GEARING UP FOR THE SPLINTERNET

Policy Papers on Technology, Economics and Structural Change 2023:2

Richard Allan

Comments by
Joakim Wernberg

ENTREPRENÖRSKAPS
FORUM

SWEDISH ENTREPRENEURSHIP FORUM

is the leading Swedish network organisation for initiating, conducting and communicating policy relevant research in the field of entrepreneurship, innovation, business dynamics and growth.

Swedish Entrepreneurship Forum is a network organisation with the aim:

- to serve as a bridge between the entrepreneurship research community and all agents active in development of new and small enterprises.
- to initiate and disseminate research relevant to policy in the fields of entrepreneurship, innovation and SME.
- to offer entrepreneurship researchers a forum for idea sharing, to build national and international networks in the field and to bridge the gap between research and practical application.

Swedish Entrepreneurship Forum is the founding organisation behind the most prestigious international research prize in the field, the Global Award for Entrepreneurship Research.

www.entreprenorskapsforum.se/en

SWEDISH ENTREPRENEURSHIP FORUM

POLICY PAPERS ON TECHNOLOGY, ECONOMICS AND STRUCTURAL CHANGE 2023:2

GEARING UP FOR THE SPLINTERNET

RICHARD ALLAN

1. INTRODUCTION

The internet has a profound impact on business and society around the world. Inevitably, a technology this powerful will be subject to geopolitical forces.

We can consider the evolving shape of the internet in terms of two types of forces that may act on its components, shaping the network to be more coherent or more splintered. CENTRIFUGAL (moving away from the centre) forces cause objects to fly apart, fragmenting the whole into separate splinters. CENTRIPETAL (seeking the centre) forces pull and hold objects in an orbiting motion, creating a unified coherent system.

Following a timeline of the development of the internet, we can identify factors that have been pulling it together as a single global communications network and factors that tend to force it apart into functionally separate networks.

2. YESTERDAY: A NEW PROTOCOL

We start by looking back to the origins of the internet to understand the intent and choices of those who developed the technology.

2.1 The foundations

Once upon a time, it was impossible for computers to talk to each other without significant expense and technical expertise. Most of the important and interesting computers were hosted in institutions, primarily universities, and researchers felt that they could be much more useful if there were some way to connect them permanently to each other.

Thus, a group of academics and engineers set out to develop a set of common protocols that would enable computers everywhere to communicate with each other. The foundational Internet Protocol (IP) offered computers a common way to send packets of data to each other reliably via a range of types of hardware and network cabling.

For a full account of these early stages of the development of the internet and the thinking of the key players, the book *Where Wizards Stay Up Late* by Katie Hafner is recommended.[1]

2.2 A common toolkit

Once this basic model of data exchange was established, a series of other protocols were adopted to provide useful functions for the users of these now-interconnected devices. For example, interoperable email systems were developed in the 1980s using protocols called SMTP, POP3, and IMAP to replace earlier proprietary email services that were tied to a single type of computer.[2]

These days, we take for granted our ability to access information from a wide range of services via a common interface, our web browser. However, this was not possible in the early days of the internet. The creation of standard ways to format information to make it readable by different computers in the form of the World Wide Web protocols, notably HTML, was an effort of the late 1980s and 1990s.[3]

All of these developments had a strongly centripetal effect, pulling more and more computer systems into a single technical sphere. This is not surprising given that the primary motivation for all of these developments was precisely to bring computers and services together in a common information system that had previously been split across separate spaces. The early proponents of the internet believed that a network of interconnected computers would open up opportunities for creativity and technical developments that would fundamentally differ from those offered by unconnected computers. The experience of the last few decades has demonstrated how much power lies in connection.

[1] Hafner, K. and Lyon, M. (1998). *Where Wizards Stay Up Late.* . https://katiehafner.com/books-new/where-wizards-stay-up-late/.

[2] For a history of email development, see https://en.wikipedia.org/wiki/History_of_email.

[3] For a history of the World Wide Web, see https://home.cern/science/computing/birth-web/short-history-web.

2.3 IP rules

The adoption of common standards sometimes occurred in spite of organisational policies that favoured other technologies as internet technologies were easier and cheaper to implement than formal international networking standards such as X.25. We now often now talk about 'network effects' in terms of how online services can grow to dominate a sector once they have enough people signed up, and we can see the adoption of the internet itself as one such network effect. Alternative systems were available, but you got more out of connecting to the internet once it had reached a critical mass of users.

Using IPs is so commonplace today that they are replacing older technologies in telecommunications company networks. This was not a given from the outset, and many telecom companies were dragged kicking and screaming into offering internet services that they saw as cannibalising their traditional sources of revenue.

Although the nodes in the networks were all located somewhere and the carriers of the network signals were companies with national or regional establishment, a remarkable feature of these new protocols was their lack of respect for borders. This created an important power shift as we moved from telecoms services that were very much rooted in a nation-state, publicly owned or private but dependent on government-issued licenses, to internet services outside of local control.

2.4 Global governance

At the heart of these protocols is an addressing structure that ignores physical location: each address is a unique set of numbers that can be assigned to a device anywhere in the world. The only absolute requirement is that everyone agrees on which device the address belongs to so that data can be correctly routed to it.

A system of regional entities was set up to handle the allocation of unique addresses to the various entities wanting to use them, but this was an administrative convenience rather than because the technology conformed to geography. A pseudo-geographical layer was added with the development of the Domain Name System (DNS), which allows users to refer to services using names rather than their IP addresses. The domain contains a national element—for example, ".se" for Sweden and ".uk" for the United Kingdom—but it is not a given that a service with a national label is actually located in a particular country as many registries do not require this. For instance, the Pacific island nation of Tuvalu (with a population of around 12,000 people) gains significant revenue from over 90,000 registrations of ".tv" domains, often by global media companies. Similarly, more than 230,000 ".nu" domains are registered by companies who wish to appear "new" (as per the

Swedish translation, "now"), despite being entirely unrelated to the 2,000 residents of Niue, which has the right to this suffix.[4]

The bodies that maintain the protocols and infrastructure of the internet are proudly non-governmental and most commonly organise along regional and global lines rather than being interested in individual countries. The core body defining technical standards, the Internet Engineering Task Force (IETF), works by issuing Requests for Comments (RFCs) inviting any interested person to contribute to the development of protocols. In true IETF fashion, the body defined its own mission and processes in 2004 by issuing an RFC (n. 3935), which states clearly and simply that "[t]he goal of the IETF is to make the Internet work better."[5] The IETF was established as a private corporation that answers to a global civil society organisation called the Internet Society. Various attempts have been made to link internet governance to intergovernmental structures, most notably through the UN-sponsored Internet Governance Forum, but the internet remains a world where national governments have little direct sway.[6] This operation outside of direct government control has been a strength from a technical point of view, creating positive conditions for innovation, but is a weakness from a geopolitical perspective. The fact that the internet infrastructure is largely owned and managed by private corporations can mean that accountability mechanisms are relatively weak. Although these are not entirely absent as companies have legal personalities and obligations, governments can and do argue that more direct accountability is needed, especially when key companies are outside their jurisdiction.

