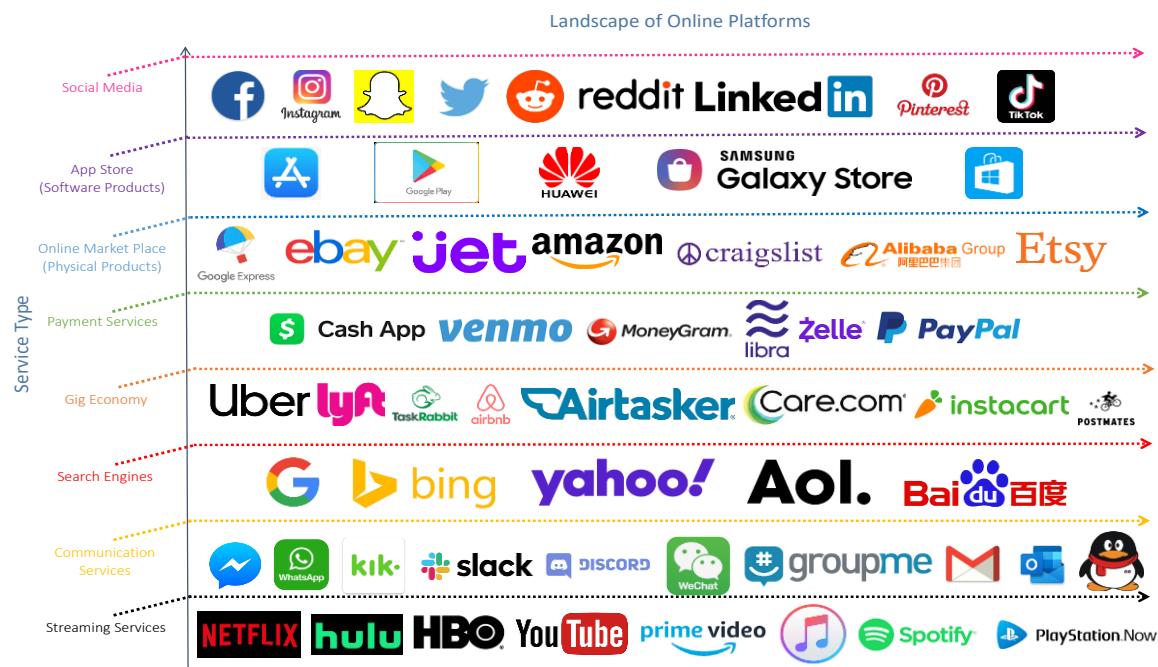


PLATFORM COMPANIES & RESPONSIBLE BUSINESS CONDUCT

Over the last decade, online platform companies have become increasingly essential parts of daily life for much of the world. Whether it is communicating with friends and family via Facebook or calling a car through the Uber app, online platforms have played a powerful role in shaping the modern world.

Definition and Overview

The OECD defines an *online platform* as “a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet.”¹ Online platforms include a range of services available via the internet – including for example, online marketplaces (e.g. Etsy and E-Bay), search engines (e.g. Google and Baidu), social media (e.g. Facebook and Twitter), app stores (e.g. Apple App Store), communication services (e.g. WhatsApp and WeChat), payment systems (e.g. Venmo and PayPal), and platforms supporting the gig economy (e.g. Uber and Task Rabbit)², among others.



