Economic and Social Council

Sanne van den Brande and Sumneet Kaur

Research Report

The Question of:

Local accountability and taxation of the globally operating web-based service industry

Introduction

The exponential growth of the web-based service, such as Google, Dropbox or Facebook, has gone hand in hand with question regarding accountability and taxation issues. It is often unclear whose laws the companies must adhere to, especially regarding taxation and privacy laws and thus to which laws the companies can be held accountable.

Besides the lack of clarity on who can be held accountable where, and who has to pay taxes to which government, there are many other questions that arise. There is a main question on how to avoid double taxation, but at the same time ensure that the industry pays a fair amount of taxes. A lack of international cooperation makes this difficult. Financial secrecy gives companies the opportunity to hide from other governments what they have and have not payed in taxes.

The lack of international cooperation is also apparent when trying to hold companies accountable for their actions. Countries often lack up-to-date laws on data protection and digital privacy and some lack institutions with the authority to regularly check if companies uphold the law and if those institutions do exist, they often lack the capacity to properly investigate and prosecute any violations.

The Committee

The Economic and Social Council (ECOSOC) was established in 1946 by the UN Charter. It is the central mechanism for the UN system activities and its specialized agencies and supervises the subsidiary in the economic, social and economic fields.

The ECOSOC committee underwent reform in the last decade to strengthen the council and its working methods. It gave attention to the outcomes of all major UN conference summits related to environmental, social and economic fields.

Economic and Social council (ECOSOC) aims to achieve sustainable development goals. It follows the standard rules of procedures, which means it is not an ad-hoc debate. It related work of 15 UN specialized agencies, their functional commissions and five regional commissions. The ECOSOC has 54 members. The General Assembly selects 18 new members for ECOSOC each year for the term of 3 years with a provision that a retiring member can be re-elected. It holds one seven-week session each year in July. ("UN Economic")

Key Terms

The following key terms were used throughout this report:

Web-based Service Industry

The web-based service industry consists of companies that sell their services online, using the Cloud. In varying degrees these services offer individual consumers and companies alike the opportunity to host things online. Some services only offer a way to use certain software online, such as Google Docs. Google Docs allows document editing online without having to install something. Some services host everything online, including servers. These different ranges are called SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) – for more info read this. Individual consumers can use these different services as they please, such as having a Dropbox account or using Google Docs to share documents. Companies can also use these services to host their entire costumer database in the Cloud.

Tax avoidance and evasion

Tax avoidance is the act of trying to avoid paying taxes. The difference between tax avoidance and tax evasion is that the former is using loopholes or tax havens to minimize the amount of taxes a company (or individual) must pay but is otherwise legitimate and legal. Tax evasion is hiding or lying about income, revenue and more to evade taxes, and is illegal.

Though legal, tax avoidance is often considered immoral and frowned upon by the general public. In 2016, the Panama Papers gave a glimpse of the amount of tax avoidance (and in some cases evasion) going on.

Tax Havens

Tax havens are places or countries with very low 'effective' tax rates compared to other places or countries. Though official tax rates can be higher than neighbouring countries or places, due to exemptions, loopholes and other methods to bring down the amount a company effectively has to pay. Tax havens often also offer financial secrecy, meaning it won't pass on information about the financial situation of the company to other governments. Financial secrecy is not required to be considered a tax haven.

Countries that are considered tax havens today include the Netherlands, Ireland, Singapore and the UK, as well as Switzerland, Luxembourg, Panama and much of Caribbean (the Cayman Islands, Bermuda and more). Some countries make the decision to become a tax haven to increase their own tax revenue, as what little taxes the companies do end up paying goes to their treasury, rather than that of another country.

Double taxation

Double taxation refers to when a company has to pay double taxes over something earned only once. If company X is based in country A and sells their goods or services to someone in country B, both A and B have legitimate claims that X has to pay taxes to their government, meaning X would have to pay taxes to both A and B, even though it only sold their product once. Countries realised this is unwanted and as a result started signing tax agreements which try to limit or remove the amount of double taxes a company as to pay.