2.5 Global business

The impact of the internet on businesses has been felt in three main areas: a global customer base, lower barriers to entry, and a trend towards more rapid change. As more people have come online, they provide an ever larger potential customer base for internet-enabled businesses, with the default mode enabling easy connection to customers anywhere in the world. The ability to reach these customers varies according to the type of business—for example, those delivering physical goods and onsite services face different challenges from those delivering entirely digital products—but the potential pool is likely to be larger and more widely distributed than pre internet.

[4] For ".tv" domain registrations, see https://zonefiles.io/list/tv/. For ".nu" domain registrations, see https://zonefiles.io/list/nu/.

[5] IETF RFC 3935, 2004. https://datatracker.ietf.org/doc/rfc3935/.

[6] https://www.intgovforum.org/en.

There can be significant technical and cost challenges to setting up shop online, but these have been falling dramatically over time such that it is now possible to buy cheap off-the-shelf packages to set up an online business. These packages have evolved with the development of software-as-a-service (SaaS) models, which allow users to rent at a reasonable cost highly sophisticated tools such as specialised custom servers and machine-learning models, which were previously only available to a few big businesses. This again varies according to the type of service, but the trend is clearly towards lower barriers to entry for creating and running most kinds of business. This lowering of barriers to entry can happen across a host of areas, from a cheaper 'shopfront', through more cost-effective marketing and to lower administrative costs thanks to cloud services for banking, accounting, or office applications, among others.

A more equivocal shift that the internet brings about is in the speed of change which it enables as a result of both technological developments and shifts in markets as more people join the network. This can provide considerable opportunities for businesses offering a valuable service with the right technology and capable of keeping up with trends, but it can also be massively disruptive, threatening established business models as well as new ones.

Several aspects of these economic shifts are of concern to governments. The first is the turn from established pre-internet businesses to these new platforms and services. Sectors such as telecommunications, media and retail are seeing profound changes in value as new internet-based services provide alternatives to the products they have offered for years. These are sectors that typically employ a large staff and have significant political influence, which they naturally use to raise concerns about whether the transition benefits society overall.

The second aspect is the dynamics between internet services themselves as there may be concerns about market concentration and dominance of particular sectors by a few large platforms. This debate often contains a global trade element when local internet businesses feel that they are treated unfairly by global players headquartered in other jurisdictions. These concerns are evident in the competition case brought by the European Commission against Apple following complaints by Spotify.[7]

Third, the fact that barriers to entry have been lowered for everyone has created new opportunities for illegal activity as well as legitimate enterprises. For most people most of the time, using the internet is a safe activity, but new risks certainly exist,

[7] European Commission case AT.40437, Apple App Store Practices (music streaming). https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_AT_40437.

which people have to watch out for, such as emails and messages from fraudsters and abuse of personal information. Much like when navigating any city, although the main public areas are well maintained, a certain amount of "street smarts" are needed that come from familiarity with the space. Additionally, some people have used internet technology to create spaces outside the mainstream with the express intent of enabling criminal activity – the so-called "darknet". Governments are concerned with both aspects: ensuring that the main streets are safe enough for their citizens and limiting the scope for criminal threats to emerge from unpoliced spaces.

All these elements have contributed to the increasing interest of national governments in reasserting control, which we examine next.

3. TODAY: THE EMPIRES STRIKE BACK

As we have moved our engagements as customers and businesses onto a network whose architecture is by default global and designed to disregard geography, the new digital world has created both winners and losers.

The winners are those who can thrive in this environment, with much attention paid to those who have been able to develop the massive global online services that most of us use daily. It is tempting to see this as a settled situation based on the current winners, but we should also note that services can fade away over time, as the names Altavista, Myspace, and Yahoo! remind us. They were each eclipsed by newcomers, and innovative platforms continue to spring up that may take on the leadership mantle from incumbents. This is often presented as a shift in power from governments to these large platforms, but it remains a fact that corporations are established through and bound by laws that are determined by political leaders.

Increasingly, political leaders in all kinds of systems and along the ideological spectrum express their interest in asserting control over both local and global corporations. We may see this as an instinctive play by politicians who are determined not to cede control to others in areas that are important to their societies—a classic struggle between competing entities over who gets to wield power. The scale and complexity of online services mean that politicians may seek to exert indirect as well as direct control, which can create additional challenges. Regulations may require platforms to make specific decisions—for example, about whether content must be restricted to comply with the EU's 'Right to be Forgotten', and this is experienced by users as the platforms having more rather than less power even though they are responding to a government mandate.[8]

[8] For an explanation of the EU Right to be Forgotten, see https://gdpr.eu/right-to-be-forgotten/.

Nonetheless, we should also recognise that in many cases, individuals ask their politicians to take greater control in response to material harms that they believe they are suffering and are not being fixed by the current power brokers of the internet. Bad behavior by users is a phenomenon that drives regulation.

Most politicians see their primary duty as to protect people in the regions and countries they govern. There can be widely differing views about the policies that would best protect people hence, there can be very hostile partisan divides, but the common thread that connects politicians is the belief that the policies they advocate will benefit people. The feeling that 'nothing can be done' to deal with online challenges is therefore a source of considerable frustration for politicians across the political spectrum. This feeling is turbo-charged when the reasons for the inability to act stem from the fact that online service providers are private companies that are outside of the politicians' jurisdiction. The frustration is often expressed in language that compares the internet with the 'Wild West'[9] The assumption is that services are lawless because local law cannot be applied even if the companies are subject to a whole raft of legal obligations in their home jurisdictions.