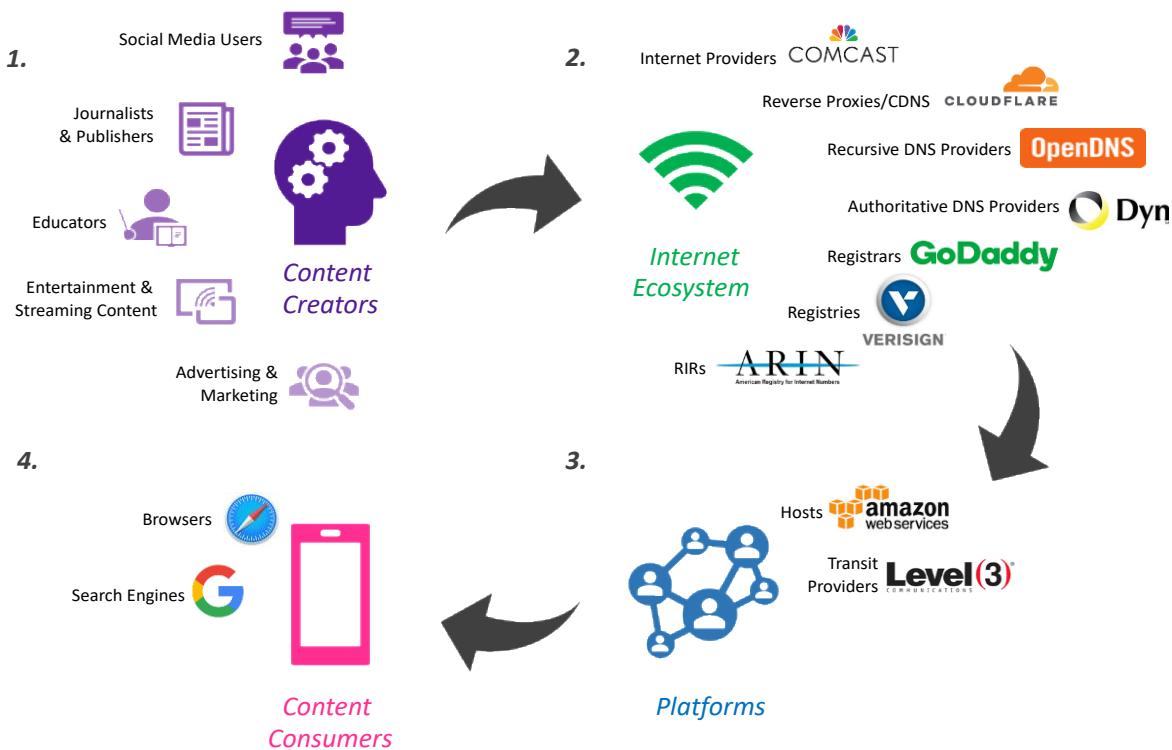
¹ OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, <https://doi.org/10.1787/53e5f593-en>, hereafter, OECD (2019)

² Some streaming services or gig economy ‘platforms’ may not be considered as platforms when it has only one set of customers, eg. subscribers or riders (for example in the case of delivery or transport platforms where in certain jurisdictions the company’s drivers are considered by law to be employees, not contractors).

Platform companies have the ability to bring significant value to consumers, business and governments. Indeed, online platforms have the potential to ease communication, increase access to information services and customers, and provide new opportunities for entrepreneurs, artists and workers.

However, given the speed at which platform companies have emerged, they have operated within a limited regulatory framework and oversight. Existing regulation has mainly been developed with older business models in mind, leading to questions about the applicability and suitability of existing regulations for platform companies. This reality is compounded by the speed of innovation which often leaves regulators scrambling to keep up.

It is important to note that platform models vary and as such not all risks highlighted are relevant to all models. Likewise, a broad variety of companies are involved in the online platform “value chain”, their roles are described in the mapping below.



The value chain starts with *content creators*, who author the actual content online. Created content can include text, audio, video etc and is published on online platforms. In order to be published on an online platform, the content must be transferred through the internet ecosystem. The consumer enters the internet ecosystem through an *internet service provider* (e.g. Comcast), and the use of Regional Internet Registries (*RIRs*) (e.g. ARIN, RIPE) that provide the IP addresses used by Internet Infrastructure. *Reverse Proxies* (e.g. Cloudflare) provide networks to ensure content loads fast and is protected from attack. *Registrars* (e.g. GoDaddy) register the domains of websites, and *registries* (e.g. Verisign) run the top-level domains like .com, .org etc. ICANN (Internet Corporation for Assigned Names and Numbers) is a global

multistakeholder, private organisation that manages Internet resources for the public benefit. It acts as technical coordinator of the Internet's Domain Name System (DNS) and thus the rules for the registrars and registries. *Authoritative DNS Providers* (e.g. Dyn) resolve the domains of sites, whereas *Recursive DNS Providers* (e.g. Google) resolve the DNS queries of content consumers, ie. providing the correct IP address of the intended domain name to the requesting host.

