SHAPE OF THINGS TO COME

How should policy and regulation adapt to times of rapidly changing convergence? **JEAN-JACQUES SAHEL** shapes the discussion

Being actively involved in many activities of the International Institute of Communications (IIC), I have been able to get a feel for the underlying shifts, patterns of evolution and concerns common to the sometimes very different themes explored in our workshops and conference sessions. One underlying question raised regularly is the role of the regulator. Beyond IIC circles, where regulators have long occupied a central role in our international regulators forums (IRFs), there seems to have been an intensification of late in the discussions on their role.

It is no wonder that the role of regulator in the TMT/ICT sectors has come more to the fore in recent discussions, in light of the enormous impact of the internet around the world. It fuels much of our economies, and harnessing its power is a key objective for many governments. Take this statement delivered at a recent IIC UK chapter event:[1]

"It is now obvious to most that 'digitising' the UK is a must, both for consumers and for other end users like government and industry: UK GDP and productivity stand to gain tremendously if the nation can embrace digital technologies. Businesses need to be able to thrive in this environment, all end users should be able to enjoy more and better services, and engaged, digitally literate and active consumers are both the trend and a necessity in that successful vision of the future."

For those regulators whose remit covers the ICT sector, this has translated into a significant focus on convergence, and the intertwining of the various sectors it encompasses – a growing phenomenon which the IIC has been dealing with for several decades, in fact. As was raised recently at an IIC event on the European Union's flagship digital single market initiative:[2]

"It is the first time that the EU has a truly holistic approach to the 'convergence industries', and that all of these in turn have indeed, at last, converged:

broadcasters like publishers are now increasingly active, if not dependent, on their online activities. Telcos' future is now intricately intertwined with the continued growth and stability of the internet – and almost all of them have advanced online and content strategies. As for internet companies, they are of course still active in their 'own' field (if there is such thing as an 'internet-only' field) but also across other sectors, either directly or as intermediaries and platforms."

EXPANDING THE ROLE, OR DOING IT DIFFERENTLY?

Many of the recent discussions on the evolving role of the regulator have tended to focus on whether to extend their scope to cover a broader market than originally contained in their remit. But some analysts are already asking whether we should do exactly the opposite and narrow the scope of sector specific regulation to network access bottlenecks only (see Brian Williamson's article on page 22).[3]

But instead of how much bigger the role and scope of the regulator should be, could the more important question be in what manner policymakers and regulators should approach and conduct their mission? The response to ever-evolving markets, marked by merger or convergence, as well as the rapid evolution (or obsolescence) of products and sometimes business models and organisations, need not be primarily about scope of regulation. It may be about shape of regulation: how to do the job differently to achieve the desired outcomes of both a competitive and dynamic market situation – with market/economic and consumer/social benefits – and the appropriate respect for societal values more widely.

In positing a suitable future scenario, some of the key patterns that emerge from today's challenges are interesting, and may inform the appropriate future way to legislate, and then to implement legislation – which one might call the conduct of regulation.

A PLETHORA OF DILEMMAS

First, there is a need for balance. ICT policymaking and regulation seem to face increasing numbers of tensions between apparently exclusive propositions. An obvious one would be what some have described as the dilemma of privacy versus security.

In the most recent IIC UK discussion[4] we explored how:

"Policymakers and society more widely are faced on one hand with the need to fight complex and novel types of threats that (mis)use the internet for the benefit of either transnational criminal or terrorist groups to propagate their messages – eg. in encouraging radicalisation – or to directly cause harm – for instance through cyber-attacks, for extortion or for damaging critical infrastructure. On the other hand, there has been growing discomfort by citizens-users at having their online data not only used by others for monetary gains but also increasingly (many feel or perceive) monitored by security agencies."

Regulators seem to face an impossible choice, but must act to avoid potentially disastrous impact.

Regulators seem to face an impossible choice, and yet they need to act to avoid potentially disastrous impact. Indeed these trends:[5]

"...have created a climate in which the debate over data protection, privacy, security and surveillance is becomingly increasingly polarised. These security and anti-terrorist imperatives have given rise to various measures around the globe to promote the creation of 'local clouds', restrict data flows at the national or regional level, or extend the 'long arm' of national law to cover the surveillance of personal data held outside the jurisdiction.

"This is an explosive mix. The world now faces the risk of internet fragmentation and very real conflicts between concerns for privacy and fundamental freedoms, and the often seemingly incompatible objectives of achieving network security and national security."