Financial Secrecy

Countries at times don't share information about what a certain person or company pays in taxes to that country, or what that person or company has in assets in that country. This enables both individuals and companies to hide what they've payed in taxes and/or how much money they have on the bank to other countries, thus potentially enabling tax avoidance or even tax evasion. However, this is not just an issue on tax avoidance, as financial secrecy can also be seen as part of privacy protection.

Accountability

Accountability in short means answerability: the amount to which a person or company has to answer for his/her/its actions and has to take responsibility. It is frequently described as A is accountable to B when A is obliged to inform B about A's (past of future) actions and decisions, to justify those decisions and to suffer punishment in the case of misconduct.[1] In context of this issue, accountability means that web-based service company X knows which laws it must obey, which procedures it must follow, and to which authorities it needs to report to. It also means that company X gets punished if they do not do those things.

Transparency

[1] Schedler, Andreas (1999). "Conceptualizing Accountability". In Andreas Schedler; Larry Diamond; Marc F. Plattner. *The Self-Restraining State: Power and Accountability in New Democracies*. London: Lynne Rienner Publishers. pp. 13–28

Transparency can be defined as official businesses being in efficiency in a way that procedural and substantive information becomes available to them. This is accessible and understandable by people and more specifically groups and society, that are the key towards setting limits to the protection of security and privacy.

General Overview

The rise of internet has blurred many national lines and the question discussed today is one of the foremost questions that needs to be answered. As web-based service companies, such as Google, Facebook, Dropbox and many others work globally and earn revenue globally, it begs the question to which laws they must adhere to. If an individual consumer in Canada uses Google Drive, must Google then adhere to Canadian laws, even though it currently has no data centres in Canada? If the information of that Canadian is stored in a data centre in the US, does Google have to adhere to American law? Could American law enforcement demand access to it? Whose privacy laws does Google need to obey in this case?

Google Drive is free to use to use up to 15 GB, but what if our Canadian buys a subscription to increase that amount? Google is registered in Ireland, its headquarters are in California and it's stock listed in the USA as well. Does the revenue from that subscription fall under Canadian, Irish or American tax law? And who decides which it is?

These questions become even more complicated when dealing with companies using web-based service industry. An insurance company is often subject to very strict privacy laws, as it deals with sensitive information, such as medical history. If that insurance company hosts their database in the Cloud, and the data centre hosting that database is in a different country, whose privacy laws apply? What if those laws contradict each other?

What enables tax avoidance?

For a simple video on the basics of corporate taxes, please view this video.

Corporations pay a lot of taxes over their revenue, profit and others and each country has their own system for dealing with those taxes. This works well if the company stays within the borders of that country, but many corporations now deal in multiple countries. This makes tax systems more complicated, and as a result countries signed tax agreements to deal with taxes. These tax agreements try to reduce 'double taxation'.

This in turn let to companies trying to find loopholes to reduce the amount they have to pay even more. One method Google used was to create a new company 'Alphabet' which holds all the intellectual property of Google. To use the intellectual property (or patents) of another company – which Alphabet now was – Google has to pay them a fee. That fee was roughly the same as the profit Google was making, reducing the profit of Google to nearly zero. As a result, Google had to pay very little in taxes, because it wasn't making a large amount of profit. Alphabet on the other hand, was making a lot of profit. Alphabet was listed in Ireland, but 'managed' in Bermuda, a construction which allowed Alphabet to pay even less taxes to the Irish government. To get a more detailed reconstruction of how Google avoided taxes, please read this article.

The complexity of accountability

As discussed previously, one of the main aspects of accountability is the question of whose laws web-based service companies have to adhere to. Another is who can hold them accountable. If someone from South Africa wants to sue Facebook, can that person go to a South African court, or do they have to go to California?