Online platforms have their own set infrastructure which allows them to be accessed through the internet ecosystem. This infrastructure includes *hosts* (e.g. Amazon Web Services) and *transit providers* (e.g. Level(3)) that connect the host to the rest of the internet. Content consumers can access platforms and the rest of the internet through *browsers* (e.g. Safari), and by using *search engines* (e.g. Google) that help users discover new content and organize relevant information.

Platform Companies and RBC

Platform companies face a number of challenges when it comes to responsible business conduct (RBC). Below we outline a non-exhaustive list of these potential challenges.

Potential Human rights infringements (Chapter IV of the MNE Guidelines):

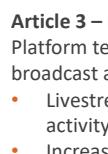


Article 2 – Right to Non-Discrimination: Risk of social media platforms exacerbating vulnerable groups' exposure to hate speech including through inaccurate or inappropriately framed content, causing on and offline harms and infringing on the right to non-discrimination.



Article 19 – Freedom to Opinion and Expression: Platform companies might adversely impact these rights in several ways:

- Risk that human rights defenders self-censor their expression if they fear being under surveillance.
- Risk of AI bots influencing social media with misinformation or biased views and opinions.



Article 3 – Right to Life and Personal Security: Platform technologies have been used to broadcast and incentivise offline harms by:

- Livestreaming violent content and terrorist activity
- Increasing accessibility to illicit content and illegal activity



Article 12 – Right to Privacy: Platform companies collect large amounts of data, creating a risk that:

- Law enforcement and intelligence agencies make illegitimate requests or demands for personal information (i.e. location, personal relationships).
- Companies collect, use, or share a person's personally identifiable information without informed consent.



Article 20 – Right to Freedom of Association: The right to freedom of assembly and association can be adversely impacted if:

- Governments use social media to monitor and repress individuals' civic engagement
- Platform companies participating in the gig economy undermine opportunities for collective bargaining



Article 21 – Right to Take Part in Government: False information perpetuated on internet platforms may delegitimise electoral processes and threaten the human right to participate in government and free elections.



Article 23 – Right to Work: Platform companies might adversely impact the right to work by:

- Contributing to job losses due automation of online marketplaces or undermining unionised labor
- Providing new avenues for employers to surveille potential hires and current workers outside of work



Terrorist, Violent & Extremist Content

Online platforms, and social media companies in particular, have been used by extremists for recruitment and to live stream violence and terrorist activity. In 2019 for example, a terrorist

attack on a mosque in Christchurch, New Zealand killing 51 people was live streamed by the perpetrator on Facebook before being shared on other sites. It is estimated that over 200 people watched the live-stream footage without reporting it. A report found that the video remained on Facebook for six hours and on YouTube for three hours. Facebook reported that it took down 1.5 million videos of the attack within 24 hours of the incident.³ Facebook, YouTube, Twitter, and other platforms have adopted policies prohibiting violent and harmful content and have put in place resources to review and take down content violating these standards, including through human reviewers and the use of AI.

In response the governments of New Zealand and France partnered to issue the Christchurch Call which while recognising the right to free expression is a “commitment by Governments and tech companies to eliminate terrorist and violent extremist content online.”⁴

This topic is linked to work from the [OECD Directorate for Science, Technology, and Innovation \(STI\)](#), with the OECD Committee on Digital Economy Policy, to create standard reporting templates for social media platforms covering how many attempts there were to upload violent or extremist content and how the company dealt with the material that was posted using their platforms.