This apparent dilemma between privacy and security comes with a set of further dilemmas. Encryption is one, where companies like users are told at the same time, and often by the same authorities, that either encryption is good, or it should be banned. Both privacy and cybersecurity professionals have argued that it is essential to protect communications and data through encryption.[6] After the Snowden revelations in 2013, there was a huge debate and pressure on internet and communications companies to encrypt all data flows. Those cloud companies that had not encrypted their data exchanges were severely criticised.

Yet, in the past year or so a number of governments have raised the prospect of banning encryption, in order to facilitate the work of law enforcement, notably in the background of increasing terrorist threats, as this recent quote illustrates:[7]

"Messaging encryption, widely used by Islamist extremists to plan attacks, needs to be fought at international level, French Interior Minister Bernard Cazeneuve said."

A similar dilemma concerns the retention of data for law enforcement purposes versus data protection regulation. Underneath it all, there is a wider social question: how to balance two different and potentially conflicting types of security: on one hand personal security, which includes the security of user's personal communication and data, and on the other hand, collective security (which includes 'national security' but perhaps not only).

There are many other aspects which some pit as dilemmas in ICT discussions, such as the infamous 'competition versus investment'.

A PLETHORA OF REGULATORS

At the same time, convergence between various policy spheres and imperatives is mirrored in the complex family of regulatory agencies involved. Different regulators increasingly have related competence as they get to deal with similar actors. This is apparent in privacy and the 'market of data' as just one example, where privacy authorities, consumer protection and competition agencies and telecoms regulators (and others) have at least some competence and remit.

From the perspective of business, organisations such as internet service providers (ISPs) or registries that have to take down rogue websites or domains may be dealing with consumer protection authorities, trading standards authorities, or the police and other law enforcement agencies (which, under the UK's long-debated RIPA legislation for instance, would include some 250 different agencies – for the UK alone).[8]

It does not mean that converging (merging) the different regulators is the obvious step forward: one would rightly argue that each may have very specific know-how and perspective which need to be preserved and not diluted in a bigger structure. Data protection regulators, for example, have fundamental values to protect that are distinct from the economic focus of other types of regulator. There is also still a case for different technologies and different sub-markets within the broader converged ICT sector to be treated differently, and

by different regulators, as NERA notes:[9] *"...differences in technology may require different regulatory treatment to achieve a common objective."*

In the face of these dilemmas, how will policymakers decide? And who will implement the outcome: the law enforcement agencies, or the data protection agencies, or the telecoms regulator, or in some other cases, the audiovisual regulator? From the perspective of businesses concerned, how can they thrive or simply plan for the future if they can be forced to do something by one side of an administration, and fined for doing that very same thing by another side, because it could be seen to breach other, seemingly unrelated rules?

The answer, and even the framing of the question, should probably not be Manichean: we should be able to move from worrying about what seem like opposites to dealing with them together, in other words 'converging' the policy and regulatory approach to combine principles such as the respect for privacy and the protection of personal data, with the need to enable government authorities to protect national security interests. As pillars of the rule of law, they should (must) be mutually reinforcing, not opposites.

It is not simple of course, but balancing different perspectives is not a new aspect of policymaking. It may be a skill to develop further for some regulators more used to traditional black and white rules, together with mainstreaming collaborative ways of working with other regulators. And who said the job of regulators would be simple?

Mainstreaming and strengthening collaboration between different regulators will likely need to be on a case-by-case basis, merging their efforts rather than their structures. Indeed, rather than adopt an ongoing inter-ministerial type of arrangement, it is likely that certain agencies would need to collaborate with certain other agencies only on certain topics and investigations. Methods of collaboration centred on project work will need to develop, embedding a way of doing things whereby when certain issues arise, the parties concerned know how to contact each other when they have related concerns and remit, and can quickly and easily put in place tried and tested mechanisms to discuss and handle the issue jointly.

INTEGRATING THE GLOBAL DIMENSION

The internet and the apps, services and content that flow over it are inherently cross-border, often global. Some voices have called for global legislative and regulatory frameworks to apply to ICTs including the internet. But can we genuinely envisage full, global regulatory convergence in the near future or indeed, in the next generation or two?

At national as at international level, simpler norms and legislations based on essential values are most likely to be acceptable to most or all, and best placed to cope with the fast pace of technological innovation.

The examples of the OECD's and APEC's privacy documents (APEC's is the Cross-Border Privacy Rules, CBPR) can be useful here. In 2013, the OECD published the first update of its 1980 privacy guidelines,[10] which had served as the first internationally agreed set of privacy principles. The update increased the text from 3 pages to 4. The rationale was to focus on core high-level principles which the 30+ countries of the OECD, across vastly different parts and cultures of the world, could agree on and detail in their respective national or sub-regional legislative frameworks. It provided enough commonality to allow for a viable, safe environment for transborder data flows, without making it so specific as not to be acceptable to a nation's particular conception of private life.