We can walk through a non-exhaustive list of areas in which this dynamic of demand for political intervention is unfolding. These are the centrifugal forces that push us away from a single sphere as national governments look to control their splinter of the internet.

3.1 Intellectual property

One of the earliest areas in which governments were asked to intervene was the enforcement of intellectual property rights. As content such as music and movies was digitised and the internet provided a cheap data-transfer capability, the barriers to transferring content to other people fell.

There was a significant movement of people in the internet space who believed that the public interest lay in the widest possible distribution of content, whether protected by copyright or not. The legal owners of content, unsurprisingly, felt that just because their property could now be transferred more easily did not mean that this should be done without their permission and appropriate compensation.

The difference of opinion between content owners and some sections of the internet-using population survives to this day, but governments have largely sided with content owners, and the trend has been towards tightening and extending copyright law as it applies to online services. A legitimate business aiming to

[9] The Huffington Post (2018). "MP Matt Hancock Demands More Control Of 'Wild West Free-For-All' Internet Companies", March 22. https://www.huffingtonpost.co.uk/entry/matt-hancock-data_uk_5ab3659ae4b0decad046ca7a.

become a serious player at scale and that needs copyrighted content thus has no choice but to negotiate with the relevant licensing bodies and pay the required fees.

In many cases, this necessitates country-by-country licensing, and enforcement action against any breaches typically falls to national courts, in line with local laws and policy. Consequently, this is also part of a broader geopolitical debate about respect for intellectual property rights that plays out in bodies such as the World Intellectual Property Organisation.

3.2 Law enforcement

A priority for any government is to be able to identify and prosecute people who are suspected of committing serious crimes. Longstanding arrangements are in place in most countries for the authorities to request information from local businesses with appropriate legal safeguards, but these do not typically apply to entities outside of the country.

A major driving force of moves to bring services into jurisdictional scope is this need to secure access to data when residents of a country commonly use foreign services. This push is especially fueled by cases in which serious crimes have been committed, triggering public outrage, but the lack of data is complicating the work of investigators.

The pressure may also be acute when an ongoing threat (e.g., from terrorists) needs to be monitored but the intelligence is not coming through. There is scope for conflicts of laws here as one country requires data to be collected and disclosed while another forbids it. In these cases, companies have had to decide whose law to respect and whose to defy, with the winner generally being the law of the country hosting their headquarters.

3.3 Speech

Standards for what constitutes legal and illegal speech vary widely from country to country. Something close to a global consensus has been reached in a few areas (e.g., in relation to the worst kinds of child-abuse imagery), but significant divergence remains in many others (e.g., on the issue of whether blasphemy should be illegal).

Because these can be highly contentious and emotive issues for people in a country, politicians are under pressure to ensure that local standards are upheld even when people are using global services. These concerns may be compounded when services are 'foreign' and seen as operating on standards that differ from local norms. This is a driving force for many of the current legislative proposals that aim to regulate social media, for which the common rallying cry is that governments rather than private companies should set the standards (whether making them more restrictive or more permissive).

While governments want to be able to set the standards for speech online, the scale of online activity is such that they do not realistically have the capacity to enforce these. This has led to the adoption of legislation like the Network Enforcement Act in Germany, which requires platforms to enforce German legal standards. The rules are set by the state, but private companies act as judge and jury.[10] This model of private enforcement of public law is criticised but is found in an increasing number of legal instruments in the absence of any realistic alternative. Policymakers know that their court systems simply could not assess content at the speed and on the scale required if they were to take this role away from platforms.

There are particular sensitivities around political speech and suggestions that services are operating in a biased or partisan way. These criticisms often come from both the left and right of the political spectrum as each side feels that it is being discriminated against. Politicians may become very personally invested in trying to shape the rules of internet services because they see these as materially affecting their fortunes. This can cut both ways, with some believing that service providers are too permissive and others that they are too restrictive of certain types of speech. Questions exist about the rules themselves and about their enforcement. Do restrictions on hate speech have a disproportionate effect on people raising questions about immigration and multiculturalism? Do variations in how content is reported mean that there is stricter enforcement against some groups than others?

There are concerns that any biases could become even more significant if regulation 'bakes in' specific rules and processes as a requirement for all platforms. This could potentially remove the scope for some platforms to take a deliberate stance of being more permissive of speech that other platforms might reject. In the future, we may see concerns about biases shift from being directed at platforms to being aimed at regulators as platforms claim to be acting under instruction rather than at their own discretion.

In many cases, there will be very broad public support for governments regulating this area when people feel that service providers are unaccountable, especially in the context of high-profile instances of 'bad' decision-making by platforms. There may be concerns about governments stepping in if they are also seen as untrustworthy, in a democracy, the government and its representatives are at least more directly accountable for any mistakes they make.

[10] German Network Enforcement Act. https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html.

A common criticism of moves towards more explicit speech regulation is that the same legal tools would be extremely harmful in the hands of a less democratic regime. These are legitimate concerns but are unlikely to win political arguments. A country that has strong freedom of expression obligations in its constitution and is willing to comply with the rulings of bodies like the European Court of Human Rights will argue that it can be trusted to regulate speech precisely because of these constraints.

3.4 Finance

The original spirit of the internet as a radical force that would cause positive disruption to established business and societal models has been taken up recently by promoters of new financial products and services. Evangelists for these products often echo the language used by champions of the internet as a force bypassing traditional governments. This sentiment was captured by John Perry Barlow in his "Declaration of Independence of Cyberspace": "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of 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."[11]

These new financial products are bundled under the banner of crypto-assets and decentralised finance as tools that will liberate people from services that have traditionally been tightly regulated and controlled by nation-states. We are still in the midst of this debate, but the direction points strongly towards national governments reasserting control and creating a raft of new regulations. Governments have been progressively tightening up the rules for traditional financial services to combat money laundering and tax evasion, and the last thing they want is for these to be displaced to a new unregulated space.

