For example, a father who took a picture of his infant son's inflamed penis at the request of the nurse at a medical practice got a visit from the police, and lost access to his Google accounts, after the company's AI flagged the photo as abusive.[8]

The European Commission now proposes, in its child sex abuse regulation currently before the European Parliament, to extend AI-based scanning from images to text and to insist that end-to-end encrypted services such as WhatsApp build scanners into their app, so that text can be scanned before it is sent or after it is received. Ofcom has consulted on similar proposals and on extending text scanning from 'grooming' to terrorist radicalisation.

Extending scanning from known-bad images to suspect images and then to text will greatly increase the number of false alarms and thus the number of innocent people caught up in the surveillance dragnet. The European Commission admitted internally that there might be a false alarm rate of 10 per cent, but claimed that if there were 1,000,000 grooming messages, then 100,000 false alarms could be dealt with. However, there are about 10,000,000,000 text messages every day in the EU and with a false alarm rate of 10 per cent, the number of false alarms is not 100,000 but 1,000,000,000. Europe's 1.6m police officers would each have to scan 625 of them every day. Such a system would be simply unworkable.

A deeper objection is that this is the wrong type of initiative to help with the prevention and detection of violent sexual crimes against children (or violent political extremism, to which we will come in the next section). Both types of crime are embedded in local communities; detection is a task for local police forces, while prevention also involves teachers, parents, social workers and community leaders. Automated online scanning cannot substitute for local knowledge and social context.

Violent crime against children is largely family violence; worldwide, there are about 100,000 homicides of children a year. About 200 of these are in the UK; the figure rose slightly in 2020-21, possibly because of the lockdowns. The typical perpetrator is the mother's partner, although from puberty onward a growing number of homicides are committed by acquaintances. Child homicides are the visible tip of a largely invisible iceberg of child abuse, of which by far the most common kind is simple neglect. This is associated with multiple deprivation: unstable families, poor living conditions, structural unemployment leading to endemic poverty, exacerbated by alcohol and drug abuse. It should surprise no-one that patterns for sexual violence are similar.

Abusers increasingly use mobile phones and other devices to monitor their victims. They may take indecent images of their victims or even photographs of actual abuse as a means of extortion or control. By no means are all the victims minors; a woman trying to escape an abusive husband can find him using technology to track her down and threaten her and her children. Technical policy options must therefore be assessed in the context of abusive families. Some tech companies have started trying to redesign products to be more resistant to intimate partner abuse, but this is difficult: the abuser can compel the victim to install spyware on their phone, share passwords and so on.

Once children reach puberty, abuse by and of peers becomes an issue. Even in the absence of abuse, about a third of teens send explicit images to each other as part of the normal process of flirting.[10] When relationships break up, one of the participants may either disseminate an image of the other without consent ('revenge porn' or 'non-consensual intimate imagery') or threaten to do so ('sextortion'). About 5-10 per cent of children and young people report victimisation; the offenders are usually peers of the victim, with about 2 per cent (almost all male) offending.

Another objectionable aspect is the proposal that end-to-end encrypted services such as WhatsApp should be required to scan private messages for illegal images and for potential grooming content on each user's phone or laptop, scanning sent messages before they are encrypted and received messages after they are decrypted.[11] This 'snoopers' charter' would be a significant departure from British law and practice. It would also fall foul of the European Court of Human Rights, which maintains a staunch position against bulk surveillance without warrant or suspicion. It would also be ineffective, as the error rates for text scanning are so high that the police would be swamped in false alarms.

The only known effective way to detect grooming and new CSAM is by user reporting. The problem here is that dealing with user complaints costs money, so the large service providers make it inconvenient to contact a moderator. Here the Online Safety Bill can help by mandating that services provide an effective way for users to report illegal content and have it rapidly taken down. Tech companies already do this for copyright owners; the law should compel them to treat

vulnerable users, such as women and children, with the same consideration. When such users encounter harassment or abuse they must be able to contact moderators quickly so that they can preserve evidence, remove illegal material and block people who are trying to exploit them.[12]

The scanning of private text messages has also been mooted in the context of combatting terrorist radicalisation and recruitment, so we consider that next.

VIOLENT ONLINE POLITICAL EXTREMISM

For the last ten years, London's Metropolitan Police have run an internet referral unit that looks for terrorist material online and asks service providers to take it down. Extending this service from material published online to private material on people's phones and laptops would be a major extension of police power. Reconciling it with human rights law would likely be impossible.

A growing body of scholarship challenges the approach to terrorism taken by the intelligence and defence community since 9/11, suggesting that there are more effective tools than extensive surveillance. One finding in this research is the very strong link between misogyny and violent political extremism, which extends across both Islamist and far-right violence. As one example, Joan Smith has studied all the terrorist murders in Europe since 9/11 and a significant number of mass shootings in the USA. In the great majority of cases, the killer committed a violent crime against a female acquaintance or family member before going on to murder members of the public.

It is hard to see any case for infringing everyone's privacy, in contravention of the settled British tradition, in order to intercept communications at a greater scale when more effective routes are available. And there is also a real risk that such a policy choice would feed the narratives on which extremism relies – that the government doesn't care about its citizens, that it spies on them, that it considers itself above the law, that officials lie and ministers are corrupt, and so on. MPs and ministers should consider the costs and benefits to their constituents and to the institutions on which we rely for maintaining trust in a democratic society.

RECOMMENDATIONS

We have argued that the Online Safety Bill is right to impose a duty of care on important digital platforms. We have also challenged some of its current provisions as having costs that outweigh their purported benefits, especially when there are more effective – offline – ways to tackle the harms. We end here with some specific recommendations:

1. The Bill's scope should be extended to gaming service providers. Gaming platforms expose children to the same risks of abuse as social media, as well as to financial harms.

2. The power for Ofcom to mandate the use of 'proactive technologies' should be dropped from the Bill. Client-side scanning is technically ineffective and impractical as a means of mitigating violent online political extremism and the circulation of child sexual abuse material. It also undermines fundamental freedoms. In general, Ofcom must not be able to mandate the use of 'accredited technologies' but rather regulate for the desired outcomes.

3. There is no technological 'silver bullet' that can solve violent political extremism and child sexual abuse. These harms are better tackled at local community level through increased funding of policing and social work. There needs to be more focus on family violence and better recording of men who threaten, or commit violent crimes against, women and children – not only as a child-protection measure but as an early warning for other types of violent crime, including terrorism.

4. However, the Bill should require all firms offering regulated user-to-user services to enable users to contact them easily in order to block other users who are harassing or attempting to exploit them, to obtain the rapid removal of illegal material and to secure evidence.

5. Teachers should be given a liability shield by the Crown Prosecution Service with respect to indecent images, so they are better able to help deal with the less serious cases of online harms like sextortion.

ROSS ANDERSON *is Professor of Security Engineering at the Universities of Cambridge and Edinburgh.*

SAM GILBERT *is an affiliated researcher at the Bennett Institute for Public Policy*

This article is extracted from 'The Online Safety Bill' policy brief, available at: https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/09/Policy-Brief-Online-Safety-Bill.pdf

REFERENCES **1** For the avoidance of doubt, internet service providers (ISPs) are not within the Bill's scope. **2** Age verification for online services has been proposed several times before and abandoned once ministers and officials started to examine the cost, complexity and likely side-effects. **3** Department for Digital, Culture, Media & Sport (2022). Online Safety Bill Factsheet, 19 April. **4** These include the Declaration for the Future of the Internet, the Santa Clara Principles on content moderation, the Internet and Jurisdiction Policy Network Toolkits on Cross-border Content moderation and the Council of Europe guidelines on combating hate speech. **5** Smith, G (2022). 'Reimagining the Online Safety Bill'. Cyberlegal , 18 August. **6** Zuckerberg, M (2017). Building Global Community. Zuckerberg Transcripts 989. Marquetta University, 16 February. **7** See for example Ring PJ et al. (2016). Taking notice of risk culture – the regulator's approach, Journal of Risk Research, 19 (3). **8** Hill K (2022). A dad took photos of his naked toddler for the doctor. Google flagged him as a criminal. The New York Times, 21 August. **9** Meineck S, Reuter M and Meister A (2022). EU-Kommission nimmt hohe Fehlerquoten bei Chatcontroller in Kauf. Netzpolitik.org, 29 June. **10** Hymas C (2022). Sending nude photos is 'the new flirting' for teenagers. The Daily Telegraph, 23 June. **11** Milmo D (2022). UK could force messaging apps to adopt new technology to tackle abuse images. The Guardian, 6 July. **12** The EU's new Digital Services Act will give such rights to its residents, so the tech majors will have to build the machinery. It would be an embarrassment if they were not compelled to deploy it in the UK too.

THE GEOPOLITICAL INTERNET

The digital world is increasingly being driven by ideology rather than efficiency, with profound impacts on governance and the digitalised society, argues **VLADIMIR RADUNOVIC**. Political trends are shaping the regulatory environment, and regulators need to adapt

John Barrow famously declared the independence of cyberspace in 1996 – describing it as a unique space in which governments were not welcome and would be allowed no control. (Reflecting the Zeitgeist, Barrow was both an internet civil liberties pioneer and a lyricist for psychedelic rock band the Grateful Dead.)

'Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.'

Seen as naïve even at the time, what has since emerged is a structure of internet governance designed to address a range of societal and policy issues. At my organisation, Diplo, we describe this as a building with seven floors, or levels. (See illustration on page 15.)

It begins with infrastructure, including standards and security – once a firm ground which is now becoming shakier. The legal level encompasses jurisdiction issues, intellectual property rights, copyright, labour law and other aspects of law. Development, especially important for small and developing countries, includes knowledge transfer, boosting development in markets, and innovation. The economic level includes taxation, e-commerce, the gig economy and markets broadly. Increasingly, many of these issues are being discussed under the framing of free flow of data. We describe as 'sociocultural' issues of multiculturalism, education and diversity, with human rights covering privacy and freedoms, among others. It is interesting to observe the number of people or idea groups that are working on this construction, from IT professionals and engineers to governments, multinational corporations, human rights movements and grassroot user organisations, to international organisations (all mixed in a big soup of acronyms) – this is the multi-stakeholder environment that is shaping the internet today.

⬅ DIGITAL SOVEREIGNTY AND INTERDEPENDENCE

25 years after the Barrow declaration, this structure reflects 'an age of interdependence', in which the UN has called for co-operation in areas such as an inclusive digital economy, human rights, trust and security, and institutional capacity. Interconnectivity means that the same standards are being pursued globally, with the internet maintained as a single space. Yet, the concept of 'digital sovereignty' is growing in prominence. Russia and China are very open about their demands for sovereignty and are setting up national firewalls, and the EU asserts its right to act independently in the digital world, with its own cloud and even a DNS resolution system. The US has introduced protective economic and regulatory measures against the influence of China, attempting to rely only on the digital supply chain from like-minded states – and its own. Many small and developing countries treat the localisation of national data as a policy priority partly in response to the enormous power that foreign big tech has accumulated. Whether good or bad, this will result in a fragmentation of the 'digital axis'. For example in routing, priority may be given to ideology over functionality – to whether data is going through an unfriendly territory rather than by the quickest global route. This is changing international standards and the implementation of core internet protocols, including DNS and BGP (border gateway protocol), increasing fears among internet communities about the 'splinternet' – a fragmentation of the global internet into parts that are less interoperable or even disconnected one from another.

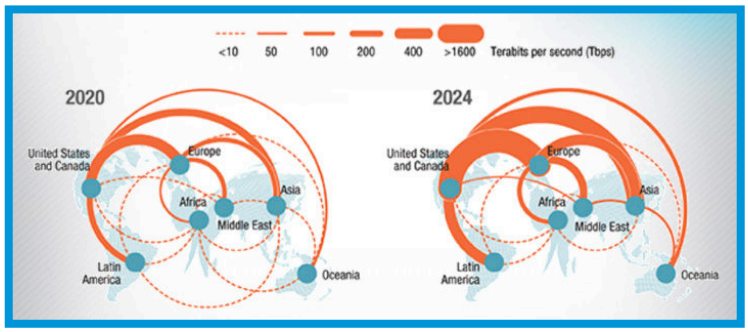
In response, governments are increasing their regulatory grip. The EU has brought in a number of regulatory acts, such as the Digital Services Act, the Digital Markets Act and the General Data Protection Regulation, which shape not only the political environment of Europe but also impact how other countries have to behave and operate in order to be able to work with that huge market. In addition, those regulations (often useful, but not easily implementable) set examples that other countries can follow. The US and China are also shaping their own environments, especially in advanced and emerging technologies such as semiconductors, AI and quantum computing. This is resulting in a less harmonised, less competitive and more fragmented global market. There is also the issue of the supply chain, trusted providers and software with vulnerabilities (or backdoors to allow surveillance or cyberattacks). Such an internet, fragmented through divergent regulatory environments, may place developing, especially smaller countries at a disadvantage, limiting their ability to export home-grown digital services across borders. In this emerging reality, countries may need to band together along common lines and increase efforts to harmonise their regulatory environments at least at the regional level.

