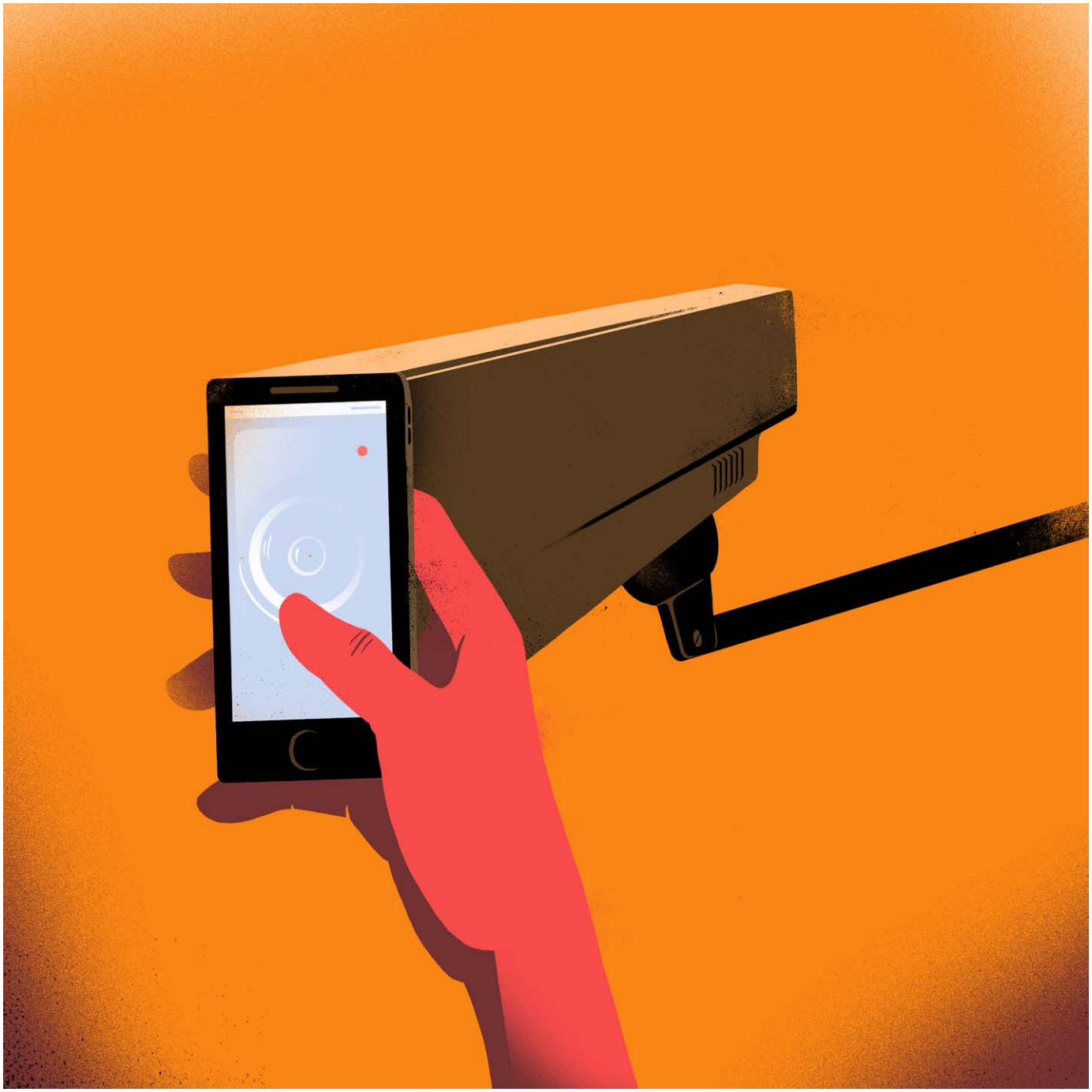


SURVEILLANCE GIANTS:

HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS

AMNESTY INTERNATIONAL

Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

First published in 2019 by Amnesty International Ltd
Peter Benenson House, 1 Easton Street, London WC1X 0DW, UK

Index: POL 30/1404/2019
Original language: English
amnesty.org

All images: © Sebastien Thibault/agoodson.com

AMNESTY INTERNATIONAL

SURVEILLANCE GIANTS:

HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS

CONTENTS

1. EXECUTIVE SUMMARY

The internet has revolutionised our world on a scale not seen since the invention of electricity. Over half of the world's population now relies on the web to read the news, message a loved one, find a job, or seek answers to an urgent question. It has opened social and economic opportunities at a scale and speed that few imagined fifty years ago.

Recognising this shift, it is now firmly acknowledged that access to the internet is vital to enable the enjoyment of human rights. For more than 4 billion people, the internet has become central to how they communicate, learn, participate in the economy, and organise socially and politically.

Yet when these billions participate in life online, most of them rely heavily on the services of just two corporations. Two companies control the primary channels that people rely on to engage with the internet. They provide services so integral that it is difficult to imagine the internet without them.

Facebook is the world's dominant social media company. If you combine users of its social platform, its messenger services, WhatsApp and Messenger, and applications such as Instagram, a third of humans on Earth use a Facebook-owned service every day. Facebook sets terms for much of human connection in the digital age.

A second company, Google, occupies an even larger share of the online world. Search engines are a crucial source of information; Google accounts for around ninety percent of global search engine use. Its browser, Chrome, is the world's dominant web browser. Its video platform, YouTube, is the world's second largest search engine as well as the world's largest video platform. Google's mobile operating system, Android, underpins the vast majority of the world's smartphones.

Android's dominance is particularly important because smartphones have replaced the desktop computer as the primary way people access and use the internet. Smartphones reveal information about us beyond our online browsing habits—such as our physical travel patterns and our location. They often contain thousands of intimate emails and text messages, photographs, contacts, and calendar entries.

Google and Facebook have helped to connect the world and provided crucial services to billions. To participate meaningfully in today's economy and society, and to realise their human rights, people rely on access to the internet—and the tools Google and Facebook offer.

But despite the real value of the services they provide, Google and Facebook's platforms come at a systemic cost. The companies' surveillance-based business model forces people to make a Faustian bargain, whereby they are only able to enjoy their human rights online by submitting to a system predicated on human rights abuse. Firstly, an assault on the right to privacy on an unprecedented scale, and then a series of knock-on effects that pose a serious risk to a range of other rights, from freedom of expression and opinion, to freedom of thought and the right to non-discrimination.

This isn't the internet people signed up for. When Google and Facebook were first starting out two decades ago, both companies had radically different business models that did not depend on ubiquitous surveillance. The gradual erosion of privacy at the hands of Google and Facebook is a direct result of the companies establishing dominant market power and control over the global "public square".

In Chapter 1, 'the Business of Surveillance', this report sets out how the surveillance-based business model works: Google and Facebook offer services to billions of people without asking them to pay a financial fee. Instead, citizens pay for the services with their intimate personal data. After collecting this data, Google and Facebook use it to analyse people, aggregate them into groups, and to make predictions about their interests, characteristics, and ultimately behaviour - primarily so they can use these insights to generate advertising revenue.

This surveillance machinery reaches well beyond the Google search bar or the Facebook platform itself. People are tracked across the web, through the apps on their phones, and in the physical world as well, as they go about their day-to-day affairs.

These two companies collect extensive data on what we search; where we go; who we talk to; what we say; what we read; and, through the analysis made possible by computing advances, have the power to infer what our moods, ethnicities, sexual orientation, political opinions, and vulnerabilities may be. Some of these categories—including characteristics protected under human rights law—are made available to others for the purpose of targeting internet users with advertisements and other information.