The control of money is a major concern for any government, but we should not overlook the protection of citizen interests as a genuine motivation for regulation. As the pool of investors has expanded dramatically, there are many potential losers from any drop in market value. Some people may accept losses as a fact of life, but others will turn to their governments, asking them to do more to protect people and avoid future losses.

Some of the state's significant interests may also be at risk, as well as those of individual citizens. Some of these are systemic, but others are more immediate, such as the risk that new channels are being created for money laundering.

[11] "Declaration of Independence of Cyberspace." https://www.eff.org/cyberspace-independence.

The founding rationale for the development of technologies like Bitcoin was that it would create a common, borderless sphere for people to exchange value. This is consistent with the early philosophy of the internet itself and has wide appeal in the technical community. However, this is challenged by pressures steering us back towards nationally organised and regulated stores of value, whether these are maintained as traditional currencies or in the form of digital tokens.

In the case of finance, there has been a rapid shift from the 'Wild West' of these technologies' development and adoption towards a more regulated model. This reflects the critical importance of money compared to other areas such as speech, where the regulation has taken longer to catch up with reality.

4. TOMORROW: RETURN OF THE INTERMEDIARIES

As the trend moves towards more national government intervention, the effects on business are likely to limit the opportunities that the internet offers, namely, a global customer base, lower barriers to entry, and a trend towards more rapid change. Rather than being by default open to a global customer base, service providers may be more inclined to open up market by market, using technology to restrict access to customers in new countries until they understand the full legal and cost implications.

Any geographical restrictions will necessarily be imperfect as there is no foolproof way to know the location of a user connecting with an internet service. It is common today for people to seek access to locally licensed content like TV and movies by using technology that makes them appear to be connecting from a permitted location. We may move to a world where some people have tools to access a much wider range of services than those with a simple internet connection that is linked to one location. Resource-rich users will thus have the online equivalent of a private jet that can transport them anywhere in the virtual world whenever they fancy.

As well as absolute barriers to access based on geography, there may be restrictions on specific features, making the various national versions of a service more or less attractive. This is visible today in the different catalogues of content that are offered by Netflix depending on the country in which it believes the user to be located when they access it. The bigger the gap in functionality between different national portals, the stronger the incentive for people to want to choose an alternative location if they are stuck with a low-powered version in their country.

New barriers to entry may emerge as regulation requires certain things to be put in place before a service can be offered, which can be technically and financially material—for example, if you have to rent local data centre space separately for each country. From a financial perspective, this may encourage service providers to spend more time building a revenue base in their home market before opening up to other countries. While this may previously have been cost free as a single hosting provider could accept connections from anywhere, an active decision to pay for additional hosting services for new markets will now have to be made.

By nature, the regulation of technology tends to slow down innovation not because that is the intent of the lawmakers but simply because it captures the state of play at a particular moment in time. A different kind of innovation may emerge as people try to develop products that circumvent the regulated space, but within it, developments are likely to be slower. There is a complex array of forces at play in the relationship between technology and innovation, which the UK government summarises in its 2020 paper "Regulatory types and their impacts on innovation: a taxonomy."[12]

A rational response to this new environment is for businesses to reduce their own compliance complexity by having others take on this task for them. This is where we may see a very profound unintended consequence of regulation.

One of the great promises of the internet was that it would 'disintermediate' a range of activities, allowing people and organisations to connect directly with each other in ways that were previously impossible. Yet, we have seen phenomenal growth in new forms of intermediaries, such as search engines, social media, and e-commerce platforms, and regulatory trends may steer us yet further in this direction.

A critical difference with the new intermediaries is that they share the characteristics of other internet businesses in terms of operating at a massive scale, globally rather than nationally, and at a low cost. This contrasts with the old world, where intermediaries were commonly limited to one or a small number of countries and only enabled access to relatively small numbers of players for relatively high prices. If we think of an independent media production house trying to get their content out, there are now many video distribution platforms they can use rather than being limited to negotiating deals with a small group of television broadcasters.

In practice, the new intermediaries offer many of the benefits that were the goal of European single-market legislation. While the EU previously sought to create a pan-EU market for video content by imposing quotas on each national broadcaster, we now see intermediaries making much more content from every member state available across the region.

[12] UK Department for Business Energy and Industrial Strategy (2020), research paper. https://www.gov.uk/government/publications/regulatory-types-and-their-impacts-on-innovation-a-taxonomy

4.1 Interpersonal communications

The archetypal interpersonal communication system that the internet brought us was email. All you needed to do was install email servers and clients built to the relevant open standards and you could happily message away. For a number of years, this worked well, and the centripetal force of the common standards brought millions into the network. However, over time, we have seen significant shifts both in how email itself works and in terms of people moving to alternative modes of communication, notably interpersonal messaging systems.

The primary force effecting these changes has not been regulation but rather bad behaviour. The very open nature and low cost of email meant that it supported business models based on sending irrelevant and unwanted communications at scale. Email continues to be a widely used tool in spite of the fact that around 85 percent of all email is spam, but it is only useful because filtering technology has been introduced. In an effort to raise the barriers against spammers, additional protocols have been added that aim to sort out trusted and untrustworthy sources of email.

The effect has been to steer people towards large email services such as those offered by Google, Microsoft, and Amazon, as well as many large web hosting services. Businesses wanting to have their email delivered on the same day are likely to use the underlying engine of one of these big providers. While they can still technically set up their own email server, they may find that their emails are filtered out, making the server useless.

As well as email converging towards large, verified server platforms, a significant substitution effect has led people to use tools other than email for interpersonal communications. The switch to mobile has contributed to this shift as messaging apps are more nicely integrated into phones than email clients. This has been a splintering issue, with users moving from a unified interconnected system—email—to disparate unconnected systems such as iMessage, WhatsApp, and WeChat.

There are now moves to force these separate services to interconnect, bringing us into an entirely new sphere. We are moving from an open unified system developed by technologists (email) through a phase when people have chosen to use more closed systems (WhatsApp, etc.) and into one when regulation will try to force the closed systems to interconnect so as to create a new unified network. Significant technical doubts exist about how this new interoperability may work in practice, but it seems likely in all scenarios that we will continue to use some form of intermediary for our interpersonal communications.