Another point we can note is that a range of actors – telecoms, content, infrastructure – are mixed across different levels. Digital convergence is resulting not only in telecoms companies offering or creating content as part of their packages, but also cloud and service providers (Google, Meta or Microsoft) operating at the telecommunications level, for example by laying cross-continental submarine internet cables. Business models based on vast data collection often enable existing monopolists to lead in other areas, like AI. Convergence creates complexities in many areas, from DNS protocols and cybercrime to content issues such as hate speech and disinformation. It also influences policies around emerging technologies like the metaverse which connects VR and AR solutions, social media platforms, and crypto and blockchain technologies. Traditionally governments have turned to telecoms regulators to deal with these issues. But these bodies may not have a sufficient understanding of the internet or the content issues, especially while definitions of those concepts continue to change.

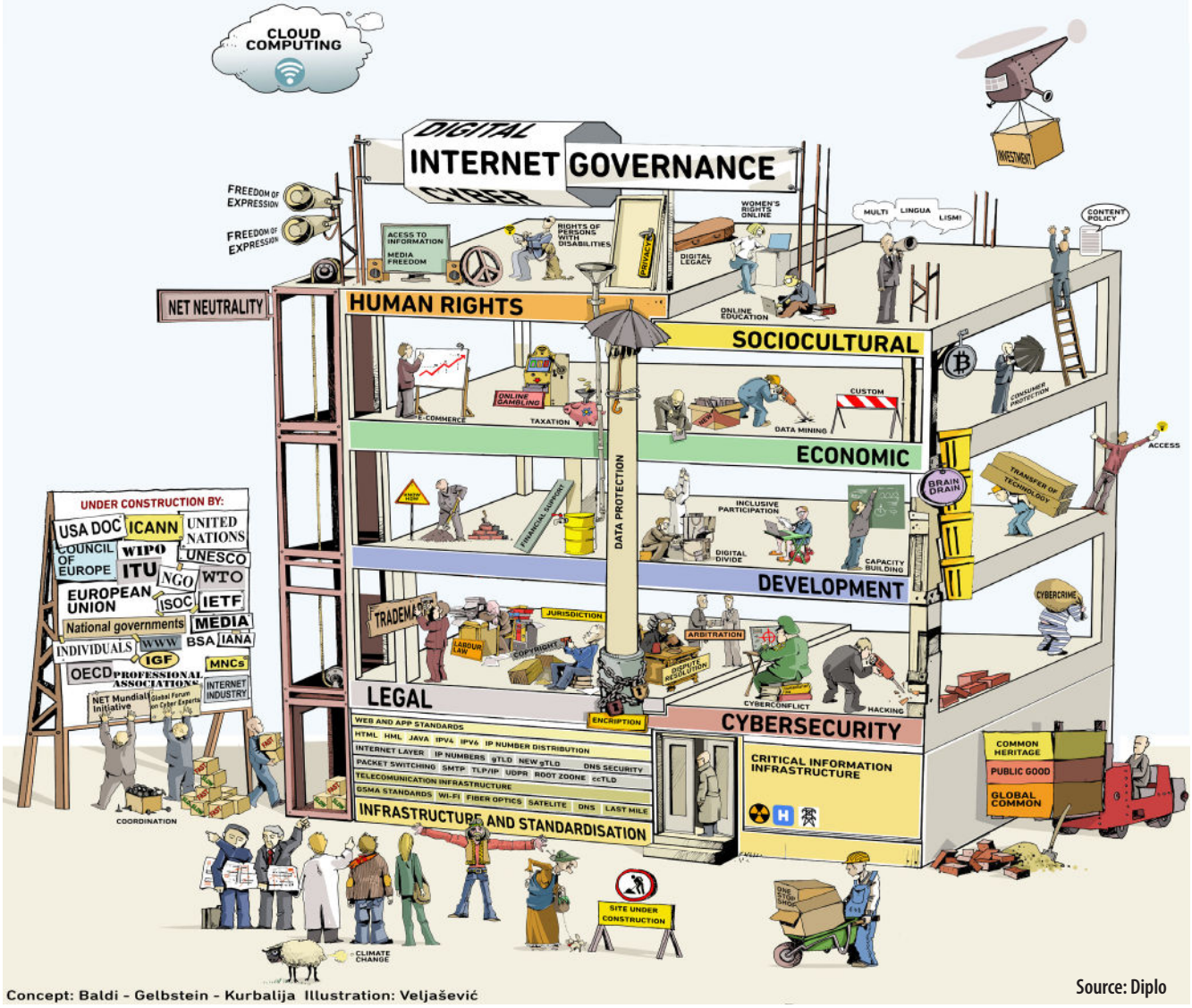
CONNECTIVITY

Cables are a critical part of the connectivity of smaller countries and there have been many improvements in recent years, especially in Africa and the Caribbean. But this too is geopolitical, shaped by the flow of the data and the ability to access information. Many cable networks are created by public-private partnerships, or by big players like Meta and Google. This raises the question of what ownership a small country has – for example, who is liable if a cable is broken, especially where it's crossing a continent. This concern is inflated in times of increased threats of military operations against submarine cables, as a result of geopolitical tensions and hybrid (or open) warfare. The emerging issue is that of satellites, with some countries launching their own, and some commercial satellites operating semi-independently from governments while having great national importance, as witnessed in the case of Starlink following a tsunami in Tonga or for reconnecting Ukraine during the war with Russia. Other regulatory questions emerge in relation to satellite connection provided by global big tech: how does a country exert control and how does it manage issues such as spectrum and conditions for connectivity.

CROSS-BORDER DATA FLOWS



Source: UNCTAD



Another aspect of connectivity is the value of the data flow. There is a natural discrepancy between larger and smaller countries, in part a bandwidth issue, but also because the global companies providing services store their customer data in the cloud, mainly in developed countries. This has a profound effect on the distribution of power. Whoever collects the data can then sell it, and many big tech companies have a turnover comparable to the GDP of a developing country. This provides large technology companies with the influence to shape many policy issues, including competition, taxation (and its distribution), privacy and content policy, and what happens to citizens' data. Should Google be the oganisation to use data for the development of AI and then monetise it? Is there an opportunity for small and developing countries instead? And can this be done by regulation or by creating the environment where this is possible? This is another area where smaller states could work together in a coalition to better negotiate with big tech to set favourable conditions thanks to their bigger market and political power when working together.

CONTENT AND CYBERSECURITY

The world hasn't had to deal with politics and negotiations around content much in the last few decades but now there are huge challenges for social media policies to address issues of disinformation, hate, cybercrime and the dark web without crossing the lines of human rights, free speech and broader freedoms. It's hard to balance these at a national level. Harder still when taking into account global relations.

Arguably, there is no such thing as 'cyberspace' or an 'offline life'. Everything is connected, and everything can be hacked. Increasingly the targets are critical sectors of society, such as energy and healthcare. Costa Rica was locked down for months in a ransomware attack that was supposedly criminal. The threat has evolved from kids and hackers, to criminal gangs, sometimes tolerated and sometimes enabled by states. Countries are openly developing offensive cyber capabilities, many with unlimited resources and political will. So high politics – what's happening in Ukraine and between China and the US, for instance – is something that businesses and governments need to take account of in their threat modelling.

CYBER ARMAMENT

Source: Digital Watch observatory

THE BATTLE FOR THE ITU

Politics is also influencing the adoption of standards. There are battles over, for example, whether human rights should be embedded in new internet protocols, or whether they should include more sovereignty and control. These issues reached the governance of the International Telecommunication Union, which for years hadn't been seen as especially important for geopolitics. The body responsible for creating standards and interoperability had seen increasing political influence, particularly from Russia and China. Their vision for the internet, focused on rejecting 'American dominance', was represented by the Russian candidate for secretary general in the recent leadership election, Rashid Ismailov. At the 2022 Plenipotentiary Conference in Bucharest, however, it was the US candidate, Doreen Bogdan-Martin, who was elected as the new secretary general.

Emerging technologies mean that policies need to be future-proof, and there is much buzz around new concepts like the metaverse. The best way to look at this is to consider the building blocks – in this case blockchain, AI, augmented reality, quantum computing – and examine the challenges and policies related to them. What are the building blocks that can't be seen, and what impact will they have when put together in the metaverse? The buzz can often lead to disillusionment, so it's important to be wary of 'overhype'.

REGULATORY APPROACHES

The roll-out of a technology like 5G raises multiple issues, including infrastructure security, content and protocols, which in turn require a multi-disciplinary approach. This is a particular capacity challenge for smaller countries without access to the range and depth of skills available to larger jurisdictions. However, at Diplo we see many individuals from small states, with specialist knowledge, who are involved and recognised in global internet governance processes. They are often not consulted by their governments, because they are actors from business or NGOs, or the tech community, but they represent a valuable resource. These people could be mapped, perhaps by cyber ambassadors or line ministries or regulators, and utilised to supplement capacity.

CONTENT REGULATION

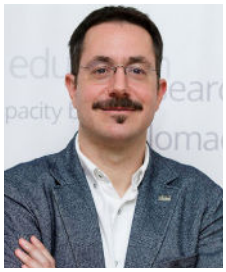
Content regulation is always at risk of extending into internet regulation and then censorship. There is a difference between regulating traditional broadcasters and new media with a different modality but which in many cases operate like broadcasters, for example in the streaming of live video. Often these are viewed at larger scale and as quickly as traditional broadcasters. The massacre in Christchurch, New Zealand in 2019 was live-streamed and re-broadcast many times on social media – content which most believe should have been censored outright. But there is a thin line between content regulation and internet censorship. Because so much content is broadcast in jurisdictions over which a regulator may have no control, there is certainly a need for better cross-border cooperation. While there is a distinction between curated and non-curated content, a company like Netflix operates much more like a broadcaster than, for example, Facebook. Pushing on these 'new media' companies too hard will result in them self-censoring and valuable content could be lost. An open policy challenge is how to distribute responsibility, set clear criteria about objectionable content and enhance capacities for policing such content, including the proper and ethical use of AI to assist humans.

CRYPTO AND NFTS

NFTs and cryptocurrencies raise particular issues for all economies, but especially for small jurisdictions. Here the use of policy rather than regulation is likely to be most productive, working with developers or the crypto community. It's important to avoid overhype but also to avoid responding to overhype with overregulation. While primarily the responsibility of financial regulators, NFTs incorporate issues of creativity and copyright, or smart contracts, and so require broad regulatory involvement.

SUMMARY

Geopolitics leans heavily on the digital environment, shifting the internet increasingly away from the functional and towards the ideological. Cyberspace has blended with the real world without recognising real world borders. As everything is cross-border, so must be co-operation and above all diplomacy. The 'three Ms' of internet governance are multi-disciplinary, multi-stakeholder, and multi-level. It's a holistic area that needs all hands to work and cooperate at the local, regional and national level. Governance is a diversified portfolio, not the responsibility of a single ministry, because everything in the political environment, from energy and finance to education, has a digital component. Internet governance needs to be approached holistically – through a 'whole of government' and 'whole of society' approach.



VLADIMIR RADUNOVIC *is Director of Cybersecurity and E-diplomacy at DiploFoundation.*

REFERENCES AND RESOURCES:

The Age of Digital Interdependence: report of the UN Secretary-General on Digital Cooperation, 2019. https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf

An introduction to internet governance at https://www.diplomacy.edu/resource/an-introduction-to-internet-governance/

Diplo's online courses on digital issues and international relations at https://www.diplomacy.edu/courses/

Digital Watch observatory at https://dig.watch/

HumAInism project at https://humainism.ai/

PIRACY AND THE VALUE OF SITE-BLOCKING

As online piracy continues to grow, **FELIPE SENNA** and **LUÍSA ROMAN** show how site-blocking contributes to a better environment for content and telecommunications industries alike

Piracy is a stark worldwide reality, annually generating enormous losses for rights-holders, content distributors and for society in general. The practice not only prevents holders and intermediaries from receiving access to legitimate remuneration for their efforts, it reduces employment and results in the loss of tax revenues. The profits from copyright infringement serve to fund organized crime, and online piracy can undermine the security of the network itself.

Multiple industries around the globe are affected by piracy: from physical products such as liquor, toys, luxury goods, medicines, cosmetics, and seeds, to academic books and articles, videogames, software, music, and especially audiovisual content. In Latin America, according to a survey by FNCP, the Brazilian National Forum Against Piracy and Illegality, in one year Brazil alone lost 287 billion BRL ($50 billion) to the illegal market, spread across fifteen industrial sectors.[1]

A PROLIFIC ENVIRONMENT FOR CRIMINALS

When it comes to copyright infringement that does not involve physical goods, network infrastructure has become a prolific environment for criminals. Technological development, coupled with increased access to internet connectivity has brought economic growth to the entertainment and telecommunications industries and allowed consumers to access more diverse programming at affordable prices. However, this process has also facilitated the proliferation of piracy in the digital environment. The illicit commercialization of audiovisual and musical content that was previously centred on the physical world has been transposed to the digital sphere, along with the efforts needed to combat it.

According to a 2020 survey by the Latin American consultancy company EtherCity for CET.LA, digital piracy in the region annually causes potential losses for the audiovisual industry of $733 million.[2] By contrast, the study shows that the infringers pirating the content have a potential gain of $675 million a year.