Labour Rights

Online platforms provide multiple opportunities for workers in a digital economy – including matching employees with employers (e.g. LinkedIn and Monster.com) and providing opportunity for flexible “gig” work (e.g. Uber and TaskRabbit). Using platform companies to secure income is becoming increasingly popular. One study from the US found that in the US alone “app economy employment” reached 1.729 million in 2016 – almost four time higher than five years prior.⁵

Workers in online platform markets may benefit from low barriers to entry, new opportunities to earn income, and greater flexibility. At the same time pay, job security, social protection and upskilling options vary greatly and are often poorer than for standard workers.⁶ An example are the legal procedures in several countries to clarify the status of Uber drivers as contractors or employees and their respective coverage by social security schemes. This challenge is compounded by the limited options for collective bargaining and limited protection as for traditional workers, including minimum wage requirements.

Given this new reality, regulators are starting to look at new models to provide “gig” workers with the level of protection needed. In addition, some companies have started to explore opportunities for benefit provisions and collective bargaining (e.g. Hilfr.dk).⁷

³ South Morning Post (2019). “New Zealand shooting: More than 200 users watched live stream video of Christchurch mosque attacks, but nobody reported it, says Facebook.” <https://www.scmp.com/news/asia/australasia/article/3002436/new-zealand-shooting-more-200-users-watched-live-stream-video>

⁴ Christchurch Call: <https://www.christchurchcall.com/>

⁵ OECD (2019)

⁶ idem

⁷ idem

This topic is linked to work from the [OECD Directorate for Employment, Labour and Social Affairs \(ELS\), Skills and Employability Division](#). The ELS team on Future of Work is carrying out a new series of reviews to help countries identify policies that will shape a future of work with fairer access to high quality jobs.

Right to Privacy

Most online platforms benefit from the significant collection and use of user data. This data may include items users are searching for online, products they “like” on Instagram or where they travel using Lyft or Uber. While often required to sign user agreements, most users do not fully understand the depth of data collected and who would have the right to use that data.

The most famous case of improper use of platform company data comes from Cambridge Analytica. In 2016, a researcher at political consulting firm Cambridge Analytica gained access to data on up to 87 million Facebook users through a quiz game app the researcher developed and promoted on Facebook. The data was reportedly used to develop a micro-targeting campaign and techniques to influence political processes and elections without knowledge from and consent of users.⁸

Other cases include requests for user data by government agencies. While many government requests for user data for criminal investigations, law enforcement and other purposes may be legitimate and covered by the law, many social media platforms receive thousands of government requests each year, in some cases from governments with a track record of suppressing freedom of speech and political participation. Given the lack of an international regulatory framework, the Global Network Initiative was launched as an industry-led united approach to protect the privacy of users against government overreach and to push back on illegitimate government requests for both user data and content takedowns.⁹

Additional Human Rights Impacts

In addition to the impacts on privacy and labour rights, platform companies can impact additional human rights including the right to free expression, non-discrimination, the right to information, and the safety and security of persons among others. These risks are especially prominent for social media platforms that allow individuals to communicate at scale in new ways – helping to promote the right to free expression.

Engagement on social media platforms has resulted in some marginalized and vulnerable groups being the recipients of hate speech. For example, Amnesty International reported that Twitter is a “toxic place for women”¹⁰ and that the abuse experienced by female users has resulted in limitations on their free expression and an unequal experience in engaging on the platform. This example and others reveal how vulnerable groups (including ethnic minorities, LGBTI individuals,

⁸ Vox (2018). “The Facebook and Cambridge Analytica scandal, explained with a simple diagram.” <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>

⁹ Global Network Initiative: <https://globalnetworkinitiative.org>

¹⁰ Amnesty International (2018) “Toxic Twitter.” <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>

women, and individuals with disabilities) face amplification of their vulnerabilities given the scale and reach of online platforms.

