***No User is an Island:***

***A collective approach to protecting individual rights and the impact of internet intermediaries***

When designing local and international approaches in the evolving communications environment, policy-makers should be mindful of the communal nature of how citizens interact and engage with internet intermediaries. While policies in the EU and UK have been focused on promoting the rights of the individual online and protecting against online harms, it may be useful to consider a collective or community perspective when setting such policies.

'Internet intermediaries' is a blanket term which refers to a broad range of digital service providers that facilitate internet-based interactions between users. Some of these intermediaries connect users, host web-based services, enable data processing, facilitate the sale of goods/services or other commercial transactions, assist searches and gather information. Many internet intermediaries execute some of these functions simultaneously, including in parallel with other functions that are not classified as 'intermediary'. Algorithmic processing is a key element in how internet intermediaries rank or moderate content, and this poses a challenge for policy-makers at both the local and international level due to legal, regulatory and cultural differences.

When it comes to internet intermediaries such as digital platforms, the reality is that we are not merely individual users of these platforms, but rather collective users of individual accounts or profiles. This applies to electronic communications services, including social media networks, and other forms of internet intermediaries that leverage the personal data of both active and passive users.

Who is Privy to 'Privacy'?

The approaches to dealing with internet intermediaries and indeed personal data differs across countries and cultures. A recent article in the Financial Times outlined how academics have highlighted the problematic ways that discourse on online privacy tends to be western-centric. Many of the Big Tech companies with origins in the USA perpetuate the dominant 'western' ideas of what constitutes online privacy. These ideas are at odds with alternative traditions from other parts of the world, where privacy is perceived as belonging to communities and groups. Research Associate at Oxford Internet Institute's digital ethics lab, Nikita Aggarwal, believes that understanding this variation in approach could help policy-makers think differently about the management of data-governed technologies. Better data sharing from models of group-level privacy could allow better public safety and public health initiatives – which, of course, are of paramount importance during a pandemic.

Indeed, recent public health measures have uncovered a whole host of challenges and opportunities posed by the role of open data to mitigate the COVID-19 pandemic, with responses from authorities in South East Asia diverging from that in Western regions. For example, early in the pandemic South Korea disclosed information on geolocations of the places visited by infected persons, including retail shops and religious facilities. While this was an attempt to curtail the spread of the virus, the risk of reidentification caused human rights activists and academics to be alarmed over civil liberties being breached, both for the case of individual damages and stigma being increased for minority groups.

The General Data Protection Regulation (GDPR), while notoriously difficult to enforce, has protected the personal information of EU citizens and set the standard for privacy which was the backdrop pf the COVID-19 response across the region. There has been much ongoing debate on the trade-offs between individual privacy concerns versus public health risks.

When it comes to any policy initiative aimed at internet intermediaries, it is evident that this too is a balancing act between the quality of service offered and curbing the potentially negative societal and economic impacts of these service providers and platforms. The balance between protecting freedom of expression and preventing online harms is currently being engineered through the EU's upcoming Digital Services Act (DSA), as is the balance between encouraging innovation and promoting the values of a level playing field and fair competition with the Digital Markets Act (DMA).

By taking lessons learned from a community-based approach and applying these to the EU's stalwart policies of enshrining personal rights of citizens, we can observe a paradox: a community-centric perspective may be needed to protect individuals who are active and passive users of internet intermediaries.

Collective Harms

In his July 2020 article 'The Data Delusion', Martin Tisné, Managing Director at Luminate, emphasized that the approach of protecting individual data isn't enough when 'the harm is collective'. Tisné stressed that individuals may enjoy benefits in the short term from what will harm the collective in the long term, if the collective data rights continue to be ignored by institutions such as European Commission – whose Data Strategy focuses primarily on empowering individuals with respect to 'their' own data.

The concept of 'collective harm' can be insidious, as this can be less visible in comparison to the harm incurred by an individual, where there is often legal protection in place, especially in the EU with the aforementioned GDPR. In the case of discrimination experienced by a person on the grounds of gender, ethnicity, or age, this can be evidenced, and redress may be sought. But what happens at the level higher than the individual, where an algorithmic decision lies at the root of discrimination? Our current public policy tools and legal instruments are poorly equipped to appropriately respond to inferred and optimized harms which have been made possible by such algorithms.

An example of 'inferred harm' is where an individual is presumed to be a member of a group or community, while there is no harm caused to that person whose data is used. This type of harm occurred when users uploaded photos of themselves onto a dating website in the USA, and researchers then used this data to develop controversial algorithms to determine a person's sexuality based on their facial features. While those users who uploaded the photos may not have been harmed, other people – who never had any connection to this dating website – are the harmed parties, whose sexuality may have been identified by this algorithmic technique where data is collected and processed.