More and more countries have regulations on how to deal with data protection, but also who should have access to certain data. In some countries, law enforcement demands that they could gain access to information of individuals suspect of some crimes. Other governments have written very strict data protection laws demanding that no one should be able to gain access to the information. If two people from two different countries with conflicting sets of legislation both have an subscription to Netflix and thus are stored in a data center hosted by Amazon, whose laws does Netflix or Amazon have to obey?

In the case of data breaches, who is to be held accountable? Who is held accountable? In a recent data leak millions of Facebook users had their data leaked to hackers, yet Facebook has not (yet) been fined or penalised in any other way by any government, though their stock market prices dropped.

The case of data breaches also shows a lack of transparency. Often it takes a while for companies to announce that there was a breach and that data has been leaked. This poses security issues for any affected customers, as they might not be able to change their passwords on time or try to prevent certain forms of identity theft.

Transparency can also be improved by improving clarity on what happens with the information of users. Facebook and Google sell personal information to third parties, but most consumers don't have a clear idea of what happens with their data. The terms and conditions of use are often so complicated that users don't understand what it says and what they're potentially giving permission for.

Major Parties Involved

China

China, like India, is an important player, though not as vocal on some issues as some other countries. China has the biggest e-commerce market in the world already, and it is growing as more and more citizens gain access to internet and online web shops. China has stopped web-based companies such as Google from operating in China for refusing to limit their search results to those approved by the Chinese government, as well as refusing to share information regarding its users.

EU

The EU is one of the main players in this issue. Controlling a market of over 500 million people, the EU could dictate laws companies would have to adhere to – or lose access to those 500 million people. At the same time, many EU member states, such as Ireland, the Netherlands and the UK are considered tax havens. In terms of data protection, the EU has some of the strongest laws of the big powers, but it is still struggling to deal with enforcing those laws.

Germany

One of the main players in the European Union, Germany has been pushing for both more taxation and stricter privacy laws, though there are voices in Germany urging to not push ahead too much, but rather make international agreements with many partners first.

India

Though not as vocal on this issue as some other countries listed, India is certainly an important player. One of the biggest countries in the world, whose population has more and more access to the internet, India will surely be an important player in the coming years. In 2017, India ordered Google to pay its due taxes, though Google argued that would force them to pay taxes twice. The

Indian courts did not go along with this argument[2], in an important case that showed that double taxation will not always give blanket coverage to aid in tax avoidance.

On the other hand, India has very little data protection laws, and even fewer enforcement capacity, meaning that holding companies accountable is very difficult for them. [3]

Ireland

Ireland is one of the most commonly used tax havens by multiple corporations. There has been debate on whether or not to continue to do this, but the country is reluctant to miss out on the tax revenue those corporations do pay.

The Netherlands

The Netherlands is one of the most commonly used tax havens by multiple corporations. There has been debate on whether or not to continue to do this, but the country is reluctant to miss out on the tax revenue those corporations do pay.

UK

The United Kingdom is often considered a tax haven, though not as often used as Ireland or the Netherlands. As part of the EU – though perhaps not for much longer – it has to find its own balance in dealing with taxation and accountability. Thus far, they have fined several companies in violation of tax laws or data protection laws, but those fines have been comparatively small, showing the need for stronger enforcement.

USA

Home of many of the large internet companies, the USA plays a key role in this issue. It is home to many data centres and many of the companies are stock listed at American stock markets. The USA have a complicated relationship with those companies and other countries regarding the issues. It lobbied against the General Data Protection Regulation by the EU, as it would diminish access to information for them as well. The USA have also failed to impose significant fines for data breaches, showing that they too lack appropriate oversight. Due to the system of the US, it is sometimes unclear who has authority, as sometimes individual states decided, and sometimes federal level institutions make the calls. Tax laws trying to force companies to pay VAT in the states of the buyers have failed,[4] citing that it would be disastrous for small businesses.