In addition, social media platforms are also part of the so-called “attention economy”, which incentivises the promotion of content that will keep users engaged on the platform. In Myanmar, this model was found to have contributed to the genocide against Rohingya by allowing the promotion of content by the Myanmar military – potentially resulting in offline violence and even death.¹¹

In part because of the incentives of the attention economy, misinformation has spread through online platforms at staggering rates. According to the OECD “private individuals and groups as well as government have used, and continue to use, online platforms to propagate falsehoods and propaganda for diverse aims, including dividing societies, influencing elections, securing economic gains and recruiting intelligence sources.”¹² One clear example of the adverse impact of misinformation on social media platforms is the spread of anti-vaccination campaigns which may have contributed to a reduction in vaccination rates in certain countries.¹³ Platform companies have taken steps to respond to these risks, but also raise concerns about their role as being the arbiters of truth.

Finally, Platform companies provide new avenues for users to access illicit content, such as child pornography, and conduct illegal activity, such as human trafficking, weapon sales and drug trades. As the OECD pointed out, “online classified ad platforms can be as efficient for marketing trafficked human beings, including children, as they are for marketing books and music.”¹⁴

Of note, in the recent case *Glawischnig v Facebook*, the ECJ ruled that the relevant law, the Directive on electronic commerce (2000/31), does not preclude a court of a Member State from ordering a host provider to remove content previously declared to be unlawful.¹⁵

Competition (Chapter X of the MNE Guidelines)

As platform companies have grown in size and scale, some policy makers, particularly in Europe, have raised questions about potential their consolidation and anti-competitive practices and whether consumers have a real choice in providers. In 2017, for example, the European Commission fined Google EUR 2.4 billion for anti-competitive manipulation of search results by displaying its own shopping service more prominently in search results and in 2019 another fine of EUR 1.4 billion followed for imposing a number of restrictive clauses in contracts with third-party websites which prevented Google's rivals from placing their search adverts on these websites. Another example from the European Commission who announced an investigation into

¹¹ UN Human Rights Council (2018). “Report of the independent international fact-finding mission on Myanmar.”

https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf

¹² OECD (2019)

¹³ The Independent (2019). “Social media fueling anti-vaxxer movement with Europeans the most skeptical in the world, global poll shows.”

www.independent.co.uk/news/health/anti-vaxx-vaccination-myth-poll-europe-pro-nature-birth-a8964441.html

¹⁴ OECD (2019)

¹⁵ <http://curia.europa.eu/juris/document/document.jsf?docid=218621&text=&dir=&doctlang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=8168317> accessed 29/10/19

whether Amazon is violating EU competition law by misusing data collected on third party sellers who use their platform. In the US, a congressional anti-trust investigation regarding Amazon, Apple, Facebook and Google is ongoing.¹⁶

This topic is linked to work from the [OECD Directorate for Financial Affairs, Competition Division](#). The Competition Division is investigating how competition agencies can respond to the challenges posed by platform markets, which are particularly common in the digital economy.

Taxation (Chapter XI of the MNE Guidelines)

Given the global nature of online platforms and the limited physical infrastructure required, online platforms may operate in a way that is not always accounted for in existing taxation frameworks. Some of the largest online retailers, for example, have been criticised for paying lower taxes than their brick and mortar peers.

This topic is linked to work from the [OECD Centre for Tax Policy](#) on providing practical guidance to tax authorities on the design and implementation of revenue collection solutions for digital platforms, including e-commerce marketplaces.

Consumer Protection (Chapter VIII of the MNE Guidelines)

When it comes to consumer protection, it is unclear to what extent platform companies are responsible if one of their users is harmed at the hands of another. For example, if a third-party seller fails to provide a product purchased on the platform, is the platform responsible? Similarly what responsibility would a platform have if the product sold by a third party was unsafe and posed a threat to consumer wellbeing?