An 'optimized harm' occurs by virtue of how machine learning systems are optimized, where people are profiled by an algorithm, often without the user's knowledge or awareness. Activist and academic Zeynep Tufekci has written that genre of harm can range from relatively harmless topics, such as guiding those who enjoy sports to become athletic enthusiasts, to far more damaging examples where users who are politically disillusioned may become radicalized. These algorithms developed by/for the service providers or platforms are solely concerned with targeting its users - who generate revenue for the company – and often ignore externalities which can impact non-users across society.

Dr Johnny Ryan of the Irish Council of Civil Liberties (ICCL) has also drawn attention to the dangers of internet intermediaries collecting and leveraging personal information of users without their knowledge, at both the Unites States Senate and the International Committee on Disinformation and Fake News. This data mined, stored and capitalized on includes not only sexual orientation, political views, religious affinity, and medical information, but also what users are listening to, watching and

reading, as well as exact location with GPS coordinates. This enables digital service providers to create and maintain 'digital replicas' of individuals by collecting information on personalised decision-making, behaviours and even thought processes/patterns.

Competition Concerns

Furthermore, the economic implications of data harvested from communities of users allow Big Tech companies to leverage this data across different lines of business, which has an adverse effect on competition and gives rise to antitrust concerns as innovation is stifled, and consumer choice is reduced. In their analysis for Vox EU 'The antitrust orthodoxy is blind to real data harms', Cristina Caffarra, Professor Gregory Crawford and Dr Johnny Ryan argue that there is increasing harm being caused by the misuse of personal data, and that the lack of privacy is an 'often unobservable' price of using digital platforms. This absence or lack of privacy then enables harms such as exploitation of users and anti-competitive abuse of dominance by digital platforms.

The more users a platform has, the more data is collected by the platform/service provider, which amplifies network effects or 'cross-group effects'. A Body of European Regulators for Electronic Communications (BEREC) Report from 2019 on the Data Economy outlined the 'winner-takes-all' outcome, or 'tipping markets' that can result from these effects. The quality of targeted advertising offered by services or platforms is directly correlated to the number of users engaged, and this in turn increases the probability that users will interact with advertisements shown. This in turn again attracts more advertisers and thus advertising revenue, and improved the capacity to invest in the service or platform to attract even more users. This cyclical phenomenon is referred to as a 'monetisation feedback loop' and makes it extremely difficult for competitors to enter the market, as potential entry would require the coordination of switching users to facilitate comparable network effects. A 'tipping point' is a moment after which it is incredibly difficult to re-establish competition.

It is clear that the rules for competition or antitrust policy need to be – and currently are being - rewritten in the context of internet intermediaries. This was the topic of my 2018 master's capstone thesis entitled 'Modern Monopolies: New Rules for the Digital Titans' at Schwarzman College, Tsginghua University. This discussion paper explored the question of how regulatory bodies should approach digital platforms leveraging the interactions between massive amounts of data collected from users.

The Digi-Tragedy of the Commons

On the subject of 'tipping' – there is another 'tipping point' that is becoming more urgent and more ubiquitous across multiple sectors for public policy discussions: climate change. Professor John Fernández of MIT has discussed this inflection point in the context of sustainability issues for industry.

As more and more users access internet intermediaries, the number of devices also continues to climb. For the Internet of Things (IoT), the number of devices worldwide is expected to triple from 8.74 billion in 2020 to more than 25.4 billion IoT devices in 2030. China currently has the highest number of such devices, with 3.17 billion IoT devices in 2020. This ever-growing demand for data usage and consumption is driving energy demand, especially when it comes to the operation of data centres. The International Energy Agency (IEA) estimates that approximately 1% of global electricity use (250 TWh) was consumed by data networks in 2019, with mobile networks accounting for two-thirds of that figure. Despite advances in current energy efficiency improvements, forecasts for this electricity consumption are 270 TWh for 2022. For Ireland, which houses 70 data centres with more under construction, there are forecasts that up to a third of Irish energy demand will come from these

centres by 2030. While data centres may be viewed in certain circles as tangential to policies surrounding internet intermediaries, it is likely that the role of these infrastructural systems will become increasingly important for digital strategies at national and international level.

Over the past decade, demand for digital services has grown with the IEA estimating that global internet traffic has multiplied twelvefold since 2010. Additionally, at the very start of the COVID-19 pandemic there was a surge in global internet traffic by almost 40% between February and April 2020. This was primarily driven by internet intermediaries where there was an international boost in video conferencing and streaming, social networking, and online gaming during regional lockdowns.

While there have been positive environmental consequences of the digital transition which was accelerated by the pandemic, the flip side of the coin is that our increasingly virtual society and services will require more energy consumption and even more innovative solutions to keep these developments sustainable for our only planet. A more holistic, community-centric approach to policies regarding internet intermediaries would help address the societal, environmental and economic impacts that these entities have on our world. As illustrated by Tisné in 'The Data Delusion', the individualisation of data-driven harms along the lines of the GDPR approach is akin to *'requiring that a case on the CO2 emissions of an entire country depend on its provable impacts on one person'*.