In telecoms, the situation was arguably the same when the World Trade Organisation (WTO) came up in 1993/94 with the Reference Paper on Basic Telecoms,[11] a 3-page document that summarised key regulatory principles which should be adhered to throughout the now vast WTO 'footprint', like independence of the regulator or non-discriminatory interconnection. Today, the reference paper arguably provides the common underpinning for most of the liberalised telecoms markets around the world.

"Regulators will ideally have an 'international by design' element in their policy."

Aiming to have a very detailed common legislative framework throughout the world is a long-term endeavour, if it is achievable at all. In the foreseeable future, for a global system that works we will probably need fairly simple, essential rules at global level – strong enough, but also broad enough that they can 'interoperate', coexist with local values, and do not end up imposing a particular geography's vision and cultural preferences on others.

It is a question of balance, this time between the global reality of the internet-driven environment we now live in, and the desire to have local values protected appropriately by a dedicated national or regional framework. National regulators will ideally have an 'international by design' element integrated into their future regulatory policy development process. The role of the international function within a regulator's structure will need to increase correspondingly, as will transborder cooperation processes.

TECHNOLOGY EVOLVES TOO FAST FOR LEGISLATION AND REGULATION

Another key trend has been the desire for law to 'catch up' with technology. The EU's telecoms framework is now in its third revision in 15 years – and that's not counting the several 'side-legislations' such as the Connected Continent package which impacts businesses and users in various ways. The trend is the same in privacy: no sooner has the 'Brussels bubble' agreed on the massive new General Data Protection Regulation (GDPR) then it starts reviewing the e-Privacy Directive. As technologies and uses continue to evolve, we are bound to hear further demands for yet more updates to the legislation.

While this never-ending development of legislation may benefit the jobs market – at least for Brussels-based lobbyists and the legal profession – one has to wonder whether it truly benefits the market and consumers/citizens. Businesses find it difficult to make long-term plans as legislation may change so often; they are often also confused by some of the new rules that are hastily concocted to protect against the latest scare; consumers may be confused as to exactly what rights they have; etc. We risk ending up conflating long-term essential values and needs with short term 'red flags' which can end up stifling innovation and consumer benefits.[12]

Here again, the OECD experience provides food for thought. Not only is it more realistic for international acceptance – and so more useful – to develop simple and short rules, but relying on essential principles rather than very detailed rules ensures long-term viability of the framework. The OECD privacy guidelines were revised only once in 33 years, and despite the massive market evolution and

technological progress that happened in that period, the update only added a short number of sections to the text.

Whether it be at global, regional or national level, legislation that remains short, based on essential principles and values, is far more likely to stand the test of time than often updated, rushed, confusing detailed rules based on the latest scare or craze.

NEED FOR ACCOUNTABILITY

The next step in that scenario is to rely more and more on those implementing the legislation to interpret these long-term rules on the latest cases and concerns brought about by the latest technology. Even if we do not move (back) to devising long-term legislation that requires regular re-interpretation by regulators, the short-term fixes to the law which we are getting accustomed to will unavoidably create vagueness which only regulatory interpretation will be able to fill. In both cases, the regulator's role is bound to become more important, as they would be in charge both of implementing, but also increasingly updating or clarifying, the interpretation of the law and how it should be applied as technology (and society) progresses.

With this renewed importance and responsibility, the regulator would need to balance many perspectives, and work more with other regulators (nationally, with other agencies dealing with similar markets from other perspectives, as well as internationally) and also involve stakeholders across the board as a matter of routine.

This direct involvement of others in evolving policy or interpretation of the law will become more crucial as the importance of the regulator grows: the validity and legitimacy of its role will need to be covered by reinforced accountability to stakeholders – across business, the technical community, civil society and academia – including by their direct participation in developing regulatory policy. To ensure this increased power is exercised fairly and rooted in reality rather than in technocratic ivory towers, stakeholders' involvement should not be limited to responding to consultations, but instead stakeholders should be able to work genuinely together with the regulator and with other concerned parties in jointly analysing situations and coming up with consensus decisions.