A survey conducted in Brazil by Ipsos MORI in 2019 estimated that pirate platforms were accessed two billion times in the country in only three months.[3] The study also revealed that 78 per cent of respondents (users over the age of 11 with internet access) considered it very easy to access pirated content on the internet, while only 4 per cent said they found such content very difficult to find. The report concluded that the revenues of the audiovisual industry in Brazil could be 17 per cent higher if piracy did not exist.

The chart at Figure 1 shows the total visits, in the first months of 2022, of the five most popular pirate sites in Brazil, Colombia and Barbados. In Brazil the figure represents 30 per cent of visits to Netflix over the period; in Colombia, 27 per cent; and in Barbados, 80 per cent.[4]

FIGURE 1: VISITS TO MOST PIRATED SITES IN LATIN AMERICA

Unfortunately, the same technological tools that allow the development and the improvement of legitimate activities in the digital environment make it more difficult to fight piracy. Pirates make use of the network's facilities, and of their access to internet services, to quickly disseminate illicit content

and then hide, evading surveillance.

Tackling digital piracy requires efficient mechanisms. One strategy often used around the world with remarkably successful results is the use of site-blocking against internet applications dedicated to content infringement. Site-blocking can prevent the consumption of pirated content by stopping users from accessing websites and apps that are aimed at copyright violation.

In the case of Latin America, given the multiplicity, recurrence and dynamism of copyright infringement, the use of site-blocking is the most effective strategy for fighting online piracy. In the process, it can contribute to increases in subscriber numbers and incomes for content distributors, such as internet service providers and pay-TV operators, as well as for rights-holders.

HOW SITE-BLOCKING WORKS

Site-blocking is an anti-piracy and content protection tool that has been used in several countries to prevent access to websites and apps that make protected content available without authorization. In Europe site-blocking is used widely, especially in Germany, Portugal and Spain, with excellent results. In Latin America, blocking is less common, but growing.

Site-blocking is implemented by the internet service provider on the internet infrastructure layer. It can take two forms:

1. 'DNS', which prevents the application from being accessed via a certain domain name, and
2. 'IP', which prevents the application from being accessed via a certain internet protocol number.

These two forms can be used in a complementary manner, but even separately they produce an important reduction in the number of accesses to illicit online content. DNS blocking is the simplest and easiest to implement, since all the Internet Service Providers (ISPs) have to do is program their DNS servers so that a query to a blocked domain name returns an unavailability response to the user. However, this type of blocking does not prevent users from accessing online destinations whose IP addresses are known, nor does it stop illicit streaming devices from receiving content directly from previously programmed IP addresses. Therefore it is important that, to complement DNS blocking, IP blocking is also implemented.

IMPACT ON NET NEUTRALITY

It must be emphasised that site-blocking in any of its forms, including any put in place with government support, does not constitute an offence in network neutrality. The latter is usually a rule directed at the connection provider to promote the preservation of fair competition, and not at a given public administration. Site-blocking, when led by a competent government body, is merely an exercise of authority to curb crimes against intellectual property due to its content, origin, destination, or application, and not data discrimination. The same principles apply for ISPs willing to deploy a site-blocking program throughout their networks for the purpose of 'duty of care'. Neither does site-blocking represent a restriction on freedom of expression. It is not a form of content moderation or state censorship since it only targets websites, applications, and platforms that exclusively, or primarily, transmit protected content without the authorization of rights-holders.

For this reason, site-blocking applies only to internet applications whose main purpose is to promote and distribute pirated content and not to messaging applications, user-generated content websites, social networks or e-commerce platforms.

INCREASED REVENUES FOR DISTRIBUTORS AS WELL AS RIGHTS-HOLDERS

All strategies to combat copyright infringement in the digital environment have limitations and none of them can solve the problem in isolation. This is also true for site-blocking; for example, it cannot target peer-to-peer piracy carried out using applications whose original purpose is lawful. However, by preventing applications which would normally receive millions of visits per day from being accessed by users, site-blocking can provide a significant improvement in the anti-piracy landscape, reducing the unlawful supply of protected works and making it harder for pirates to profit from their activities. A consistent site-blocking programme can result in gains of new subscribers and enhanced incomes for content distributors and rights-holders. Site-blocking experiments conducted in several countries have yielded notably positive results. A survey conducted by INCOPRO in Portugal showed that site-blocking resulted in a 69.7 per cent reduction in access to the blocked pirate websites.[5] Research conducted by Carnegie Mellon University concluded that blocking pirate websites was also an important tool in encouraging users to migrate to legal platforms. In the United Kingdom, after 53 web addresses were blocked, an increase of 7 to 12 per cent in the consumption of legitimate sources was recorded.[6]

"A consistent site-blocking program can result in gains of new subscribers and enhanced incomes for content distributors and rights-holders."

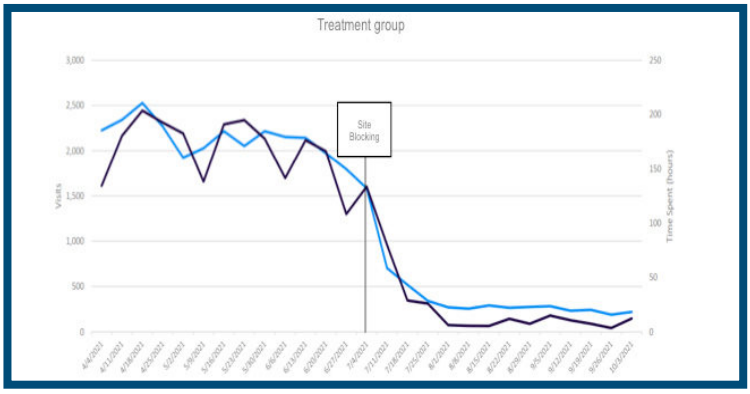
PERU LEADS THE WAY

In Latin America site-blocking has been carried out more recently and on a smaller scale. Of the countries on the continent, Peru is the one with the fastest and most efficient site-blocking mechanism, since it is done administratively, without the need for court orders. In July 2022 alone, INDECOPI, the Peruvian copyright office, was responsible for the administrative site-blocking of 147 pirate sites.[7]

Site-blocking has also been taking place in Brazil, mainly within the scope of an anti-piracy drive known as 'Operation 404'. However, it is dependent on authorization via criminal court orders. In 2022, during the fourth wave of Operation 404, 226 illegal sites and 461 apps were blocked. [8] This represents a significant advance in the fight against digital piracy in the country, but it is imperative that this tool is used more frequently and quickly – and especially through an administrative procedure.

A 2021 monitoring conducted in Brazil, also showed that site-blocking significantly reduces the number of visits as well as the time spent on websites that illegally broadcast audiovisual content.

FIGURE 2: VISITS TO BLOCKED WEBSITES



This evidence makes clear the importance of site-blocking in the fight against piracy and the need for it to be promoted, as well as the benefits for the audiovisual content and telecoms industries.

SITE-BLOCKING MODALITIES

When it comes to the implementation of site-blocking, there are three main modalities: judicial, administrative or through self-regulation. Judicial site-blocking occurs by action of a judicial authority – that is, the rights-holder, upon detecting a violation, reaches out to the judiciary branch and obtains a court order that requires the connection provider to block the content.

Judicial site-blocking is the most common modality of site-blocking in Latin America. However, even though it certainly brings benefits to the fight against piracy, judicial blocking is not the fastest or most efficient solution. Because it depends on a court decision, in judicial systems that are usually already overloaded with demands, the procedure ends up being slow and costly for rights-holders.

In contrast, administrative blocking is granted by a government authority, without the need to initiate a judicial procedure. In countries that adopt this modality, it is usually up to the telecommunications and/or intellectual property regulatory agency to issue such orders, based on due process of law and objective criteria for the identification of infringing websites. Due to the simplicity and speed of the process, administrative site-blocking is very efficient.

In some countries, such as Germany, there is self-regulation regarding site-blocking. The rights-holders and the ISPs enter into agreements that allow direct requests for the blocking of the illicit websites, based on objective criteria and respecting the defence rights of the infringers. In these cooperation agreements it is up to the rights-holders to prove that they are the owners of the pirated work and that there has been an infringement. In return, the ISPs do not oppose taking the necessary measures to curb the illicit website.

Rights-holders, as a rule, do not have the technological tools necessary to effectively identify infringers and remove websites and

other internet applications that promote piracy. This is why, regardless of the site-blocking form or modality adopted, an effective fight against piracy in the digital age requires the involvement and the action of internet service providers.

ISPs provide users with the necessary connection to online activities, legal and otherwise. They are the ones with the technology capable of identifying those responsible for suspicious activities, with incontestable certainty, as well as preventing specified web pages and apps from being accessed by their customers.

COOPERATION BETWEEN RIGHTS-HOLDERS AND ISPS

At first sight there is a dissonance between the interests of rights-holders and those of ISPs. It could be argued that the telecoms industry does not control the activities of those who contract their services and therefore should not have liability over the content generated by third parties or accessed by them. Moreover, given the nature of the services offered by ISPs, it would be commercially advantageous for them to interfere as little as possible with their customers' activities.

Cooperation between rights-holders and ISPs in combating piracy is beneficial to both parties. The development of a system based on constant dialogue and the weighing of interests between ISPs and rights-holders, sometimes with the participation of the public administration, avoids unnecessary litigation, either between themselves or with third parties. This reduces the costs involved in lengthy judicial and administrative proceedings.

Moreover a specific advantage for ISPs is that reduced access to sites that distribute piracy would expand bandwidth space, which is widely consumed in the use of illegal torrent, streaming and IPTV services. Fighting piracy also mitigates cybersecurity risks for ISPs, since pirated websites and applications often contain viruses and malware that threaten not only users, but the stability and security of the wider network.

From a business perspective, preventing access to digital piracy provides a mass of potential new subscribers to legitimate content distribution services – of particular value to ISPs, many of whom also offer linear or non-linear audiovisual programming.

For all of these reasons, discussions to develop a joint strategy to combat piracy have been held between ISPs and rights-holders around the world. Initiatives have come from different sources. In Denmark, for example, the government now hosts regular roundtable meetings between rights-holders and ISPs to discuss regulatory issues. In Germany, on the other hand, discussions were initiated by the rights-holders and ISPs themselves, with government involvement and approval.

As a result of such discussions, in Germany, Portugal, Denmark, the UK, and Belgium agreements between rights-holders and ISPs (memorandums of understanding and/or codes of conduct) have been produced with state approval. In Spain, Italy, Greece and Lithuania discussions have resulted in a decrease in ISPs' resistance to judicial or administrative proceedings, which imposed anti-piracy obligations on them.

SUMMARY

The benefits of site-blocking, both DNS and IP, in judicial, administrative, and self-regulatory modalities, are clear. It must be further promoted in Latin America as an efficient and effective way of reducing the consumption of pirated content and encouraging access to lawful sources. Implementation of these measures can enlarge the legitimate subscribers' market for rights-holders and content distributors, leading public administrations to collect more in taxes, creating formal employment and receiving more private investment. The advantages of administrative site-blocking stand out because it does not depend on a court order, making it faster and less costly than other mechanisms. Expanding of the use of administrative site-blocking would represent a major advance in the combat against piracy in the continent.

Latin American countries need to make changes to their regulatory and legislative frameworks to reduce the obstacles to site-blocking and expand their use. There is also a need to develop a greater dialogue and closer cooperation with ISPs, whose actions are essential to curb effectively copyright infringements on the internet. Regardless of the form or modality of site-blocking adopted in Latin American countries, it is necessary to promote discussions among the different stakeholders involved – not only rights-holders and ISPs, but also government bodies, application providers, civil society organizations and others who could be affected by the issue. Only then will more effective solutions to the problem of online piracy be developed.

FELIPE SENNA *is a Brazilian lawyer, a partner at CQSFV law firm and Director, Public Policies and Industry Relations at LTAHub.*

LUÍSA ROMAN *is a Brazilian lawyer and an associate at CQSFV law firm.*

REFERENCES 1 CNN BRASIL. Pirataria: prejuízo do Brasil com comércio ilegal ultrapassa R$ 280 bilhões: valor atingido no ano passado é a soma das perdas registradas por 15 setores industriais e a estimativa dos impostos que deixaram de ser arrecadados. 2021. **2** ETHER CITY. Dimensión e impacto de la Piratería online de contenidos audiovisuales en América Latina. CET.LA, 2020. **3** IPSOS MORI. Television and Movie Online Piracy in Brazil. 2019. **4** Data collected from SimilarWeb considering the average audience from the specified countries from February to April 2022. **5** INCOPRO. Site Blocking Efficacy in Portugal. 2017. **6** DANAHER et al. The Effect of Website Blocking in Consumer Behavior. 2019. **7** Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. ¡Golpe a la piratería digital! Indecopi bloquea 147 webs ilegales que explotaban obras y producciones protegidas por el derecho de autor. 2022. **8** AGÊNCIA BRASIL. Justiça faz 1ª ação de busca e apreensão contra pirataria no metaverso. 2022.