4.2 Public broadcasting

The internet has lowered the barriers for people to distribute content that they have produced to a wider audience than their interpersonal communications. This was initially restricted to those who had the technical skills to build and maintain their own websites or other forms of content-serving technology. Nonetheless, over time, simpler tools were created for the content producer under the broad banner of “blogging,” although running these remained non-trivial. More recently, large platforms have made publishing to the world accessible to everyone, requiring little technical skills and no upfront cost—debates are raging about whether 'free' means free, but there is typically no or a low upfront cash cost.

The centripetal forces steering people towards these large platforms have been cost and technical capability. Although this has provoked some backlash, with people advocating for more distributed and open alternatives, these have not taken off to date.

Adding new regulations into the mix would seem to increase the pressure for most people to use an intermediary platform over the do-it-yourself options. People who do not wish to conform to the regulation may experience pressure to break away from the large platforms as these come into compliance; however, this may be a limited-term strategy.

Regulations such as the UK Online Safety Bill include provisions for degrading or blocking non-compliant services, which the regulator can apply to anyone defiantly striking out on their own. The outsourcing of many of the regulatory obligations to the platforms will be attractive to content creators who want to focus on their creation and not build an infrastructure for risk assessment, complaint handling, and so on.

4.3 Commerce

The potential of the internet to create economic growth led many governments to take a deliberately hands-off approach in the initial stages of its development. This meant refraining from seeking to control what was being bought and sold and from taxing these new activities. As more and more business has moved online, the sector has become too important to be left alone, and governments are becoming ever more hands-on. Thus, companies need to understand a host of regulatory matters in every country where they wish to operate and make arrangements to pay any taxes or duties that apply to their activity.

If companies could previously build their own websites to advertise goods and services globally and take customers from virtually anywhere with a low risk of interference, this is an increasingly challenging model. The intent of regulation is not to drive people to use large platforms, but this is its effect as a simple matter of good business sense.

Platforms carrying out all the compliance functions make life simpler for the business. This comes at a cost but has the benefit of predictability and can significantly reduce risk. If a platform guarantees compliance for a markup of five percent when a seller sells in a country, the latter can calculate whether it is still worth doing business there and factor this into their pricing. Except for large volumes of business, the costs of doing one's own due diligence work are likely to outweigh the cost of the platform markup and may leave companies exposed to greater risk. In simple terms, it is more likely that the large platform will have done all the due diligence and meet all the required standards as it has more resources and its business depends on getting this right.

The incentive to use an intermediary is especially strong for smaller markets where the legislation is complex and/or there is a need to work in unfamiliar languages. For instance, we can imagine a small business in Australia wanting to sell in Slovakia. They may look for a Slovak lawyer to advise them, but this will likely mean using a large, expensive global law firm with a local branch. Alternatively, the company could sell through a platform that is already established for sales in Slovakia and will take on the responsibility of paying taxes (inter alia) for it.

We are seeing this process play out following the UK's departure from the EU. A range of new obligations have been created as the UK stepped out of the single market, and businesses involved in cross-border trade have struggled to manage these themselves. A common strategy to continue trading is to use intermediaries who can handle all of these processes.

5. CASE STUDIES: THE RISE OF REGULATION

We can bring these changes to life by looking at some cases of national regulations and considering how these might impact business decisions.

5.1 The united kingdom

The UK Online Safety Bill provides a painfully detailed example of what a comprehensive set of regulatory obligations can look like as well as some indicative figures of the cost of compliance for businesses. The UK Government has estimated that around 24,000 entities will be within the ambit of the new regulatory scheme. The law does not just cover British entities but anyone who offers services to people in the UK over the internet and meets certain criteria in the bill. Most of the new costs will fall on these entities, but there may also be some costs for all online service providers as they try to establish whether or not they are concerned.

The UK Government published a regulatory impact assessment[13] document that includes estimates of compliance costs for various aspects of the legislation. The actual figures are open for debate, but the list of tasks is a good starting point for understanding the impact of these new kinds of regulation on businesses.

In-scope businesses may have to update their terms of service and other policies to ensure compliance with the requirements of the new legislation. They will have to do this for their UK users and will need to decide whether to maintain two sets of terms—for UK and non-UK users—or apply the UK ones to their global community.

For a micro business that essentially uses boilerplate text for its terms of service and policies, the initial compliance costs may in practice be quite low. Some enterprising advisory firms will likely offer compliance services including "Online Safety Bill Compliant Terms," and smaller businesses may feel that these are sufficient.

However, any larger business whose terms may be tested either by the regulator or in court will want to do this work very carefully and is thus likely to require extensive internal and external legal advice. Not everyone will require the same scale of effort as a major player like Facebook (which has faced repeated challenges in settling on its updated terms despite dedicating massive resources to this task) but it is going to involve a lot more than a few hours of advice from a regulatory professional.

The law will also place requirements on entities to provide people with ways to report specific types of content or behavior on their services. Many services already have some kind of reporting system, but these will presumably need updating to meet the specific requirements of the new legislation. Again, the costs may be manageable for micro-businesses, who may simply display a new contact email address on their website, but any larger entity larger that offers dedicated user reporting functionalities is likely to have to do much more work.

Changing any kind of public-facing feature on an internet service, especially a sensitive one such as capturing reports of illegal or harmful content, requires putting together a team. The team will comprise "programmers" to write the code but also a range of designers and content experts to assess the different ways in which the form could be presented and how users react to various options. Any change to an input form is likely to generate more work for changing the systems that process submissions through the form, which sometimes entails developing entire new workflows for the content moderation teams. There is also an ongoing maintenance challenge as global services may update their reporting systems

[13] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1061265/Online_Safety_Bill_impact_assessment.pdf.

regularly for various reasons and have to ensure that the special UK features are not lost as they do so.

Service providers will also be asked to pay a fee to the UK regulator, Ofcom, to cover the costs of their supervision. The precise level of the fee has not yet been determined, but the impact assessment tells us that the levy from all regulated entities may be in the order of 50 million pounds a year. This is likely to result in annual fees in the millions for the very largest platforms, down to a few hundred pounds for businesses with smaller UK operations.

5.2 Russia

Russia is at the forefront of our minds given the current importance of sanctions and reputational issues associated with working there. Interestingly, Russia has been busy legislating for a series of onerous local obligations for years, which has not attracted significant attention outside of the internet industry itself.