The Wonderful World of AI & Algorithms

As we transition towards an increasingly digital society, users navigate through multiple virtual nexuses where we continuously leave behind a trail of data breadcrumbs – a trail which can be incredibly lucrative when in the hands of large tech platforms and service providers. The evolution of algorithms and the scalability of data collection means that the market has shifted from finding value in individual data to being more focussed on collective data. The individual remaining at the core of policy-making means that legislation is lagging behind the landscape of technological developments the reality put forward by artificial intelligence.

This year, the EU published its approach to AI in the context of the Digital Decade strategy. The Centre for Data Ethics and Innovation (CDEI) in the UK has published many reports into the ethics of AI, including a recent paper on 'Unlocking the value of data: Exploring the role of data intermediaries'. This independent report explores how these data intermediaries can play a part in responding to pressing social, economic, and environmental challenges and opportunities

It is evident that we are living in a moment that is not unlike the 'Wild West', where the standards are just beginning to emerge on how to set policies for and regulate internet intermediaries. It may be useful for the 'west' however to look to the 'east' to gain insight into the advantages that may be gleaned from a more community or collective perspective, as opposed to an individual-centric approach to these policies.

In 2019 at the World Economic Forum (WEF) in Davos, Singapore launched its Model Artificial Intelligence Governance Framework, which continues to be updated but maintains the guiding principles that decisions made by AI should be human-centric in protecting the interests and safety of citizens and that AI systems should be 'explainable, transparent and fair'. To address the technology risk associated with AI, this model put forward by Singapore recommends both a rules-based and risk-based management approach, which is in alignment with other global frameworks including the recently published EU draft regulations on AI. Due to the cross-border reach of internet intermediaries, it is clear that there is a need for a global cross-cultural set of standards, not unlike the Generally Accepted Accounting Principles (GAAP), which will facilitate innovation and safeguard public

trust when it comes to AI and the policies that will legislate and regulate this area at local and international level.

It is worth noting that algorithms themselves cannot be biased in a vacuum, but that bias can be so-called 'baked-in' by the humans who ultimately design these computerised sets of inputs that produce outputs based on a given set of rules, which are either defined or learned. This was discussed on a particularly interesting episode of the European Bank for Reconstruction and Development's (EBRD) podcast - 'Pocket Dilemmas: Should Algorithms Rule the World?'. Therefore, there is a need to ensure that there are diverse backgrounds and experiences brought onboard by the teams of people who are tasked with creating these all-important algorithms. In addition to diversity in gender and ethnicity, Dawn Duhaney, Partnerships Manager at UK Wellcome Trust, spoke on that podcast about the need for social scientists and user researchers to have role in building these algorithms (alongside the data scientists and machine learning experts) as these kinds of jobs have the task of considering the long-term societal implications of technology – not just revenues and profits for internet intermediaries in the short/medium term. This will require a concerted effort at both local and international levels to incentivise and encourage education and training for workforce pipelines, in order to adequately prepare qualified candidates for these specific roles.

No User is an Island

Policies and regulation that were appropriate for traditional telecommunications can fall short due to differences in design when it comes to internet intermediaries; the internet is 'packet'-based, where pools of data points are moved from one place to another, whereas telecommunications networks depend on dedicated interconnections between consumers. Common mobile and desktop applications such as WhatsApp, Instagram and Facebook Messenger, known as 'Over the Top' (OTT) applications are digital service providers that continue to become more enmeshed in the fabric of society – and notably remain under a single parent company in the case of those three popular examples.

Whenever a user communicates with another user online through an internet intermediary, or when a user purchases a service or product online, it is important to know that these are not interactions or transactions that occur simply between two parties – the way it would if someone picked up the telephone to make a call or bought something from a brick-and-mortar shop. For every activity that takes place in the context of internet intermediaries, there are always other nodes 'in the room' - or rather, the online nexus.

Under national and regional laws, these internet intermediaries have been entitled to protection from liability for content posted by others, as they deny the label of 'publisher'. This argument was strained with the removal of Donald J. Trump's social media accounts in the aftermath of the events that unfolded in Washington D.C. on January 6th, 2021. This decision by platforms such as Twitter further sparked the debate surrounding objectives of freedom of speech and protection from harms.

Christel Schaldemose, the rapporteur of the European Parliament Committee on Internal Market and Consumer Protection, has stated clearly that internet intermediaries which are digital platforms have become a big role in our society as they provide a new kind of 'social and public space(s)' for users. This is an excellent reason for policy-makers to adopt a more community-based approach as opposed to concentrating on an individual-centric approach, as social and public spaces are available to, and impacted by, all citizens. Otherwise, we will be left with a legal and regulatory limbo at regional and international levels, where the pursuit of accountability and transparency from internet intermediaries will be greatly jeopardized.