REMUNERATING NEWS

Fresh from chairing a debate on 'Safeguarding News' at the IIC Annual Conference, **DEREK WILDING** discusses how a journalism fund could be the answer

In a room in the National Arts Centre in Ottawa, some surprising news: digital platform companies support a separate fund for journalism as an alternative to a mandatory bargaining scheme. Some further investigation revealed that Google advanced the idea of 'platforms contributing to an independent fund in accordance with a predictable and transparent formula' in its brief to a Canadian parliamentary committee. Observers of parliamentary committee hearings in the preceding week may have heard Google's policy lead in Canada, Colin McKay, speak in support of the idea.[1]

But for others in the room at the IIC Annual Conference, it was a moment of insight signalling a possible third way in the policy tussle between competition law and copyright – options that Australian scholar David Lindsay has described as 'radically different mechanisms for supporting the private production of news'.[2] In this article, I retrace some of the steps leading to this point, showing why the proposal for a journalism fund supported by platforms has merit.

COMMON GROUND

As the session at the IIC conference acknowledged, the need for regulation is contested by platform companies whose representatives have cited various voluntary initiatives to support local news. Even among those who support regulation, there's considerable disagreement as to what form that regulation should take. And there are knowledge gaps: despite much attention to the topic, there is not yet a satisfactory method of measuring the value to platforms of news, or of the value of referrals from digital platforms to news media sites. But there is some common ground, as the interventions to date are underpinned by two widely accepted points.

First, all these interventions share a recognition of the impact of digital platforms on the business model of news. Claims vary about the nature and extent of this impact. Digitisation itself and the emergence of other businesses that replaced classified advertising for jobs, cars and property are key factors. But it's well established that platforms are now a gateway for news: the 2022 Digital News Report found that 28 per cent of people across 46 countries say social media is their main point of access, compared to 23 per cent for news websites and apps. In addition, news media organisations have lost a substantial share of advertising revenue picked up by digital platforms. The result has been a loss of subscription and advertising revenue for many publishers and the under-production of news.[3]

The second common aspect of the regulatory interventions is the acknowledgment that news is different from most other goods and services. By informing communities and in helping to hold governments and others to account, journalism provides benefits to society beyond those offered to individual consumers. But these 'positive externalities' come at a cost, and the business case that depended upon its appeal to advertisers as well as consumers has been undermined in the multi-sided markets in which digital platforms play a role and in which at least some forms of news can be accessed without payment. In a recent publication, the G7 succinctly explains the combination of three factors present in digital markets that often result in large firms gaining a powerful market position: the presence of network effects, the multi-sided nature of these markets, and the important role of data.[4]

COPYRIGHT VS COMPETITION

But the agreement stops around this point – and this is where the competition versus copyright dispute begins. In the EU, after a couple of unsuccessful early initiatives in Germany and Spain, a new copyright directive in 2019 introduced a right for digital uses of press publications by 'information society service providers' such as digital platforms along with a right to fair compensation.[5] As with other European law, it needs to be transposed by member states, and after publishers – reliant on the distribution channel of internet search – agreed to licence content to Google for free, France became the first state to pass its own,

local laws to give effect to the directive. This prompted Google to adopt a position of not displaying certain content unless the publishers agreed to its use free of charge. At this stage, the deployment of copyright law gave way to competition law as several publishers lodged complaints with the French Competition Authority over the use of unfair trading conditions and the abuse of a dominant position. Giuseppe Colangelo put it this way: 'anti-trust law apparently came to the rescue of copyright law'. (Colangelo is critical of the decision of the Competition Authority requiring Google to negotiate in good faith and of the Paris Court of Appeal which rejected Google's appeal.)[6]

In contrast, both Australia and Canada have favoured an approach based on competition law. In 2019, the Australian competition regulator, the ACCC, found that Google and Meta have market power in search and social media respectively and that they have bargaining power in relation to news sufficient to make them unavoidable trading partners.[7] This supported an intervention that would require platforms to engage in mandatory bargaining with registered news media businesses, as well as mediation and final-offer arbitration if bargaining was unsuccessful. Although the scheme was legislated in early 2021 in the form of amendments to the Competition and Consumer Act 2010, it has not been applied in practice because both Google and Meta have made significant agreements with a number of news media organisations.[8] This has meant that the Australian government has not pulled the trigger for the application of the mandatory scheme which requires formal designation of digital platform corporations by the relevant government minister. Meanwhile, the Canadian Bill C-18 (An Act respecting online communications platforms that make news content available to persons in Canada) is still before the Canadian parliament. The accompanying legislative summary makes explicit the bill's origin in the Australian model: 'Bill C-18 is based on a model similar to the Australian law, but adds some new components'.[9]

A 'BLENDED APPROACH'

This is not the place to explain in detail or explore the merits of either a copyright or a competition-based approach, and it should be noted that the schemes developed by Australia and Canada are not the only examples of competition law being used to find ways to support news media, with the recent G7 report describing the approaches being implemented or developed in a number of jurisdictions. But, taking stock of these various developments, it increasingly appears that a blend of copyright and competition law might be adopted at least in some jurisdictions. Indeed, Swiss scholar Natascha Just has questioned the distinction between interventions based on competition law and those based on other forms of regulation, including copyright. She charts the acceptance of competition law as a core regulatory tool in the era of 'platformization' (and here we might recall Terry Flew's recent explanation of this concept, including what has been described as the 'turn to regulation') along with the realisation that it is not necessarily 'the proper instrument to comprehensively remedy all issues connected with the rise of platforms, most prominently privacy, consumer, and data protection'.[10] Just argues that contemporary conditions demand a blended approach rather an exclusive commitment to one or the other.

This blended approach is of course seen in the EU's coupling of the Digital Markets Act with the Digital Services Act, as well as in initiatives like Australia's Online Safety Act that was passed in 2021, the same year as the legislation that brought in the News Media Bargaining Code. Further, as the recent report for the G7 shows, there are many attempts to tackle competition-focussed issues associated with aspects such as ad tech and anti-competitive practices in the

use of online marketplaces and apps. These are sometimes pursued, as in Australia, by the same competition agency that is working on consumer protection initiatives such as those associated with online scams.[11]

Indeed, the lines used to classify forms of regulation are blurring. While in France it was the competition regulator that provided enforcement for the copyright directive, in Italy AGCOM, the communications regulator, has been tasked with developing criteria to be used for determining fair compensation under the Italian law transposing the EU copyright directive.[12] And in Australia, the ACCC shares responsibility for the News Media Bargaining Code with the media regulator, the ACMA, which applies various tests and administers a register of news businesses. Beyond this sharing of responsibilities though, it is interesting to observe the developing role of competition authorities themselves. The G7 highlighted the view held by many competition authorities that there is likely to be a need for new tools for these regulators.[13] Just argues that competition law's more recent emphasis on administrative action rather than a litigation-heavy approach to law enforcement could render it 'just ... another form of regulation'. Similarly, Colangelo describes Australia's News Media Bargaining Code as a form of regulation that 'provides a swift solution to the ongoing disputes between news producers and digital platforms by guaranteeing a payment to the former without twisting copyright laws or involving anti-trust enforcement'.[14]

> **The lines used to classify forms of regulation are blurring.**

A FUND FOR NEWS MEDIA

It is at this point that the significance of the developments in Canada can be seen because a requirement for platforms to contribute to a government-operated fund – although it has apparently not been adopted so far – represents a clear alternative to either mandatory bargaining or a form of ancillary copyright. Under this approach, platforms would contribute financially to a government-operated fund for news media.[15] This kind of alternative to the competition-based approach has in fact been part of the debate in Australia and elsewhere, but has never achieved much support.[16] Of course, there are attendant policy issues to be addressed, such as how criteria would be set for accessing a fund and how independence from government would be maintained. But these have already been addressed, at least to some extent, in other contexts: the Australian News Media Bargaining Code includes definitions of the type of news that should be protected under the scheme and a mechanism for registering news organisations that produce it, while independence from government in the interests of freedom of expression is a principle that has long underpinned the allocation of arts funding. Google itself flagged the importance of this aspect in its brief to the Canadian parliamentary committee when it proposed 'a single pool of funds, gathered from services that earn revenue from news, with clearly established and objective eligibility, contribution and distribution criteria...'[17]

Uncertainty over the long-term future of current platform-publisher agreements offers at least one reason for exploring this alternative approach. In both Australia and Canada, for example, Meta has flagged the possibility of withdrawing from news.[18] While it's understandable that competition law is seen by many as offering the most suitable regulatory approach, the carefully constructed competition model, founded on an obligation to negotiate, starts to look shaky if a platform does not carry news. It could, however, provide the springboard for some other form of regulation. An obligation to contribute to a government fund, premised on the platform companies' social obligations to contribute to the industry environment in which it operates, is not so different from longstanding schemes administered by communications regulators that support local drama production and universal service. A blended approach to platform regulation, including a platform-financed journalism fund, may prove more durable in supporting news production.

DEREK WILDING *is Co-Director of the Centre for Media Transition at the University of Technology Sydney. He is an IIC board director and President of the Australian Chapter of the IIC.*

REFERENCES **1** Google Canada (2022). Brief Presented to the Standing Committee on Canadian Heritage Bill C-18, Oral testimony from Colin McKay, 18 October. bit.ly/3XFcDT1 **2** Lindsay D (2022). Australian and EU Policy Responses to Algorithmic News Distribution: A Comparative Analysis. the Algorithmic Distribution of news. Palgrave Global Media Policy and Business. bit.ly/3U2MXgq **3** See Newman N with Fletcher R, Robertson C T, Eddy K, and Nielsen R K (2022). bit.ly/3Eup8bs. Reuters Institute Digital News Report (2022). bit.ly/3XF3Mkn **4** G7 Germany 2022. Compendium of Approaches to Improving Competition in Digital Markets http://bit.ly/3Xv7nkR For an explanation of the challenges to the business case of news media, Wilding D, Fray P, Molitorisz S and McKewon E (2018). The Impact of Digital Platforms on News and Journalistic Content. bit.ly/3XtRgnP **5** See Articles 15 and 16 of the Directive (EU) 2019/790 of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC. bit.ly/3UWJzEZ **6** Colangelo G (2022). Enforcing Copyright through Antitrust? The Strange Case of News Publishers against Digital Platforms. Journal of Antitrust Enforcement. 10. pp133–161, p141. **7** For an overview of the development of the news media bargaining code, see Lee K and Molitorisz S (2021). The Australian News Media Bargaining Code: Lessons for the UK, EU and Beyond. Journal of Media Law 13:1. pp36-53. **8** See the appraisals of these made by former ACCC Chair, Rod Sims (2022). Instruments and Objectives; Explaining the News Media Bargaining Code. Judith Neilson Institute for Journalism and Ideas. bit.ly/3XwDWii **9** Bill C-18 Legislative Summary (Preliminary Version), 13 October 2022. bit.ly/3gATh0w **10** Just N (2022). Which Is to Be Master? Competition Law or Regulation in Platform Markets. International Journal of Communication 16: pp504–524. **11** G7 (2022) See note 6, p.18. See also ACCC (2022). Digital Platform Services Inquiry - September 2022 Interim Report: Regulatory Reform. bit.ly/3VClcLH **12** See Legislative Decree 8 November 2021, n177. bit.ly/3Vj6xFW **13** G7 (2022), see note 4, p28. **14** Just N (2022). See note 10 above, p506; Colangelo, note 4 above p.156. **15** This should be distinguished from the more general digital services tax proposed by the Canadian government, at least in advance of any multilateral agreement via the OECD. **16** The author was a contributor to policy submissions to the Digital Platforms Inquiry and the development of the News Media Bargaining Code. See UTS Centre for Media Transition (2020). News Media Bargaining Code. Exposure Draft of the Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020. Submission to Australian Competition and Consumer Commission. bit.ly/3ASPsLs **17** Google Canada (2022). See note 1, p7. **18** Samios Z (2022). Facebook makes key news change in warning sign for publishers. The Sydney Morning Herald. 3 November. bit.ly/3V6EDgI

CULTURE AND CONTENT

Modern European cultural identity has been enhanced through the market dynamics of the streaming industry but, argues **AUGUSTO PRETA**, sustaining future investment will require a new, harmonised framework of digital regulation

Audiovisual content is not only an industry; it is also a fundamental element of a society that shares core common values defined as cultural identity. What Europe lacked in the past –and perhaps still lacks today – is the sense of belonging to a single community and a belief in common ideas and values. To encourage such a sense of identity is an ambitious and vital task but also one which is complex and difficult to achieve in a Europe based on cultural and linguistic diversity. Audiovisual media services such as films and television series can play a relevant role in the scope of this ambition. Conversely, in a time of profound change in society driven by the digital revolution, it can endanger it. Globalisation and digital transformation could bring cultural standardisation and a lack of diversity.

The audiovisual sector in Europe is now at a crossroads. It is developing a policy aimed at preserving national industries from the entry of new global players, while also reducing the drive to innovate: to compete on the international stage by fostering European and international investments thereby enhancing the European and national creative components of the sector.