This 'multi-stakeholder' way of working is not new, and is bound to intensify. It has proven its worth in many spheres already.[13] The IIC knows this well, since it has followed this model since the beginning: to have more fruitful, more robust, more future-oriented policy discussions, from the start the IIC brought together policy specialists not only from both the public and private sectors, but also from different industries, initially broadcasting and telecoms, and later from IT and the internet. Opening up to allow all relevant stakeholders – from business and academia to civil society and the technical community – to sit alongside public officials in the development of policy, then of legislation and then of the interpretation of how legislation should be applied, would deliver on several fronts:

- Deliver superior, more robust policy, legislative and regulatory frameworks
- Ensure the accountability of the regulatory machine
- Ensure stakeholder representation through open participation.

LEGISLATING FOR TOMORROW, REGULATING FOR NOW

In summary, the 'arms race' for legislation to be constantly updated to catch up with technology and convergence is simply not sustainable. A possible way forward is to create perennial legislative frameworks, which can stand the test of time. In that dynamic, which some might describe as simply a return to the original intention, regulators would have a newly increased role, not in scope but in responsibility. The way they work, and the importance of their work, is bound to grow. They would be the ones in charge of ensuring the continuous (re)interpretation of essential legal norms and values in the face of technological, market and social evolution.

Regulatory philosophy would need to shift accordingly. Nicolas Curien, former commissioner of French telecoms regulator Arcep, has inspired many audiences in recent years by comparing a regulator to a gardener:[14] *"...that does not try to take nature's place, but creates the right conditions for it to work; a gardener that prevents the emergence of an uncontrolled jungle without trying to design a French garden."* And so providing the right soil for this ecosystem to grow into an innovative, competitive market that delivers economic and social benefits.

> **Getting legislation constantly updated to catch up with technology is not sustainable.**

The regulators' job will likely be an almost constant 'balancing and combining' act, between sometimes apparently opposite elements, and with the global perspective always in mind. Restraint will be needed, yet regulators should have courage to act and/or send strong signals when necessary. Watchwords, if not overall institutional goals, should include innovation, user/consumer/citizen protection and choice, competition and the vibrancy of markets.

In this shifting way of working, regulators will need the ability to draw on and work directly with the range of stakeholders involved, across the public and the private spheres. Project teamwork and multi-stakeholder collaboration should be the norm, bringing at the same time a wealth of expertise, stakeholder representation and accountability.

When we look at the future of the internet and ICT, we should not be worried about the challenges, which we should be able to tackle while reaping potentially huge benefits. But we do have to work hard and through innovative approaches to reinterpret our fundamental values and norms for the reality of a transnational internet.

I look forward to expanding on these thoughts as we embark on a new programme of IIC discussions.

JEAN-JACQUES SAHEL *is chair of the UK chapter and board member of the IIC.*

REFERENCES **1** IIC UK Chapter. Future connectivity amid shifting economic and consumer demand. May 2016. bit.ly/2c7EV5P **2** IIC UK Chapter. EU Horizon for ICT policy. January 2016. bit.ly/2cszsSJ **3** Williamson B (2016). High-flown ideas. Intermedia 44: 22-26. **4** IIC UK Chapter event. Future policy approaches to the convergence of privacy and security. July 2016. bit.ly/2c5QISH **5** As noted in the context of IIC UK's February 2016 debate: 'Data protection, privacy and surveillance: Will cyber insecurity fundamentally change how we use the Internet?' **6** For an in-depth and 'different' look at encryption, see: Six times encryption made it to the movies. Mozilla blog, 11 July 2016. bit.ly/2cJCeDW **7** Vey J-B (2016). France says fight against messaging encryption needs worldwide initiative. Reuters, 11 August. reut.rs/2aR2z2V **8** Home Office (2015): Regulation of Investigatory Powers Act. Response to public consultation. bit.ly/2csIvpS **9** NERA (2016). A new regulatory framework for the digital ecosystem. pp8-9. **10** OECD (2013). Guidelines on the protection of privacy and transborder flows of personal data. bit.ly/2cU1wzM **11** WTO (1996). Negotiating group on basic telecommunications. Telecommunications services: reference paper. bit.ly/2cBVhnF **12** Rooney B (2011). The red flag act. Wall Street Journal, 27 June 27. on.wsj.com/2cU1hVi **13** Beside governments and regulators the OECD includes in its digital policy committee the business and industry, trade union, technical community and civil society advisory committees. See also Sahel J-J (2015). IANA transition: A catalyst for enhancing the multistakeholder approach. Digital Post 11 June. bit.ly/2ci7vm5 **14** Curien N (2011). Innovation and regulation serving the digital revolution. Journal of Regulation I-1.32: 572-578. bit.ly/2cU3fFs