Market competition may help correct this, however, as it stands the specific due diligence requirements for platform companies are not always entirely clear and accordingly liability demands are limited. A clear exception to this occurs in the EU where companies who want to benefit from limitations on liability must remove or disable access to illegal listings on their platforms.¹⁷

¹⁶ See <https://judiciary.house.gov/story-type/letter/competition-digital-markets-document-request-91319>

¹⁷ OECD (2019)

Collaborative Solutions

There are opportunities for risk mitigation of harms that may result from online platforms. Here is table summarising some of the challenges and potential strategies:

CHALLENGE	EXAMPLES	OPPORTUNITIES FOR RISK MITIGATION	OPEN QUESTIONS
Content Moderation	<ul style="list-style-type: none"> Broadcasting of extremist content DeepFake media 	<ul style="list-style-type: none"> Investments in scalable detection technology Increasing & incentivising reporting mechanisms 	How can harmful violent content and/or deepfakes be prevented without curtailing the right to free expression?
Protection for Workers	<ul style="list-style-type: none"> Ride sharing app drivers are inhibited from unionising 	<ul style="list-style-type: none"> Public-policy advocacy for worker rights Benefit, collective bargaining, and upskilling programs 	How can the ease of entry into the gig-economy be preserved while institutionalising protection for workers?
User Privacy Data	<ul style="list-style-type: none"> Users are unaware of how their data is being collected and shared 	<ul style="list-style-type: none"> Allowing for selective data collection, such as in-app only location sharing, or access to microphone and camera functions Enabling users to download their own data history Explaining how data will be used, terms & conditions End-to-end encryption Clearing data caches 	How can education surrounding data collection and sharing be brought to scale? What protections can be institutionalised to secure certain data sets?
Non-discrimination	<ul style="list-style-type: none"> Micro-targeting using skewed data in discriminatory marketing programmes Exacerbation of hate speech towards vulnerable communities 	<ul style="list-style-type: none"> Fostering diversity and inclusion within the tech sector Ongoing stakeholder due diligence Moderating hate speech 	To what extent is it appropriate to hold a company accountable for harmful content shared by its users?
The right to information	<ul style="list-style-type: none"> Political disinformation using data / AI systems Highly technical language in terms of service agreements is inaccessible to users 	<ul style="list-style-type: none"> Investments in scalable detection technology Increasing technical literacy among users, especially vulnerable groups Public policy advocacy for regulation of most extreme forms of harm 	What is the role of users and civil society in due diligence?
Safety Security person & of	<ul style="list-style-type: none"> Escalation of online conflict can provoke offline harm Platforms can be used to organise and recruit violent actors Limited protections for workers and users of the gig economy 	<ul style="list-style-type: none"> Monitoring conflict escalation Installing emergency help-lines and reporting mechanisms for workers and users Multi-stakeholder engagement to mitigate misuse of online platforms 	What is the appropriate level of care to ensure security?

Taken together these societal impacts suggest the need for a robust and tailored approach to RBC and a proactive approach to smart regulation to protect platform users and those impacted by platform products and value chains.

Further Reading

1. Amnesty International (2018), “Toxic Twitter.” Available at: <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>
2. Aspen Institute (2019), “Designing Portable Benefits: A Resource Guide for Policymakers.” Available at: <https://www.aspeninstitute.org/publications/designing-portable-benefits/>
3. Cloudflare (2017), “Why we terminated Daily Stormer.” Available at: https://blog.cloudflare.com/why-we-terminated-daily-stormer/?_twitter_impression=true
4. Facebook (2018), “Human Rights Impact Assessment of Myanmar.” Available at: <https://newsroom.fb.com/news/2018/11/myanmar-hria/>
5. Kaye, David (2018), “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” Available at: <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>
6. Medium (2016), “Nine Types of Software Platforms.” Available at: <https://medium.com/platform-hunt/the-8-types-of-software-platforms-473c74f4536a>
7. OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris. Available at: <https://doi.org/10.1787/53e5f593-en>
8. UN Human Rights Council (2018) “Report of the independent international fact-finding mission on Myanmar.” Available at: https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf

This paper was prepared by the OECD Centre for Responsible Business Conduct in the Directorate for Financial and Enterprise Affairs in collaboration with Article One Advisors. It was produced with support from the Government of the Netherlands in order to inform discussions at the OECD workshop on Responsible Business Conduct and Digitalisation taking place on 4 November 2019. The authors are solely responsible for any remaining errors.

This document is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries. This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

© OECD 2019