There has been variable enforcement of these requirements as the Russian government sought to balance its goals with a desire to be seen as part of the global economy. The global side of the equation has shifted in the wake of Russia's invasion of Ukraine, and enforcement action has followed against large name-brand internet services.

Prior to this there had been blocks of various services, but these had largely avoided the biggest players. The blocks are themselves imperfect because of the structure of the Russian telecoms networks, which are quite disparate, making it difficult to ensure that the blocks work. Additionally, at least as of the time of writing, the blocks have not sought to stop all virtual private network connections.

It is instructive to reflect on what this set of obligations is in Russia as we consider what it might look like in more countries. Internet service providers may be required to store data locally in Russia, block certain types of content, retain data for law enforcement purposes, and collect and provide data about certain types of users to the authorities.

The explicit goals of the Russian government are to seek sovereignty over the services used by people in Russia as well as to build a "Russian internet" that can function independently of the global internet. The size of the potential user base in Russia is attractive to global internet services, which have remained interested in the market, albeit generally not to the extent that they would be willing to comply with the increasing range of local obligations. In many cases, this has resulted in a stand-off, with services still operating without fully complying with Russian law.

6. CONCLUSIONS

There appear to be growing interest in following a path similar to the UK and the EU towards more internet regulation in a number of countries. This is evident across a range of countries from smaller countries like Singapore to major markets like India. In some cases, online service providers will be hesitant to comply with new rules on human rights grounds, but in many other places, there will be no basis to refuse cooperation, and the expectation will be one of full compliance with the associated costs.

Fast forwarding a few years, we can expect to see a situation in which a new internet service that is offered globally will, once it starts to gain users in multiple countries, receive communications from dozens of regulators asking it to pay fees and make specific changes to comply with the local regime. Absent any human rights concerns that would rule out compliance, the question will then be whether the compliance costs are worth it for the value of having users in that country.

The EU may lower the compliance burden if it can adopt a 'one-stop shop' regime, under which services are only regulated in one of the 27 member states. However, this may prove challenging given that attitudes towards restrictions on content can vary widely across EU countries. Even if the EU agrees on a single regime, and assuming that the US stays out of the game for First Amendment reasons, service providers may still face a long list of regulators asking for their time and money.

The internet itself has not necessarily 'splintered' in that computers using the common protocols can technically still communicate with each other wherever they are located. Yet, the new regulatory overlay means that the physical location of both the service and each of its customers is an important factor for compliance and the legal provision of the service.

Businesses will have to consider for each market the regulatory and legal implications of allowing people to access their services. They will then need to decide whether a market is sufficiently valuable to subject themselves to oversight, which could be costly and time consuming, and pay any applicable fees.

If they decide it is not worth it, they may use technology to try to identify and block users from a country, which is likely to be sufficient for them to defend themselves against regulatory action if done well. Blocking people will come with implementation costs but may be far cheaper than full regulatory compliance and may be seen as a less risky approach depending on the nature of the regulatory requirements and penalties.

In some cases, there could be significant penalties for unintentional non-compliance. Something similar occurred previously with online gambling service providers, whose executives ended up being arrested when they strayed into the US.[14] Although the services were based outside the US, they were still pursued by US authorities for taking insufficient action to prevent their use by US persons.

We may see a 'blacklist' of countries develop initially where legal advice is to block users unless and until compliance can be ensured. This happens today with sanctioned countries, which companies must block or risk serious criminal penalties. When the potential penalties are harsh, a safety-first approach for businesses is to take all possible steps to keep out of this market unless there is a very compelling business case that would justify full and careful compliance.

In one possible model that may develop, services remain open globally except for blacklisted countries, which would look and feel similar to the world today, where a few countries are out of bounds. However, there is another potential future model that would imply a very different world, namely, a switch to a "whitelist model," in which services are not offered globally by default but only rolled out country by country.

We still lack sufficient information to know clearly where we are heading, and a critical factor is whether new regulatory models are convergent or divergent. If governments seek to align their rules, as the EU does internally, this would steer us towards maintaining a more open internet where services can still largely be offered globally. If they opt for very different models with highly specific local requirements, this will drive us towards the country-by-country model as services have to be tailored to each market.

The impact will also vary significantly depending on the size of both businesses and countries.

It is possible that the smallest businesses may be able to carry on largely as they are today if they are excluded from new regulations or only have minimal obligations that they can meet through the use of 'compliance consultants'. This compliance work may cost significantly more than the kind of optimistic estimates published in the UK impact assessment, especially in countries where the requirements are more specific, but they should not be ruinous.

Larger businesses are likely to have to invest millions in their compliance work, hiring large in-house teams to deal with regulators in each market and using

[14] https://www.theguardian.com/business/2006/sep/30/usnews.internationalnews.

leading outside counsel from the global law firms they employ. There will be regular challenges to the policies and practices of large companies, which will require them to update their documents and tools continually with big cross-functional teams. We can see how this works in other sectors, such as the pharmaceutical industry. While many small companies are developing innovative drugs and treatments, they frequently work with a large global company to have their products tested and brought to the market. This is a rational response to the complexity and costs of the various compliance regimes that governments have put in place to ensure the safety of new pharmaceutical products coming into their markets.

There may come a time when the regulatory demands in a market cause a large company to question its presence there. Nonetheless, as irritated as it may be, it will usually find the resources to maintain its overall global presence. Where even large companies may decide that enough is enough is where we see significant compliance costs for very small markets. If a government misjudges the value of its country as a market, it may drive away some companies, which simply choose to opt out of offering their services there.

The most difficult decisions may be faced by medium-sized entities that are large enough to attract attention and, thus, have to take compliance seriously but do not have the abundant resources of the internet giants. These entities may find that decisions about whether or not to operate in a particular market are more finely balanced, especially where the risks seem high (e.g., threats of large fines or criminal action against executives) and the entity does not feel it is fully across them.

We might see mid-sized companies confine their operations to a restricted set of relatively safe and lucrative markets while staying out of those where the risk-reward calculation falls the wrong way. This would result in fewer services for consumers and less competition for the large established players in non-core markets.