Timeline of Events

Though the rise of globally operating web-based service industry is very new, Multinational corporations have been around, and they partly use the same methods of tax avoidance. There have been very few global efforts to hold the web-based service industry accountable and to improve enforcement and taxation, as most countries do this on their own national level.

2007	Founding of Financial Secrecy Index, goes live in 2009
2011	Norway has been the pioneer when it comes to the taxation of the digital economy, and introduced rules in 2011 dictating that companies were subject to Norwegian VAT.[5]

[2] https://trak.in/tags/business/2017/10/25/income-tax-dept-rejects-google-india-tax-rs-1457-crore/

[3] https://medium.com/@privacyint/data-protection-across-the-world-fe66ca1e138f

[4] https://www.reuters.com/article/us-usa-internet-taxation/bill-would-put-brakes-on-u-s-states-rush-to-tax-internet-sales-idUSKCN1LU2RT

[5] https://blog.taxamo.com/insights/digital-tax-rules-in-operation

2012	EU General Data Protection Regulation was first proposed by the European Commission
2014-current	Several countries began to impose new VAT rules, allowing countries to tax companies outside of that country if they sell their products or services to customers in that country.[6]
2015	Single Digital Market Strategy first proposed by the EU
2016	Panama Papers published, showing the widespread use of tax avoidance mechanisms and inciting public outrage
2016	UK imposes a Google Tax
2017	Australia imposes a Google Tax
2017	Equifax breach (fined in 2018 by the UK, in 2018 individual Americans start suing)
2018	The European Commission proposed a new 3% tax on digital sales.

Previous attempts to solve the issue

Attempts to solve the issue have not always come from countries or the UN. NGOs have also been very involved, as has public outrage over tax avoidance and privacy protection breaches. One the earlier attempts to solve the issue was to improve clarity on what was going on. It is not always clear how companies are avoiding taxes or evading accountability, and in 2007 the Financial Secrecy Index (FSI) was founded (it started in 2009) by the Tax Justice Network, a NGO trying to reduce tax evasion, to identify jurisdictions through which corporations were avoiding and evading taxes.

Other NGOs, such as Privacy International, try to protect data and privacy by exposing the exploitation of data, helping countries design legislation to protect online privacy as well as try to reduce the amount of surveillance on citizens. There are, of course, more NGOs and organisations that try to improve taxations and/or accountability of the web-based industry.

Individual countries have also tried to solve the issue. A tax often called the 'Google Tax' has been imposed by both the UK and Australia in 2017 and 2016 respectively. The taxes aim to increase the amount of taxes internet companies have to pay and were implemented after public outrage. Though increasing tax revenue for both countries, the Google Tax also shows the difficulty of the question, as Amazon announced, mere months after the UK announced the Google Tax, that they would start paying their taxes based on British Isle retail rates, ensuring that they could avoid the tax.

The UK and Australia are not the only ones who are imposing taxes on digital businesses. Many countries are demanding that web-based companies pay value added taxes (VAT) on any sale made to an inhabitant of that country. The downside is that each company has to register in each country it has customers. So if a company has only one customer in Albania, it still has to register in Albania to pay taxes. Especially for smaller companies this can become difficult and complicated, as they lack the legal knowhow and expertise to adhere to each countries tax laws. Another issue is that – to avoid double taxation – those companies don't have to pay VAT to their own governments anymore, meaning that those countries miss out on tax revenue. Though this might force web-based service companies to pay VAT taxes to countries where they have customers, it doesn't mean they have to pay other types of taxes, such as profit tax. Though it reduces tax avoidance, it doesn't completely get rid of it.