MAIN TRENDS

Digital transformation is radically changing the media industry. After music, printed media and radio, television is now experiencing the same rocky and disruptive path. This trend has accelerated as the COVID-19 outbreak has led to increased streamed media consumption – the time spent on TV and video streaming has grown consistently since 2019, as efforts to stem the spread of the COVID-19 virus led individuals to enjoy in-home entertainment. Given their increasing popularity, video-on-demand (VOD) platforms have continued to register an uptick in usage, notably involving a part of the population less inclined to the use of digital technology. For example in Italy, according to the media research company ITMedia Consulting, online TV (streaming) reached 10.1 million households in 2021, compared with 5.9 million in 2019, making broadband TV the leading platform for accessing audiovisual content in the country.[1]

VOD services have changed the way we watch content at home and on the move. They have also brought great changes to the production of audiovisual works and, given their increasingly significant position in the audiovisual media services market, they play an expanding role in fostering national and European audiovisual production and distribution. As a consequence, they present a new point of reference in the eternal debate over European cultural identity.

Recently, in an article in *The Economist*, 'How Netflix is creating a common European culture', one observer argues that 'an irony of European integration is that it is often American companies that facilitate it' and gives the example of Netflix 'pumping the same content into homes across a continent, making culture a cross-border endeavour'.[2] The author concludes that 'if Europeans are to share a currency, bail each other out in times of financial need and share vaccines in a pandemic, then they need to have something in common, even if it is just bingeing on the same series.'

DEMOCRATISING NON-ENGLISH CONTENT

Figures from a 2021 study by research company Digital i across the European big five of the UK, France, Italy, Germany and Spain may support this argument.[3] Using its methodology to track Netflix and Prime Video account viewing from a harmonised European panel, the data show that the two streaming platforms are beginning to 'democratise' non-English language content. Since 2019, the proportion of non-English language viewing has increased from 25 to 31 percent. While the catalogue make-up grew by between 5 and 6 per cent, Netflix's UK viewers spent 22 per cent of their viewing time watching non-English language content in October 2021 in comparison with 10 per cent in the first quarter of 2019. The top non-English language titles during this time period were Money Heist, Elite, Squid Game, Dark, and Lupin. For Prime Video, the percentage of the content catalogue made up of non-English language content increased from 19 per cent to 25 per cent from 2019 to October 2021. In terms of viewing, English language content viewing time dropped from making up 93 per cent of all Prime Video viewing to 84 per cent during the same period. Digital i forecasts that English language content will drop to 50 per cent of all mainstream subscription video-on-demand viewing in Europe by 2030.

THE ROLE OF REGULATION: THE EU APPROACH

In this fast-changing scenario, perhaps it is appropriate to start asking some questions: do we need regulation? And for what purpose? Going back in time when television was an activity developed on a national basis and subject to national legislation, EU regulation was specifically created to impose on national broadcasters, including public services, a set of rules to harmonise the system and to increase European production. The 1980s was also a time when the overabundance of American films and TV series fuelling the offer of the new private television channels was considered a major threat to domestic audiovisual industries.

In 1989, through the Television without Frontiers directive, the EU considered it necessary to increase production in member states not only by establishing common rules opening up national markets, but also by imposing quotas for European production.[4] In particular, more than 50 per cent of broadcasting time had to be devoted to European works. 10 per cent of broadcasting time or, alternatively, 10 per cent of the programming budget had to be dedicated to independent European producers.

The Television without Frontiers Directive was radically overhauled in 2007, changed to the Audiovisual Media Service Directive (AVMSD) in 2010, revised and updated in 2018, and finally incorporated into national law by most EU member states from 2019. However, the quota obligations that apply to TV services have not changed since they were first introduced in 1989.

EXTENDING THE QUOTA REGIME

The 2010 version of the AVMSD introduced for the first time the distinction between linear services (broadcasting) and non-linear services (VOD). It required only a minimum level of regulation for the latter since VOD services at the time were still in their infancy. In 2018, things dramatically changed. The quota regime was extended to VOD services, which were required not only to devote at least 30 per cent of their catalogues to European works but also to give them visibility. Obligations such as investment in European production remained optional but, where introduced, they could also be imposed nationally on the basis of the revenues gained in each member state.

From a historical perspective there has clearly been a need for regulation, but in practice it is far from being achieved. While the national audiovisual industries have maintained quality and quantity of production, they have been poor at promoting European content and cultural diversity. The level of co-production has slightly increased, while the circulation of national content in the member states has been limited.

In essence, European content has continued to be, with rare exceptions, a national business. Only with the arrival of the global American players has this scenario finally changed, providing a wider circulation of national works in the member states.

EUROPEAN WORKS AND CULTURAL DIVERSITY

This brings us to a further question: does fostering European content still require regulation? The answer, as for the previous questions, depends again on the scope. If we want to increase the amount of European works and their circulation around the world, undoubtedly the on-demand services

are now the biggest producers in Europe and the ones that make possible the widest circulation and consumption of EU works. Netflix spent 4 billion euros on European films and series between 2018 and 2021, with Disney and Comcast following the same path.[5] In this respect, the streamers succeeded in spreading European works across the EU as never before, without the need for regulatory obligations or incentives (the AVMSD was not yet in force).

The role of VOD players will increasingly be key to the development of European audiovisual productions in the coming years and it is essential to continue to attract investment from these operators. Prescriptive, rigid regulation, left to the discretion of individual member states, imposing in a few cases fixed heavy investments in production for VOD services is the worst scenario for a global player who has to decide in which country it wants to invest more. This also carries a risk of shifting the focus away from producing high-quality content that consumers want, and could ultimately lead to less diversity, less innovation, and less availability of quality content.[6] It may also alter the market dynamics. Most streamers are already spending enough to meet investment obligations relatively easily anywhere. But, at some point in the future, when the market will no longer be growing at the same spectacular speed as in the past (signs of this can be seen in the quarter ending 31 December 2021), they might be in a position in which they need to fall back on a more sustainable model.[7] 'The regulation has thrown sand in the engine.'[8]

REFLECTING SOCIETAL CHANGE

A different solution (and answer) might be given if we move from a mere market perspective to a cultural perspective linked to a subject such as European cultural identity.

The era in which we live is now clearly linked to profound cultural and social changes. The very concept of identity is no longer linked to the past, and the cultural revolution brought about by new generations has meant greater attention to diversity and inclusiveness. We cannot expect this change to be right for everyone or to be accepted in the short term. However, it is a fact that the world has changed, society and its values have changed, and consequently so has the art industry and its protagonists. This phenomenon has led to controversies and clashes, as well as considerable resistance and hostility on the part of those who grew up watching films or TV series in which the protagonists were essentially white, straight males.[9] Women, as well as those who belonged to a minority group, were often either invisible or relegated to limited roles.

Film and fiction TV play a fundamental role in popular culture. They can shape social perceptions of identity and encourage the creation of engaging narrative formats made to enhance the values of diversity, mobility and transcultural exchange in the constitution of a European identity. It can be argued that successful international series such as Money Heist, Lupin, and Call My Agent! would not have had the same reach across borders without the global platform provided by Netflix. However, Netflix's border-crossing content policy does not necessarily originate in the EU. A recent, spectacular example of this is the South Korean series Squid Game, which became the most successful series in the history of Netflix. It follows that if the company's investments in local production don't depend on a specific territory, how can we expect Netflix to care about European cultural diversity?

HARMONISED, NOT ADAPTIVE REGULATION

If we want regulation and not just market dynamics to deal with this goal, it is clear that the AVMSD is not the right tool. The AVMSD is based on a sector-specific framework stemming from the era of analogue television which tries to adapt to a completely changed environment. It does not take into consideration the disruptive innovations that have reshaped the media and communications industry in the digital age and in practice is just an unconvincing attempt to extend, readjust, and refit its past rules to the new ecosystem. In the context of digital transformation, adaptive regulation cannot be the right way to foster the European industry in the innovative global market of content or to promote Europe's values and cultural identity.

In this new framework, a more horizontal approach that tends to harmonise the different sectors into a (digital) single market, seems a more consistent and desirable policy. The European Commission moved in this direction when it proposed two legislative initiatives to upgrade rules governing digital services in the EU: the Digital Services Act (DSA) and the Digital Markets Act (DMA).[10] These initiatives form a single set of new rules applicable across the EU to create a safer and more open digital space where the fundamental rights of users are protected and a level playing field is established for businesses. The extension of these legislative proposals, primarily the DSA, to the world of audiovisual media services, would seem to be a foregone conclusion. In reality, however, these services are the concern of the DSA only where it co-ordinates with parts of the AVMSD. It is the latter that formally remains the directive responsible for developing European audiovisual media policies, including cultural identity.

AUGUSTO PRETA *is CEO of IT Media Consulting and a visiting professor of Media Economics at Urbino University, Sassari University and Università Cattolica di Milano. He is an IIC Board Director and President of the Italian chapter of the IIC.*

REFERENCES **1** ITMedia Consulting (2021). Il Mercato TV in Italia 2021–2023 (Report XV) **2** The Economist (2021). How Netflix is creating a common European culture: Streaming subtitled box sets is the new Eurovision, 31 March. **3** Advanced Television (2021). Forecast: English language SVoD content down 50% by 2030, 22 December. **4** European Council of the European Communities (1989).Council directive of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities. Official Journal of the European Communities, L 298, 23–30, 17 October. **5** Barker A and Abboud L (2022). US streaming giants feel squeeze of regulation in Europe. Financial Times, 8 February. **6** ITMedia Consulting (2021). Obblighi d'investimento in opere europee dei servizi a richiesta, 20 October. **7** Hayes D and Goldsmith J (2022). Netflix narrowly misses subscriber target in Q4; stock tumbles. Deadline, 20 January. **8** F. Godard quoted in the article referred to in endnote 5 above. **9** Harrison E (2020). 11 of the most controversial films and TV shows on Netflix, Independent, 13 September. **10** European Commission (2022), The Digital Services Act package, 4 March.

TELECOMMUNICATIONS IN BELARUS

How does governance work in an autocracy? **EWAN SUTHERLAND** reveals the story of a secretive state

Anyone who had not known of Belarus would have learned of its role as a location for Russian military manoeuvres in preparation for, and in the execution of, its second invasion of Ukraine earlier this year. Formerly the Byelorussian Soviet Socialist Republic, it became independent in 1991 when the USSR was dissolved. In 1994 Alexander Lukashenka was its first elected president, an office he has retained in a series of elections described by international monitors as 'neither free nor fair'.

The governance of telecommunications in autocratic states has not been a frequent subject of academic research, largely for pragmatic reasons. The available documents do not paint a clear picture of how authoritarian systems work. There are no reports of parliamentary inquiries or from the auditor general, and only very rare appeals to the courts or to international arbitration to provide detailed insights. Individuals are not readily available for interview and might not tell the truth, which could never be verified. Often seemingly commercial companies are registered offshore, concealing their ownership, sometimes in an opaque web of firms.

While there have been frequent discussions about a transition to an information society in Belarus, the government has made limited progress in developing the essential skills in information and communication technologies (ICTs). Only 1 per cent of the population have advanced ICT skills, while 37 per cent have only basic skills. There are conventional digital divides, with significant differences between younger and older citizens, between women and men, and between urban and rural dwellers. Nonetheless, there has been a gradually rising share of the economy attributed to ICTs, now about 1 per cent of exports and 4 per cent of imports, while ICT-based services have been growing rapidly. One focus for economic development has been the High Technology Park on the eastern outskirts of Minsk, founded in 2005. A decree on the digital economy reduced VAT and income tax for the Park until 2049, with further tax concessions for the ICT sector. Despite such initiatives, there has been a failure to achieve the level of innovation that would be expected given what the United Nations Economic Commission for Europe has described as its 'highly educated population and a skilled workforce, a strong tradition of fundamental and applied research in several important fields, and a relatively diversified economy with a strong international position in ICT and pockets of excellence in manufacturing.'

In 2019, 87 per cent of the eligible population was enrolled in tertiary education, of which 33 per cent were taking science and engineering courses. Nonetheless, Belarus has a declining position on the Global Innovation Index. It has an especially bad performance in the creative

industries sector, thought to be the result of stringent censorship.

Belarus is a member of the Commonwealth of Independent States and the Eurasian Economic Union, which both have digital programmes, but seem to be making little progress. One specific problem is that open data and open procurement will inevitably reveal patterns of corrupt relationships. Consequently, Belarus is falling behind the Baltic States and Poland, which are part of the more effective, if more demanding, European Union programme to create a single digital market.

POST-SOVIET TELEPHONY

Belarus began in 1991 with a small, fixed telephone network, having been built and run on the Soviet model and controlled by ministries in Minsk and Moscow. It served principally the government, state-owned enterprises and the nomenklatura, using outdated and unreliable electromechanical switches, with 16 lines per 100 people, if they all worked. It was subject to extensive surveillance, in a tradition dating back to the Extraordinary Commission to Combat Counter-Revolution (VChK), better known as the Cheka, later renamed the NKVD and then the KGB, a name uniquely retained in Belarus. International telephony was routed via a facility in Moscow, where calls were individually tape recorded. It was important that citizens should know that surveillance was practised and not merely a possibility.