The impact on growing companies will be a key test of whether the new regulatory models are working. It is certainly not the intention of policymakers to entrench the position of today's large platform leaders. Their preference would be for new entrants to continue to be able to displace incumbents just as the present winners displaced those that came before them. For this reason, it is common to see tiers of obligations in the new regulations, which place a much greater burden on the largest platforms than on smaller companies. The hope is that this will help new entrants catch up with existing players as they grow under a lighter regime to the point where they have the resources to play on the same field as the biggest platforms. Time will tell whether this hope is realised.

We are still in the early stages of this next evolution of the internet, and it is not yet clear where current pressures will eventually take us. However, the push for increased local sovereignty seems material and unlikely to be reversed and should thus be factored into business strategies.

It would be a mistake to think that the desire to regulate will recede. The activities that take place online are simply too important, and increasingly so, for governments not to want to have a say in how they should be managed. Government intervention can happen on an ad hoc basis when policymakers put pressure on companies to act in a particular way. This has been a regular occurrence for some time, as evidenced by the frequent headlines in which politicians criticise internet platforms for their inadequate response to a matter of public interest. Yet, there are advantages to moving away from ad hoc requests to a model in which governments codify their demands in legislation. A regulated model is likely to be more consistent and predictable, which is helpful to both businesses and consumers.

The ultimate impact on businesses of this shift towards a more regulated online world will depend on the extent to which they are workable and interoperable across jurisdictions. It is possible that governments will use regulation to make entirely unrealistic demands of online service providers and that these will be incompatible or even contradictory between different countries. Still, with the right political will and a sound understanding of what is reasonable and effective, it is equally possible that governments will adopt common standards, compliance to which is not too onerous technically or financially for businesses operating in many places.

Businesses have an important role to play in steering us towards the right model. Policymakers need evidence and insights into the likely effects of particular regulatory measures, and this can only come from an open dialogue with the companies that will have to comply with them. This can be challenging for both sides, but it is worth the investment to maintain the economic benefits of the internet while ensuring sufficient local accountability to safeguard societal interests.

Comment to "Gearing up for the Splinternet"

GET THE BALANCE RIGHT

JOAKIM WERNBERG

"When you think you've got a hold of it all
You haven't got a hold at all"

- Depeche Mode, Get the Balance Right (1983)

In its early stages, the commercialized internet was largely shaped by expansion and interconnection. Technological development and political priorities jointly promoted globalization and economic integration. In the last decade, however, political will and policy has increasingly shifted, partly in response to increased geopolitical tensions and economic uncertainties, but partly also in response to the internet's increased economic and social importance. This shift reveals an inherent friction between on one hand legislation and regulation, which is anchored in territorial sovereignty, and on the other hand internet's infrastructure, which is highly decentralized and runs across rather than along national borders.

In "*Gearing up for the Splinternet*", Richard Allan portrays the internet´s evolution from the 1990's up until today in terms of opposing forces – one type contributing to an expanding and interconnected network (*centripetal forces*) and the other working to splinter it (*centrifugal forces*) in order to establish and maintain geographically localised control. This provides an intuitive framework for understanding both the overly techno-optimistic era in the late 1990's and the 2000's, and the backlash (or techlash) that followed in the 2010's. More importantly, Allan elegantly points out that the conflict is not necessarily one between governments and markets. Economic and political forces can interact both to expand and splinter the internet. Legislation can in fact work as a centripetal force, for instance through harmonized and predictable regulation across countries rather than ad-hoc government intervention.

Thus, the challenge that Allan's essay poses is not to reverse centrifugal forces, peel back regulation and get back to the internet of 2009, but to regulate the internet in a way that balances the increased need for geographical control with the still enormous potential for future innovation, entrepreneurship and economic integration. Another way to approach this challenge is to think of the internet's development in terms of transaction costs.

In economics, transaction costs are used to describe the entire cost of conducting a transaction in the market – not just in terms of money changing hands but also aspects such as time, effort, regulatory burden. With the initial expansion and growth of the internet, transaction costs associated with accessing any given *known* information source or contact fell dramatically. However, with the ever-rising supply of available information and potential contacts, the costs of searching and finding the right *new* information or contact increased just as dramatically. Thus, the then popular notion that you could "find anything with a click" was only true because of the rise of intermediaries – today we think of them as multis-sided platform economies or digital platform companies – whose business model is to match supply and demand at lower transaction costs.

Most if not all the big tech companies today all have in common that they act, in one way or another, as matchmakers for supply and demand facilitated by the internet. In recent regulatory debates in the EU, these platform companies have been described as gatekeepers, which is true with respect to their respective platforms, but with respect to the internet they are not gatekeepers as much as they are matchmakers. The rise of, mainly commercial, intermediaries also contributed to lowering transaction costs on the internet by introducing user-friendly interfaces and services. In fact, it required more technical expertise to use the internet in 1997 than it did in 2017. In other words, anyone with an internet connection can go online, but the digital platforms and intermediaries allow more people and businesses to leverage the full potential of the internet.

As a result, a few digital platforms and intermediaries have grown to unprecedented size and the market distribution is heavily skewed. This can partly be explained by the fact that they operate on a market that has also grown to an unprecedented size, but partly it can also be explained by transaction costs. It benefits users to coordinate to a few platforms where they can find what they are looking for.[1] While it is still easy, and most of the time free for consumers, to use multiple platforms in parallel, this still increases their transaction costs.

[1] For this reason, competition on platforms and among platform companies follow a somewhat different logic than competition among traditional production or service businesses. See: Wernberg, J. (2021). *Innovation, Competition and Digital Platform Paradoxes*. Policy Papers on Technology, Economics and Structural Change 2021.1. The Swedish Entrepreneurship Forum, Stockholm. https://entreprenorskapsforum.se/wp-content/uploads/2021/03/Wernberg_Policy-Paper-1.pdf

This does not entail that the largest platforms have managed to harness transaction costs to become too big to fail. First, the user growth of new competitors in areas like social media appears to be accelerating over time, suggesting that new competitors manage to leverage the lower transaction costs on established platforms to attract attention through word of mouth. Second, as the number of users grow, so does the share of content or contacts that is not considered relevant to any specific user. The level of noise or information pollution grows, and with it the transaction costs. For this reason, most platforms increasingly employ algorithmic solutions and artificial intelligence (AI) to curate the supply or newsfeed that each user is exposed to. In social networks there is a trend towards promoting smaller groups within the network, which can be interpreted as a way of compartmentalising transaction costs and keep them low even when the network as a whole grows very large. Individual users may also feel that they want to limit the number of friends and acquaintances they are exposed to in their newsfeed or the variety of businesses they are exposed to when shopping for something.