[6] https://quaderno.io/blog/digital-taxes-around-world-know-new-tax-rules/

A large effort to ensure web-based companies pay their fair share of taxes, the European Union has tried to address this issue a few times. In 2018 a new tax system was proposed, forcing companies to pay a 3% tax if they made money from user data or digital advertising in a country, regardless of any physical presence in that country. This means includes companies as Google, Amazon, but as Uber and Airbnb. One of the more important aspects of this proposal was that it was done by a large bloc of countries: the EU as a whole. Very few web-based companies want to lose out on the European consumer market, so – if enforced correctly – this could force companies to pay at least those 3% in taxes. This does not solve the issue though, especially not for other countries not part of such an important bloc. There is also a question if 3% is enough, and how to prove when companies made money from user data. The proposal goes further than the 3% tax rate though, and is called the Digital Single Market Strategy (DSM), a strategy that according to the European Commission, ensures access to online activities for individuals and businesses alike, under conditions of fair competition, consumer and data protection and removing geo-blocking and copyright issues. This will set privacy laws in the EU at similar levels, improving clarity on which standards companies should adhere to.

Holding web-based service industry accountable, though very complicated, has not gone unaddressed. After it became clear that data had been stolen from a credit bureau named Equifax in 2017, information of 143 million Americans was compromised, as well as 15 million Brits. Though Equifax was fined half a million pounds by the UK government, it has managed to dodge worse penalties from the authorities.[7] It has not, however, managed to dodge people suing Equifax individually through small-claims courts. [8] This requires individual action though, and authorities need to improve mechanisms. Authorities right now are often limited to fining any companies found to be violation of protocols, but the fines are often low compared to the revenue and profit of the companies, and it can be difficult to prove the company was at fault.

Besides starting some oversight organisations, nations have also tried to improve international cooperation regarding accountability. The European Union in 2016 imposed the General Data Protection Regulation[9], regulating data protection for all citizens of the EU, forcing companies to adhere to those laws if they want to keep access to European markets. It took four years for the law to be imposed, after intense lobbying from both businesses and the United States against the proposal.[10]

Though this does not protect individuals from other markets, it shows that international cooperation can force companies to adhere to certain laws – though oversight mechanisms need to be improved.

The Future

Improving tax accountability of the web-based service industry requires, first and foremost, cooperation of all member states. By improving international cooperation, countries might be persuaded to stop being a tax haven. Signing more tax agreements might set a common standard for tax rates and make it more difficult for companies to find methods to avoid paying taxes. Tax havens are legal, as is using them, so some countries might argue that it is within their sovereign right to keep their effective tax rates low.

Improving international cooperation does not just have to come in the form of common tax rates; it can also take the form of reducing financial secrecy. Countries do not share what companies

---

[7] https://techcrunch.com/2018/09/20/equifax-slapped-with-uks-maximum-penalty-over-2017-data-breach/?guccounter=1

[8] https://www.inc.com/bill-murphy-jr/people-are-suing-equifax-in-small-claims-court-its-totally-brilliant-heres-why.html , https://techcrunch.com/2018/09/08/equifax-one-year-later-unscathed/

[9] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[10] https://privacyinternational.org/impact/global-standard-data-protection-law

pay to them in taxes, allowing companies to hide what they have or have not payed to others countries. On the other hand, financial secrecy is also a part of privacy protection, especially when dealing with individuals.

The issue of holding web-based service companies accountable is a relatively new issue, and the legislation regarding online data protection and privacy laws are in many countries outdated. This reduces accountability as it is unclear what laws a company must adhere to.

Some countries lack an institution with national authority, potentially reducing the quality of oversight. Lacking such institution could mean that users with grievances don't know where to go to with their complaints, thus reducing the ability of users to hold the web-based service industry accountable. Lacking a central oversight authority also reduces the quality of oversight and often means that there are no frequent checks on the web-based service industry, allowing any transgressions to go undetected.

One of the difficulties faced by institutions trying to hold web-based service companies accountable is the imbalance of means. Oversight institutions are often overworked and lack the means to be drawn into long legal battles with companies with more means. Google spent more on legal fees than they did on Research and Development in 2012[11] – though those legal fees were not just for tax or privacy cases, but also about patents. Regardless, it shows the capacity of some larger companies to withstand long legal battles until the very end, whereas oversight institutions lack the means to hire experts or keep appealing judicial decisions.