Out of this Chekist tradition came the System for Operative Investigatory Measures (SORM), an interception and surveillance system developed in Russia. In March 2010, President Lukashenka ordered the introduction of the SORM and two years later it had reportedly been installed on the Beltelecom network and then the mobile networks. Once SORM was in place, the state security apparatus had free access to the network, with the data generated being available for analysis using a wide range of tools, such as deep packet inspection. Installation of SORM requires work on the network by the network equipment manufacturers.

The European Court of Human Rights has ruled against the use of SORM by the Russian Federation, since it gives the state security apparatus direct access to the network, without any of the checks or balances necessary to ensure the human rights of citizens. (Russia was suspended from and also resigned from the Council of Europe.) Belarus is not a signatory to the European Convention on Human Rights. Nonetheless, its use of SORM means that the right to privacy is systematically violated on its telecommunications networks.

With a moderate level of internet access some citizens, especially the politically active and those protesting against the regime, have endeavoured to use more secure apps and VPNs. In this way they have made surveillance more difficult and have been able to conceal some communications from the Belarus KGB. There has even been some hacking of government websites.

FIXED NETWORKS

Beltelecom is the state-owned fixed network operator that emerged from the Byelorussian SSR, previously built and run by the Ministry of Communications, which continues to hold a monopoly on fixed telephony. In 1992, the European Bank for Reconstruction and Development provided US$40 million to begin the digitalisation and expansion of its network. Unusually, there was continued growth of fixed lines, despite the launch of mobile services, with the government promoting fixed access in rural areas. However, a decline has been observed in recent years, falling to about 4 million fixed lines in 2022 and forecast to fall to 3.5 million by 2028. While Beltelecom has upgraded some lines to DSL broadband, it lacks the funds for large scale conversion to fibre to the home.

The Ministry of the Economy performs a few regulatory functions, such as setting tariffs, based on subsidising the provision of local fixed telephony, but has not required a reference interconnection offer or imposed non-discrimination obligations. This disadvantages around 200 companies that are licensed to provide internet access, which are mostly very small. They are located in city centres, are dependent on Beltelecom for backhaul and interconnection, and allegedly charge excessive prices. These providers also face significant costs in complying with censorship rules and installing the surveillance system.

The Soviet telephone network inherited by Belarus was already obsolete and an economic bottleneck in 1991. Today it remains a bottleneck because of the lack of a policy to support and invest in fibre to the home. Maintaining the monopoly of Beltelecom was an easy choice, but one that is limiting innovation and growth.

MOBILE NETWORKS

Like most former Warsaw Pact countries, Belarus in 1991 could not license the 900 MHz band for GSM, so opted for Nordic Mobile Telephony (NMT) in the 450 MHz band, with a 5-year exclusive licence. The BelCel service was launched in 1993 by a joint venture between Beltelecom and the first of a sequence of foreign partners, which struggled to make profits from it and to fit in an NMT service in Belarus with their other businesses. The operator later upgraded the technology to CDMA, still on 450 MHz, but ran into political and market difficulties. The government operator withdrew, and the government allowed the licence to expire, ending the service and the business in 2014.

The first GSM licence was for the 900 MHz band, issued in November 1998 to Mobile Digital Communications (MDC). This was a joint venture of the government, Beltechexport (a local commercial firm) and the Samawi Brothers (SB), Syrians who had emigrated to the United States. SB Telecom was registered in Cyprus, a subsidiary of a company in Switzerland which was beneficially owned by the Samawi Brothers. MDC launched both post-paid and pre-paid services in 1999, initially in Minsk. In 2003, it added 1800 MHz spectrum.

Lukashenka denounced BelCel and MDC as ‘monsters’, insisting on tighter controls and increased state holdings. SB Telecom and Beltechexport were ordered to transfer to the government,

without any compensation, 20.9 and 10 per cent respectively of the MDC stock, giving it a controlling 61.9 per cent. The value of this expropriation was said to amount to US$3 million, but the total investments had been far more, suggesting ten times that value.

While Lukashenka had been an opponent of privatisation, in 2007 he faced severe economic problems, forcing him to make a limited number of exceptions, in this case by an oddly indirect mechanism. SB Telecom acquired the whole stock of MDC for an undisclosed sum, then agreed its sale to Telekom Austria. Although Russian groups, notably Vimpelcom, had also been interested, Telekom Austria duly purchased 70 per cent of SB Telecom, for US$730 million. The price purportedly represented its growth potential; yet it had only a modest 2.7 million customers, with 84 per cent geographic and 95 per cent population coverage, and made minimal profits. In 2010 Telekom Austria acquired the remaining 30 per cent. While it had experience of operations in Eastern Europe, Telekom Austria had no experience of post-Soviet countries.

Unusually, Lukashenka wanted competition in the mobile market, seemingly in the hope of improving affordability for poorer citizens. In early 2001, the Ministry of Communications prepared to issue what it described as the second GSM licence, but in reality sold just 49 per cent of a new mobile operator, the majority to be held by the state-owned Mezhdugorodnaya Svyaz (Intercity Communications), later transferred to Beltelecom. It was to begin services in April 2002 on the expiration of the three-year exclusivity granted to MDC. In addition to four qualifying bids from Russia there was Saudi Oger Ltd, belonging to the Lebanese politician Rafik Hariri. The eventual winner was the Russian group Mobile TeleSystems (MTS), which paid US$21 million for the licence fee and committed to investing US$198 million, apparently with no investment by its Belarussian partner.

PJSC Mobile TeleSystems is a large telecommunications group with its headquarters in Moscow. Its strategy was to expand through greenfield operations in the former USSR, currently running networks in Armenia, Belarus and Russia. It has a complex history, including the involvement of Siemens and Deutsche Telekom, both of which sold their shares. Through Afk Sistema, Vladimir Petrovich Yevtushenkov presently owns just under half the shares. Most of the other shares had been floated in the US, which it was required to end, in compliance with a Russian federal law passed in a response to sanctions against Russia.

The international expansion of MTS was not very successful, having to terminate activities in India, Turkmenistan, Ukraine and Uzbekistan. The first Russian invasion of Ukraine made the political and market environments difficult for Russian firms, so in 2019 MTS sold its subsidiary to Neqsol Holding, a conglomerate based in Azerbaijan, beneficially owned by Nasib Hasanov. In Uzbekistan, MTS was caught paying large bribes to Gulnara Karimova, a daughter of its President, and consequently had to pay fines to the US Department of Justice and the Securities and Exchange Commission amounting to almost US$1 billion.

In April 2004, the Ministry of Communications announced it would hold a tender for a third GSM 'licence', stating that the two established GSM operators had each invested about US$160 million and had a combined total of one million subscribers. Lukashenka then intervened to suggest it could be a domestic state-owned enterprise that would win the third licence, allowing the profits to be retained in Belarus and the prospect of better served rural areas and the use of locally manufactured equipment. Six firms expressed an interest, paying the US$500,000 fee to enter the bidding, in the hope of winning a 5-year licence that was to cost US$5 million, renewable for a further 5 years. Eventually the government cancelled the tender in favour of the creation of a state-owned operator, Belarusian Telecommunications Network CJSC (BeST). Purportedly, this ensured local control over staffing, finances, modernisation, purchases and development. However, the financial crisis drove Lukashenka to its privatisation in 2008, selling 80 per cent of BeST to Turkcell for US$500 million, which at the time had about one million customers. Turkcell rebranded BeST as 'Life:-)', complete with the emoji.

The development of mobile telephony in Belarus followed an unusual and probably unique path. Ideally, Lukashenka would have developed the system without foreign investment or expertise, but needed both, forcing him to involve foreign operator groups. While he sought competition and more affordable prices, the result was a relatively stable market dominated by MTS and Telekom Austria. That the government does not have greater control is the result of the global financial crisis and the constraints on Russian subsidies as a result of Western sanctions. The government has shares and has interfered in operators, raising problems over governance and competition. These cannot be resolved in the Belarussian system, where there is neither an independent regulator nor the rule of law.

FOURTH GENERATION MOBILE

The conventional model for 4G has been for mobile operators to use the technological neutrality provision in their licences to redeploy existing

spectrum from 2G and 3G to 4G in response to demand, where they considered it to be commercially viable. This has been supplemented by additional spectrum auctioned by governments and regulators, in the case of Belarus:

- 700 MHz
- 1710-1730 MHz and 1805-1825 MHz
- 2530-2565 MHz and 2650-2685 MHz

All of this was assigned to a single entity JSLL Belarusikiya Khmarnyya Tekhnalohii or Belarusian Cloud Technologies, which trades as beCloud (2022), on a 15-year licence, allegedly bought for just US$12 million.

This firm had been established in 2012, with 51 per cent of the stock owned by the state through the National Traffic Exchange Centre, an arm of the intelligence services, and the remainder by Sabscissa Holding Ltd, in turn owned by offshore entities. Sabscissa has been reported as belonging to the Lukashenka family or to Konstantin Yuryevich Nikolaev, an oligarch and former minister of transport in Russia.

beCloud has built and operates the government data network, data centre and data cloud platform, in addition to a national 4G LTE network. The then Minister of Communications, Nikolai Pantelei, explained the approach of the government:

'Taking into account the capital cost of construction of this network it was decided to create only one infrastructure operator. All of the other operators will have the right to use the network to provide their services to individuals. Competition is quite relative.'

The beCloud wholesale service was launched in Minsk in 2015, with MTS and Life:) offering retail 4G services using its infrastructure the following year, followed much later by Telekom Austria. It had deployed 1,000 base stations by May 2018, increased to 1,500 by September and to 1,996 by early 2020.

A single network infrastructure presents particular problems. By putting an advanced network in the hands of a single state-owned entity, there is a risk that wholesale access prices will not be provided on an equal basis, with the potential for favouritism towards other state-owned companies (i.e. MTS and Beltelecom). There are also problems of information asymmetry, with the retail operators knowing very much more about their customers and their needs than beCloud, which must design and deliver the network.

The Lukashenka government did not auction the spectrum for 4G, foregoing several hundred million euros. An economic case can be made for such a decision, if the result was a much cheaper network, with capital being used not to pay for a licence but to deploy infrastructure. Unfortunately, it is difficult to find any evidence of superior availability or lower charges for 4G in Belarus. The deployment of 5G has been delayed as a result of sanctions and the economic effects of the Russo-Ukrainian war.

CONCLUSION

Belarus has little of the standard regulatory governance systems seen in democracies. Instead, it has only a ministry and even that is frequently overridden by the President. He has repeatedly intervened pragmatically, if unsystematically, to raise money or to seek better rural coverage. Lukashenka retains his view from Soviet times that services should be provided by the state, but without any understanding of the underlying economics.

Authoritarian regimes have a central concern for surveillance of their citizens, both by traditional and technological means. The system in Belarus is extensive and largely effective, though recently undermined by the poor performance of the economy. Technological surveillance is aided by the state being a shareholder, if not an investor, in two of the three retail mobile networks, the majority owner of the sole wholesale 4G network and owner of the international gateways. Despite its considerable technical capability, some citizens manage to evade the controls, perhaps the result of limited resources for the state security apparatus.

Further research on regulatory governance under authoritarian rule will be increasingly important as more countries are drawn away from democracy. An assessment of the effects of sanctions against Belarus and Russia on telecommunications manufacturers and operators would be very interesting, once the Russo-Ukrainian war is ended. In the same way that there is a 'Brussels effect', with the adoption of policies developed in the EU far beyond its borders, there are indications of an emerging 'Beijing effect', with the wider adoption of authoritarian policies and technologies, which might also be examined.

EWAN SUTHERLAND *is a consultant, a research fellow at the LINK Centre, University of the Witwatersrand, South Africa and a research associate, CRIDS, University of Namur, Belgium.*

REFERENCES

BBC (2013,). Russia seen soon having CIS-wide KGB-style wiretapping system. BBC Monitoring Former Soviet Union, 24 June.
beCloud (2022). beCloud. Retrieved 14 November, from https://becloud.by/
Belsat. (2021). How come that arms business stood at the origins of telecommunication provider "beCloud"? Belsat.eu 10 November
Council of the Baltic Sea States (2020). The importance of digital and ICT skills development for longer working lives in the age group 55+ - and how to bridge the digital divide. https://cbss.org
Centre for Strategic and International Studies (2014). Reference note on Russian communications surveillance, 18 April https://www.csis.org/analysis/reference-note-russian-communications-surveillance
US Dept of Justice (2019). Mobile Telesystems PJSC and its Uzbek subsidiary enter into resolutions of $850 Million with the Department of Justice for paying bribes in Uzbekistan 7 March. https://www.justice.gov/opa/pr/mobile-telesystems-pjsc-and-its-uzbek-subsidiary-enter-resolutions-850-million-department
Eke, S M, & Kuzio, T (2000). Sultanism in Eastern Europe: the socio-political roots of authoritarian populism in Belarus. Europe-Asia Studies, 52(3), 523-547. See also 10.1080/713663061 Fitch Solutions (2019). Belarus telecommunications report includes 10-year forecasts to 2028.
Frear, M (2019). Belarus under Lukashenka: adaptive authoritarianism. Routledge.
Open Corporates (2022). OpenCorporates: The Open Database Of The Corporate World. 14 November. https://opencorporates.com/
President of Belarus. (2017). On Development of Digital Economy (unofficial translation). Decree of the President of the Republic of Belarus, 21 December, No. 8. Republic of Belarus https://china.mfa.gov.by/uploademb/china/economy/digital/2018decree8en.pdf
Rouda, U (2012). Belarus: transformation from authoritarianism towards sultanism. Baltic Journal of Political Science, 1(1) 62-76. https://www.journals.vu.lt/BJPS/issue/view/73
US Securities and Exchange Commission (2019). Mobile TeleSystems settles FCPA violations, 6 March https://www.sec.gov/news/press-release/2019-27
UN Economic Commission for Europe (2021). Belarus. In: Sub-regional Innovation Policy Outlook 2020: Eastern Europe and the South Caucasus (pp. 171-225). https://unece.org/sites/default/files/2021-06/UNECE_Sub-regional_IPO_2020_Publication.pdf
European Court of Human Rights (2015) Zakharov v. Russia. Judgment, 4 December. https://hudoc.echr.coe.int/eng?i=001-159324

IS MY DRESS CRUMPLED?