In its early days, the internet was oftentimes compared to an open square where everyone could gather, interact, and make their voice heard. As the net has grown in importance it has become increasingly clear that the open square is no longer an apt metaphor, if it ever was. While the open internet is still there, beneath the application layer, the ability to reduce transaction costs and keep them low as the network grows relies on walls and walled-off spaces.

Platform companies and other intermediaries open up the internet to people and businesses by walling it off. They offer matchmaking services to their users, they provide user-friendly interfaces and services that attract less tech-savvy users, and they try to ward off noise or information pollution between users or groups of users. Similarly, other digital service providers that operate on the internet combine user-friendly services with curation to allow their users to leverage the internet for a specific purpose without being exposed to the negative information externalities of other peoples' similar but unrelated pursuits.

It turns out, perhaps a bit counterintuitively, that walls help to realise the potential of an open internet. Even without the regulatory push of the last decade, the internet has been increasingly divided into a network of networks dedicated to specific transactions or activities. How does this then compare to a splinternet that reinforces national borders in the digital network?

The difference between digital walls and national borders is that the former is optional while the latter is mandatory. People and businesses can choose what walled-off spaces of the internet they want to be part of, but they are bound by national borders related to their own geographical position as well as the position of the person or content (server locations, intellectual property regimes etc) they want to access. At first glance, interactions and transactions that fall within a specific country or regulatory regime may not appear to be affected by the splintering of the internet. Exchanges across borders on the other hand are subject to increased transaction costs if regulations differ or further compliance work is needed between the countries in question. Yet, if transaction costs rise at the border, then at some point competition is weakened in a way that effects domestic customers (individuals and businesses) negatively.

Furthermore, falling transaction costs have also led an increasing number of businesses to adopt software-based and data-driven services provided by cloud service providers or other actors within the growing Software as a Service (SaaS) industry. Increasing bandwidth and computing capacity at falling costs made it feasible to sell compute and storage, but also increasingly software based on that computing capacity, as a service. This has transformed large portions of the economy by introducing considerable efficiency measures, especially for small and medium-sized enterprises (SMEs), at the cost of a growing share of mutual interdependencies between firms.[2] These interdependencies are not confined within national borders, meaning even traditional businesses that are not normally associated with digital markets are likely to be affected by rising transaction costs at the border.

The perhaps greatest value of internet's contribution to market expansion (and lower transaction costs) doesn't lie in the geographical space it covers as such, but in its ability to accumulate and sustain supply and demand for more or less niche markets while being significantly less constrained by geographical distance.[3] These markets form walled-off spaces based primarily on the type of transaction even if geography may also figure into it. Consequently, the markets that will be most affected by splintering the net along national borders can be said to be those for which an open internet has provided the greatest *difference* in transaction costs. These include the markets that would not be feasible without the internet to begin with, but they may also include some very local and traditional businesses. For instance, consider a small bakery that relies on targeted advertising in

[2] Wernberg, J. (2023) Bland moln och plattformar – En kartläggning av hur datadrivna tjänster förändrar ekonomin. Entreprenörskapsforum, Stockholm. https://entreprenorskapsforum.se/wp-content/uploads/2023/05/Rapport_Wernberg_Web.pdf

[3] There is also a considerable economic and social potential for urban digital markets, where digital tools and platforms are utilized to match supply and demand that are highly localized and temporary in cities with large populations.

social media to reach customers with special offers or to communicate temporary locations from which they sell their baked goods.[4]

When legislation shifts transaction costs, it is not only a matter of regulatory burden for those in scope but also the risk of second-order adverse effects. There are two examples of this hinted at in Allan's original essay. First, increased transaction costs for offering cross-border services on digital markets may push more businesses, especially SMEs, to using intermediary services not out of productivity gains but to avoid liability. This in turn is likely to reinforce the dominant position of current large tech companies who have the resources to convert compliance costs to a competitive advantage, while would-be-competitors face greater barriers to entry.

Second, while a lot of the regulatory debate centres on the applications built on top of the internet, the underlying network is still available to those with sufficient technical skills. As long as the splintering of the net does not cut into the actual cables and basic protocols of the network, the resulting splinternet will be unequally fragmented to different groups of users. Those with sufficient technical know-how will be freer to navigate the entire network than their non-technical peers. This roughly counteracts the positive effects of improved user-interfaces and user-friendly applications that opened the internet to a wider audience from the 1990's until today by lowering their transaction costs. Furthermore, the actors with strongest incentives to gain the skills necessary to circumvent regulations and access the wider internet will include the groups that legislators oftentimes want to target with stricter regulations of the internet – those engaged in criminal enterprise, cyberattacks, disinformation and the like. Thus, regulatory measures should be expected to have an uneven impact on those within scope.

In summary, the difference between putting up walls on the internet and splintering it along national borders is that the former lowers transaction costs while the latter will tend to raise them. Legislators gearing up to govern the splinternet – and balancing regulatory measures against transaction costs - need to take into consideration how digital interconnectivity and economic integration facilitated by the internet has structurally changed their national economies in the last 25 years.

This overview of transaction costs suggests a regulatory approach that is narrower in scope, that is more easily harmonised with the regulatory frameworks in other related geographical markets (not unlike interoperability between technical

[4] As it turns out, a lot of small and medium-sized enterprises using targeted advertising via international digital platforms use it to reach customers in their established home market (see Wernberg 2023).

systems), and which provides long-term predictable rules for the market. On the other hand, legislators facing fast-paced technological development and large-scale structural change – and not considering transaction costs – may very well opt for the opposite approach: regulation that is wider in scope, is novel, and is easily adaptable over time to avoid being outdated or redundant. Currently, the scales seem to be tipping towards the latter approach rather than the former, with increasing transaction costs to follow. The trick is to get the balance right, but oh what a trick it is.

ENTREPRENÖRSKAPS
FORUM

WWW.ENTREPRENORSKAPSFORUM.SE