Another accountability issue is that data breaches are sometimes reported weeks after the company first discovered it had been breached, rather than immediately. There is no common strategy or common standard forcing companies to inform those potentially affected by the breach.

To improve accountability one can try to inform the public better than they currently are, or force internet companies to do so. Most users have very little understanding of what companies can do with their information. Instagram, for example, uses facial recognition software to recognise who shows up in photos on an account.[12] This is entirely legal, as users have agreed to it in the terms and conditions of use, but most users are not aware that Instagram – or any other social media platform – uses their information for certain purposes. Improving awareness might be a step to increase transparency and accountability when it comes to data protection.

Important Decisions a Resolution Must Take

There are several main topics a resolution should think about. One of the main questions is regarding international cooperation versus national sovereignty. Each country has the right to set their own tax rates, but the danger is that this enables tax havens to emerge. On the other hand, what right do other countries have to demand that a country changes its tax rates?

A second key issue is how to avoid double taxation, but at the same time combat tax avoidance. Some countries do this by changing how and where VAT have to be payed, but this still begs the question of where profit taxes or corporate taxes have to be payed. Does every country get to decide this for themselves, or should the UN or another collective play a key role in this?

A resolution might also try to find a balance between restricting potential tax avoidance on one hand, and access to markets on the other hand. Currently, more and more countries demand that VAT are payed to the country of the customer, which requires companies to register in those countries. Smaller companies might then lose out on those consumer markets.

A resolution might also try to address finding a balance regarding financial secrecy. As discussed previously, financial secrecy can enable tax avoidance and even tax evasion, but sharing financial

---

[11] https://gizmodo.com/5949909/apple-and-google-spent-more-money-on-legal-fees-than-rd-last-year-and-google-apparently-thinks-apple-wants-it-that-way

[12] https://www.identityguard.com/news-insights/need-know-instagrams-privacy-policy/

information can also be seen as a breach of privacy, especially when it comes to information of individuals.
A resolution might take a look at how to best improve enforcement mechanisms. Can institutions just fine corporations, or are the other penalties that could be imposed? How can international cooperation be improved? International agreements will have to be payed to protect privacy and data and to provide clarity for corporation regarding what they can and cannot do with the information from their users and customers.

Further Reading

https://www.ey.com/Publication/vwLUAssets/EY-cloud-taxation-issues-and-impacts/$FILE/EY-cloud-taxation-issues-and-impacts.pdf

https://www.dlapiperdataprotection.com/

https://www.un.org/press/en/2017/ecosoc6840.doc.htm

https://www.un.org/development/desa/dpad/tag/tax-evasion/

https://www.cnil.fr/en/data-protection-around-the-world

https://quaderno.io/blog/digital-taxes-around-world-know-new-tax-rules/

https://blog.taxamo.com/insights/international-digital-tax-trends

https://blog.taxamo.com/insights/digital-tax-rules-in-operation

Bibliography

https://www.un.org/press/en/2017/ecosoc6840.doc.htm

https://www.theguardian.com/uk-news/2017/nov/23/google-tax-crack-down-avoidance-internet-firms-uk-amazon

https://www.theguardian.com/technology/2015/may/23/amazon-to-begin-paying-corporation-tax-on-uk-retail-sales

https://www.theguardian.com/business/2018/mar/21/facebook-google-and-amazon-to-pay-fair-tax-under-eu-plans

https://www.reuters.com/article/us-eu-tax-digital-germany/germany-still-aims-for-fair-taxation-of-internet-companies-finance-ministry-idUSKCN1LL0ME

http://europa.eu/rapid/press-release_IP-17-3727_en.htm

http://europa.eu/rapid/press-release_MEMO-18-2141_en.htm

https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach

http://europa.eu/rapid/press-release_IP-18-2041_en.htm

https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market