EMMA FRYER argues for a new social contract between data centre operators and local communities

Many years ago I watched a documentary about a party planner in Chelsea, the most fashionable and exclusive London borough. I saw her rearranging table settings in Michelin starred restaurants, micro-managing guest lists and hopping in and out of taxis between florists and some of the smartest addresses in town. She was unfailingly professional and immaculately dressed.

At the end, the filmmaker asked her what sort of things kept her awake at night: what were her biggest worries? 'My worries are the same as everyone else's' she replied earnestly. 'Things like... is my dress crumpled?'

LIVING IN YOUR BUBBLE

It is tempting to ridicule her but, in her world, this is a legitimate concern. A crumpled dress could be career-ending. Who wants a dishevelled party planner? What troubles me is her assumption that this is universal; that for everyone the most pressing anxiety is not whether they can afford the mortgage or pay the electricity bill or feed their children, but whether their clothing is creased. Living with ten million others in one of the most cosmopolitan cities in the world, is she unaware of the realities of life for those outside her immediate social circle? Is she too preoccupied with her own world, or just wilfully ignorant?

The answer is that she is doing what everyone else does, as a single trip on a crowded London Underground train will prove. People pressed against each other develop a protective insulating bubble by pretending they are alone. Anyone who makes eye contact or tries to strike up a conversation is immediately identified as a foreigner, or insane.

What we have here are parallel universes coexisting in close proximity without intersecting in any obvious way. And this makes me think of data centres, where current controversies over new developments seem to represent another case of two seemingly unconnected worlds that now need to acknowledge each other. Having spent many years navigating the no-man's-land between a highly technical, fast growing and rather secretive industry, and media and policymakers in the outside world, it is clear to me that there is a communication problem.

Data centres are not new. They have been around for decades, quietly occupying obscure corners of trading estates and have, especially in the UK, largely passed unnoticed. While developers restricted themselves to brownfield, ex-industrial sites, sector growth attracted little attention. However, data centre capacity is expanding rapidly to provide the infrastructure needed to underpin our unquenchable thirst for digital services and facilities themselves are getting larger and becoming more physically obvious within communities. People are asking legitimate questions about land use and consumption of scarce resources like power and water. At the same time, data centre developments often seem to be cloaked in secrecy and as a result attract comment and speculation.

SECRECY DESTROYS TRUST

I had a friend who was a 'Bawdsey Boffin', involved in the development and testing of airborne radar in Suffolk on the East coast of the UK just before the second world war. The activity was shrouded in mystery and the locals were highly suspicious. He was accused on multiple occasions of being part of a government conspiracy to manufacture 'death rays'. There were good reasons for secrecy but it did not inspire confidence or trust within the community. Data centre developers are habitually very coy about their plans and this can be unhelpful. It fuels uncertainty, and the lack of transparency over resource use and the associated

impacts creates a perfect platform for mythologizing and mud-slinging. From this point it takes a surprisingly short time for ideological battle lines to start being drawn, irrespective of whether there is anything to fight over.

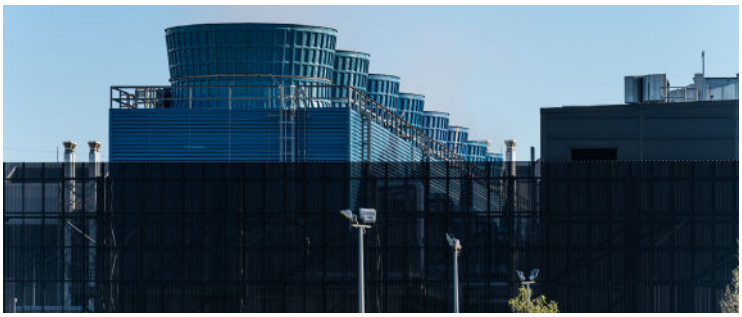
So what needs to be done to connect these two worlds? I think we need a social contract. Data centre operators and developers need to recognise that they do have impacts on the communities within which they choose to locate their operations. These may not be the issues that are often associated with new developments; data centres don't generate much traffic, they are unlikely to produce noxious chemicals, pollute water courses or present significant landscape issues. But they are electro-intensive so need a dedicated power supply. Some use large quantities of water for cooling, and they need a standby generating plant that, although it rarely runs, is noisy and polluting when it does operate.

Moreover, because data centres have locational attributes, they also tend to develop in clusters. This clustering multiplies demands on utilities and land and has consequential impacts such as land price escalation and, potentially, narrowing the range of business functions and therefore employer types in a local area. And because data centres tend to need highly skilled staff, they may only have a marginal effect on local employment or may draw in highly paid individuals who then push up local property prices or annoy people with their swanky cars.

BETTER UNDERSTANDING

Over the last ten years I have spent a lot of time talking about data centres to people outside the sector – journalists, policymakers, friends, students. Their questions are instructive. Does the internet run through the electricity grid? Why can't data centres all be built in Iceland? Why does my smartphone need a data centre? Why do we need data centres now we have the cloud? And so on. These told me two things: firstly, that people struggle to understand what data centres do and why we need them, and secondly that the sector needs to do a better job of explaining itself.

But getting people to understand that data centres are important is only part of the solution. Everybody knows perfectly well that electricity is critical but nobody wants to live under a pylon. So operators have to understand and address the concerns of local residents, of local government, of planning authorities, of utility providers and of course of other industry groups who might have an interest, particularly farmers. Developers need to think carefully how they can best help host communities achieve their educational and employment ambitions: they need to think in terms of community dividends, not share dividends. And clustering could actually be a



benefit if operators are prepared to work collectively. To do all of this successfully requires resource and persistence, and recognition that social performance is not a fluffy add-on but a strategic way of managing business and reputational risk. There are industries that have been doing this successfully for decades and while data centres may feel they have little in common with chemicals, energy or mining, it is here and not in digital infrastructure where best practice resides.

So what is this best practice? Simplistically, there are some golden rules. Social performance must be strategic, and the community engagement and community development activities that are part of this strategy must be qualitative: relevant and necessary at a local level. They should be proactive, sustained and consistent, not short term or piecemeal. This may all seem obvious but the effort is not trivial and in most regions, and for most operators, it is no longer optional.

TWO SIDES TO THE CONTRACT

As citizens, we need to accept that if we want to live connected lives, then we need digital infrastructure which means data centres. They are the physical manifestation of the digital world, where the internet lives. They underpin almost everything we do and enable our economy to function. But, despite the fact that we depend on the internet for every aspect of our daily lives we often don't make that connection. A recent demonstration opposing data centre developments was organized and publicised entirely through internet-enabled social media, but the irony was entirely lost on the instigators. There is a sense that the internet is somehow run by magic, rather than as an essential utility run on physics. Moreover, the extent to which we rely on it means that it must work – all the time – and this demands the kind of industrial-scale infrastructure that we would take for granted elsewhere.

So while our party planner, in her (hopefully) immaculate dress, might opt to maintain her insulated existence, data centre operators are choosing to engage and earn their social licence to operate. At a more general level we are seeing greater transparency and accountability: regulators are increasing their scrutiny of data centre operations and the sector is setting ambitious targets through voluntary agreements. There is a lot more to be done but things are moving in the right direction. And as transparency improves on energy and resource use, there will be less room for conjecture and we can all have a more grown-up conversation. I can't wait.

EMMA FRYER *is a partner at Environmental Resources Management.*

A version of this article was first published at Datacenterdynamics.com

THE ENABLING EFFECT OF GIGABIT CONNECTIVITY

MOLLY BRUCE discusses the findings from Liberty Global's latest policy report on the role of the telecommunications sector in the energy transition. Research and interviews conducted by EY.

The International Energy Agency has identified that digitalisation could enable important changes to global energy demand in carbon-intensive sectors of the economy. The principal sectors involved are transport, buildings and industry (27, 25 and 40 per cent respectively of global emissions)[1] as well as the energy sector itself. What is this 'enabling' effect and what might its environmental impact on these sectors be in light of gigabit connectivity? How can fast internet services help in delivering the energy efficiency measures the world needs to meet demand, as populations grow and human activity intensifies? And how can it all be done without hurting economies already under pressure from rising food and energy prices?

Research has shown that the main impacts of new digital solutions, powered by gigabit connectivity services, are improved productivity and reduced work-related travel. The use of smart connected sensors together with machine learning and artificial intelligence (AI) could increase production efficiency in manufacturing. This way the intermediate inputs required per unit of production will be reduced. Increasing the efficiency of logistics and manufacturing has the potential to greatly reduce the input of oil and coal products.

Technological advances in the telecoms sector, such as higher speeds, ultra-low latency and reliability, allow the wider use of services such as high-quality video conferencing. This incentivises less commuting and reduces emissions from transportation. Such replacement effects are usually dependent on the availability of high capacity networks with a speed of at least 100 megabits per second (Mbps). In addition, a study by the GSMA showed that mobile connectivity often works as a catalyst for the use of more environmentally friendly modes of transport through route optimisation and vehicle fuel efficiency.[2] The GSMA also showed that the use of mobile connectivity for the management of storage and inventory reduced the level of stock and storage space, increasing efficiency and reducing energy used for lighting and cooling. There is a strong correlation with the uptake of such services and the level of digital skills among the population. It is recognised that uptake is a precondition for ICT services to have a positive impact on reducing greenhouse gas emissions in other sectors.[3]

However there are challenges in achieving the strengthening of digital skills. In a Digital Economy and Society Index compiled by the European Commission, results show that only 54 per cent of Europeans have at least basic digital skills. Further, the uptake of fixed broadband with speeds of at least 100 Mbps was 34 per cent, while the uptake of services of 1 gigabits per second (Gbps) speeds was just 1.3 per cent. For very high-speed mobile broadband, such as 5G, the coverage was only 14 per cent (at the time of writing). This suggests the effects of gigabit technology in reducing emissions has significant room for growth.

⬅ Case study – EDGE

Energy-saving building technology

Smart buildings specialist EDGE has developed a solution using sensors and gigabit connectivity to allow real-time data collection of trillions of data points on room temperatures, humidity, occupation and CO2 levels. Scenarios and modelling are then used to manage and improve the building's energy efficiency. EDGE's building management systems can save up to 30 per cent of energy consumed in older buildings and 10 per cent in new buildings. The company first piloted EDGE Next technology in 2018 at its Amsterdam headquarters, before the official launch two years later. That pilot shows savings of 16 per cent of energy to date. This was the result of monitoring occupancy against energy consumption and making informed adjustments along the way.

'Current building systems cover limited elements like weather temperature, but are not designed for sustainability or connected interactions that learn to understand the environmental performance of a building. Our solution monitors the CO2 load or the virus load in the air of a room - and how air conditioning affects it. In this way, we are able to reduce energy use.'

- Coen van Oostrom, Founder and CEO of EDGE

BUILDINGS: SMART USE OF DATA TO CUT OPERATING COSTS

Daily use of houses, apartments, offices and commercial buildings accounts for a large portion of the world's total energy consumption. With current technologies and higher speeds, data can be collected and analysed to transform environmental performance and cut operating costs. Smart thermostats connected to machine learning algorithms can anticipate the likely building occupation and forecast data can then be used to better predict heating and cooling needs. Recent studies have estimated that building energy use could be cut by up to 20 per cent with the application of new technologies.

SMART CITIES: THE SUSTAINABLE WAY TO LIVE

Currently about half of the global population live in urban areas. By 2050 the UN expects this number to grow to over 80 per cent. With 78 per cent of the world's energy consumed by cities,[4] it's imperative to understand urban energy requirements and how technology and digitalisation can help monitor and reduce energy consumption. High-speed connectivity, cloud solutions, machine learning and AI are paving the way for the next phase of smart cities[5] by enabling real-time collection and analysis of data to inform city managers, including through the use of a 'digital twin'.[6] While the technology itself is not new, its use to manage city assets and resources is much more recent.

A local 'digital twin' is a virtual representation of a city's physical assets, processes and systems (such as street mapping and building heights) connected to real-time data collected by sensors all over the city. These need to be linked via high-speed networks to ensure frictionless transmission of large quantities of data. Using AI and machine learning algorithms, digital twins help to model scenarios that can be updated in real time as their physical equivalents change. It is a risk-free testing environment that increases the precision of long-term predictions and can support informed decision making to reduce energy consumption in areas such as transportation infrastructure.

Case study – Amsterdam

How a digital twin can make our cities smarter

The city of Amsterdam has spent 13 years developing and using smart solutions. There is already an impressive array of technologies in the mix – notably AI, robotics, big data and sensors to improve data coverage and gain insights into the state of the urban environment.

As part of its sustainability goals, Amsterdam wanted to stimulate electric mobility. The Smart Mobility programme 2019-2025 aims to deliver a cleaner, smarter and more accessible system of urban mobility. A key part of this is the provision of 'micro-mobility' modes of transport such as e-scooters and electric cargo bikes. Another is a string of eHUBS - offering clean electric, shared mobility options in different neighbourhoods. Research suggests that a switch from conventional cars to e-scooters would result in five times less CO2 grams equivalent per person per kilometre. To assist with peak load management on the electricity grid, a FlexPower project uses surplus renewable energy for the fast charging of Electric Vehicles (EVs) by matching supply with demand. When the energy load on the grid is high, the EV will be charged more slowly, drawing less energy.

ENERGY: THE SMART GRID IS COMING

One of the challenges of using more renewable energy is being able to match demand with supply in real time. Too often, an unwanted oversupply of energy is fed into the grid. Faster data transmission capabilities through gigabit connectivity could significantly transform the energy network by allowing instant responses to changes in energy usage. A smart grid allows communication between providers and consumers, minimizing differences in supply and demand through controls, computers, automation, and network equipment.

Faster data transmission can also help providers to manage renewable energy allocation. For example, by integrating weather

forecast data into predictive models of energy production, grids can better anticipate how much energy may be generated from renewable sources and how much will need to be drawn from non-renewable sources. The ability to better anticipate energy demand and store energy as needed are two key elements for tipping the balance in favour of renewable energy.

MANUFACTURING: REDUCING ENVIRONMENTAL FOOTPRINT

Manufacturing companies have long relied on technology and digitalisation to increase production while reducing operating costs. Factory operators use smart connected sensors together with machine learning and AI to analyse and act on production events remotely, in real time. What companies are now exploring is the potential to cut the environmental footprint of their operations.

Case study – Nestlé

Augmented reality provides site support and cuts travel

A central team at Nestlé began using intensified reality technology during the COVID-19 pandemic to connect remotely to production shop floors, research and development sites, and suppliers. Using smart glasses, 360-degree cameras, and 3D software, specialists are able to provide support on complex tasks without needing to travel long distances to sites. The technology also allows teams to be more efficient by supporting multiple projects at the same time, while contributing to the 2050 net zero strategy of the company. Augmented reality is both increasing speed and efficiency in facilities and reducing plane travel between Nestlé sites.

AGRICULTURE: BETTER MONITORING, MORE AUTOMATION

The agricultural sector is in the eye of the climate storm over the greenhouse gas emissions arising from its practices. The good news is that it is fast discovering the transformative potential of the internet of things, cloud technologies and AI, all of which are enabled by gigabit connectivity. Technological solutions can now help the agricultural industry turn itself into a more sustainable sector through better monitoring of fields and the automation of processes.

Examples of such solutions include the use of devices to monitor humidity, acidification, and nutrients in soils, and the use of drones to identify weeds in fields. This is significant because farming, grazing and storage practices release methane and nitrous oxide, two powerful greenhouse gases. The agricultural sector is responsible for between 12 and 14 per cent of total greenhouse gas emissions.[7]

The increased and repetitive use of fertilisers and pesticides in modern crop agriculture is responsible for considerable greenhouse gas emissions, through both their production and use. It also leads to environmental problems including biodiversity loss, terrestrial acidification, loss of soil organic matter, salinization, and the accelerated erosion of soils.

GREENING THE TELECOMMUNICATIONS SECTOR

In the telecoms sector, energy use accounts for the biggest part of greenhouse emissions. The speed achieved by gigabit connectivity in recent years has enabled a new range of digital services such as video streaming, video conferencing, online gaming, and social networks. The multitude of possibilities enabled by new digital solutions is feeding an ever-growing demand for connectivity. Network providers have worked to develop a more energy efficient infrastructure to handle increased bandwidth, while also expanding the network to connect more households and businesses.

A study by the Science Based Targets initiative, together with the ITU, GSMA and GeSI showed that the sector was able to meet growing capacity demand through technological advancement and the purchase of renewable electricity.[8] However, as new technologies continue to increase in both size and complexity, more initiatives will be required.[9] Telecoms operators are already addressing such challenges as they upgrade fixed and mobile networks. Virtualisation technologies will play a key role in the process. These enable a network to respond to demand by instantaneously creating the required functionality where and when it is needed. The process uses generic, physical devices which can fulfil multiple roles and thereby reduce energy consumption and use of resources. To some extent, physical devices (that consume energy) can be replaced with software.

FIXED NETWORKS: VIRTUALISATION AND A NEW TRANSMISSION STANDARD

The next generation of hybrid fibre and coaxial equipment will enable higher bandwidth and data transmission while reusing most of the existing network infrastructure, with only a limited increase in energy. Virtualisation will entail full digitisation of the distribution network and migration to a new data transmission standard on the final segment of the network, to increase capacity to multiple Gbps. This also provides the pathway to the next generation. Speeds of up to 10 Gbps could become a reality in the near future through upgrading existing infrastructure. This process extends the life of the network, reducing waste and avoiding large-scale environmental disruption during deployment.

MOBILE NETWORKS: THE EFFICIENCY OF 5G

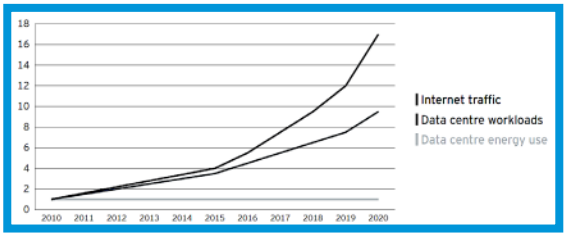
The next generation mobile network infrastructure, 5G, could result in an 85 per cent reduction in CO2 emissions per gigabit by 2030, compared to today's 2G-4G mobile networks, as it is able to transfer a significantly higher amount of data with the same amount of energy.[10] Beamforming, or directional antennas, will create a more efficient use of the infrastructure and significantly improve the

quality of service.

Other initiatives include the use of new cooling methods such as free air cooling, suppressing redundant energy intensive functions (e.g. lighting in server rooms) and updating power supplies so that they are more energy efficient.

Some companies have managed to keep their network's energy consumption steady over the last decade despite data communication growth. This is due to fixed network rationalisation and the migration of mobile network equipment to next generation upgrades. Other network operators like Telefónica have maintained their energy efficiency by switching off 3G and legacy infrastructure and powering a smaller part of the network. This has been combined with the deployment of power-saving features in the access network, equipment modernisation and the implementation of renewable energy plans.

FIGURE 1: DATA CENTRES AND DATA TRANSMISSION NETWORKS



Source: IEA

DATA CENTRES: MINIMISING THE IMPACT OF EVER-INCREASING DEMAND

Data centres are the 'factories of the digital world' and are under scrutiny for their energy consumption. As a fully connected and automated world becomes reality, limiting their environmental impact will be key. The workload of data centres has risen significantly in the last decade in tandem with internet traffic. This trend will continue with the increased use of applications like augmented and virtual reality, blockchain, crypto currencies and the internet of things. Data centres and other technical facilities need to maintain stable low temperatures to achieve peak performance, and this requires the constant consumption of energy.

Data centres and telecommunications networks account for a large part of the energy consumed by the internet. Information on the current trajectory of their energy use shows these have managed to keep their power usage flat over the last decade, despite the significant increase in data traffic.

THE VALUE OF GIGABIT

Gigabit connectivity enables real-time data analytics which in turn make it possible for carbon-intensive sectors to adjust their activities. Emissions are reduced through lowering production input and increasing the efficiency of the resources used. In most cases, normal connectivity would have been insufficient to drive the change. Very high-capacity networks, such as 5G, are a minimum requirement to unlock the use of sensors and big data in smart cities. Another key element is the matching of supply and demand, such as using the data produced through EV charging to maximise the use of available renewable energy.

Perhaps the biggest positive impact of such initiatives to date has been seen in building management. Here it was shown that smart solutions can render impressive results – saving up to 30 per cent of energy consumed in older buildings, and 10 per cent in new ones. At the same time, the study has shown the big strides being taken in telecommunications to ensure that, even with increased data traffic, switching to renewable energy and modern cooling technologies is boosting the energy efficiency of networks. However, the studies do show that a more complete framework and methodology is needed to measure the positive contributions of enabling effects, while also taking the environmental footprint of the telecoms sector itself into account.

In absolute values, estimates have shown that 5G could be 85-90 per cent more energy efficient than previous mobile technologies. Additionally, the increased use of virtualisation will make the networks smarter and more efficient. Components can be used for several purposes, limiting both energy usage and waste.

What impact might network upgrades have on an operator's greenhouse gas emissions? If the amount of data traffic increases further, could this impact future emissions due to the higher future energy use?

As we march towards a fully connected and automated world, the volume of data that will be generated is expected to increase significantly. Some sources expect it to triple by 2025, while others estimate the potential increase in data traffic could be up to 1,000 times.

Such a rise may have multiple and unintended causes, most likely related to changes in human behaviour. Rebound effects[11] may be short or long term, so are hard to fully estimate.[12] Moreover, research findings in this area differ. So far, the telecoms sector has proved able to keep its growth in energy use small, or even decreasing, while bandwidth has simultaneously and exponentially increased.

It seems probable that efficiency gains in infrastructure stemming from environmental initiatives and technological innovations could keep energy consumption at a constant level, even with the current increase in data traffic.

MOLLY BRUCE *is Vice-President, Corporate Responsibility at Liberty Global.*

The full report, 'Connecting a sustainable future, the power of Gigabit connectivity' can be downloaded at libertyglobal.com/wp-content/uploads/2022/06/Connecting-a-sustainable-future-report-June-2022.pdf

REFERENCES bit.ly/3AR1swX **1** IEA (2021). Emissions by sector. **2** GSMA and Carbon Trust (2019). The Enablement Effect – The impact of mobile communications technologies on carbon emission reductions. **3** Zhang X et al. (2022). How ICT can contribute to realize asustainable society in the future: a CGE approach. Environment, Development and Sustainability, **4** UN Habitat (2018). International Conference on Climate Change and Cities. bit.ly/3F85IKT **5** European Commission, 'defined as a place where traditional networks and services are made more efficient with the use of digital solutions for the benefit of its inhabitants and business.' **6** A virtual representation of a physical system or process. **7** Ritchie H et al (2020). Emissions by Sector. Our World in Data, 11 May. **8** GeSi stands for Global e-sustainability initiative **9** ITU et al. (2020). Guidance for ICT Companies Setting Science Based Targets. **10** Bieser J et al. (2020). Next generation mobile networks – problem or opportunity for climate protection? October. **11** Increased consumption resulting from actions that improve efficiency and reduce consumer costs. **12** GeSI (2017). ICT Sector Guidance built on the GHG Protocol Product Life Cycle Accounting and Reporting Standard. 21 July.

Events Calendar

International Institute of Communications

Events form the backbone of the IIC and take place throughout the year and around the world. They give members and non-members the chance to meet in a neutral environment, form informal bonds and explore solutions to policy and regulatory issues.

Washington DC Telecommunications & Media Forum 2022

Tuesday 13 - Wednesday 14 September 2022

This year's discussion themes will include:

- Updates from US Government – national and international priorities
- Broadband 'everywhere' rollout – supply and demand perspectives
- Artificial intelligence and machine learning – in pursuit of good governance
- Content & digital entertainment in global markets
- Tech & sustainability – balancing green and digital transformation
- Multilateral and bilateral cooperation on tech policy, regulation and supply chain

Asia Telecommunications & Media Forum 2023, Phnom Penh, Cambodia

Kindly hosted by The Telecommunication Regulator of Cambodia (TRC)

Tuesday 14 February 2023 - Regional Regulators Forum (RRF)
Wednesday 15 and Thursday 16 February 2023 - Telecommunications and Media Forum (TMF)

Further details will be available soon.

Brussels Telecommunications & Media Forum 2023

Kindly hosted by The Belgian Institute for Postal Services and Telecommunications (BIPT)

Wednesday 22 - Thursday 23 March 2023

Further details will be available soon.

Annual LatAm & Caribbean Telecommunications & Media Forum 2023, Miami

May 2023 (TBC)

Communications Policy & Regulation Week 2023, Cologne, Germany

Kindly hosted by Bundesnetzagentur (BNetzA)

16-19 October 2023

enquiries@iicom.org

Further IIC events, including IIC Chapter events, can be found at iicom.org/events/

INTERNATIONAL INSTITUTE OF COMMUNICATIONS

Inter MEDIA

Annual subscription £175

Online: www.iicom.org

International Institute of Communications
Suite 107, 143 Kingston Road, London, SW19 1LJ
United Kingdom
Tel **+44 (0)20 8772 4824** | Email **enquiries@iicom.org**