In Chapter 2, 'Assault on Privacy', we set out how this ubiquitous surveillance has undermined the very essence of the right to privacy. Not only does it represent an intrusion into billions of people's private lives that can never be necessary or proportionate, but the companies have conditioned access to their services on "consenting" to processing and sharing of their personal data for marketing and advertising, directly countering the right to decide when and how our personal data can be shared with others. Finally, the companies' use of algorithmic systems to create and infer detailed profiles on people interferes with our ability to shape our own identities within a private sphere.

Advertisers were the original beneficiaries of these insights, but once created, the companies' data vaults served as an irresistible temptation for governments as well. This is for a simple reason: Google and Facebook achieved a degree of data extraction from their billions of users that would have been intolerable had governments carried it out directly. Both companies have stood up to states' efforts to obtain information on their users; nevertheless, the opportunity to access such data has created a powerful disincentive for governments to regulate corporate surveillance.

The abuse of privacy that is core to Facebook and Google's surveillance-based business model is starkly demonstrated by the companies' long history of privacy scandals. Despite the companies' assurances over their commitment to privacy, it is difficult not to see these numerous privacy infringements as part of the normal functioning of their business, rather than aberrations.

In Chapter 3, 'Data Analytics at Scale: Human Rights Risks Beyond Privacy', we look at how Google and Facebook's platforms rely not only on extracting vast amounts of people's data, but on drawing further insight and information from that data using sophisticated algorithmic systems. These systems are designed to find the best way to achieve outcomes in the companies' interests, including finely-tuned ad targeting and delivery, and behavioural nudges that keep people engaged on the platforms. As a result, people's data, once aggregated, boomerangs back on them in a host of unforeseen ways.

These algorithmic systems have been shown to have a range of knock-on effects that pose a serious threat to people's rights, including freedom of expression and opinion, freedom of thought, and the right to equality and non-discrimination. These risks are greatly heightened by the size and reach of Google and Facebook's platforms, enabling human rights harm at a population scale. Moreover,

systems that rely on complex data analytics can be opaque even to computer scientists, let alone the billions of people whose data is being processed.

The Cambridge Analytica scandal, in which data from 87 million people's Facebook profiles were harvested and used to micro-target and manipulate people for political campaigning purposes, opened the world's eyes to the capabilities such platforms possess to influence people at scale – and the risk that they could be abused by other actors. However, although shocking, the incident was the tip of the iceberg, stemming from the very same model of data extraction and analysis inherent to both Facebook and Google's business.

Finally, in Chapter 4, 'Concentration of Power Obstructs Accountability', we show how vast data reserves and powerful computational capabilities have made Google and Facebook two of the most valuable and powerful companies in the world today. Google's market capitalization is more than twice the GDP of Ireland (both companies' European headquarters); Facebook's is larger by a third. The companies' business model has helped concentrate their power, including financial clout, political influence, and the ability to shape the digital experience of billions of people, leading to an unprecedented asymmetry of knowledge between the companies and internet users – as scholar Shoshana Zuboff states "They know everything about us; we know almost nothing about them."

This concentrated power goes hand in hand with the human rights impacts of the business model and has created an accountability gap in which it is difficult for governments to hold the companies to account, or for individuals who are affected to access justice.

Governments have an obligation to protect people from human rights abuses by corporations. But for the past two decades, technology companies have been largely left to self-regulate – in 2013, former Google CEO Eric Schmidt described the online world as "the world's largest ungoverned space". However, regulators and national authorities across various jurisdictions have begun to take a more confrontational approach to the concentrated power of Google and Facebook—investigating the companies for competition violations, issuing fines for infringing Europe's General Data Protection Regulation (GDPR), or introducing new tax regimes for big technology companies.

Businesses have a responsibility to respect human rights in the context of their business operations that requires them to carry out "human rights due diligence" to identify and address their human rights impacts. Google and Facebook have established policies and processes to address their impacts on privacy and freedom of expression – but evidently, given that their surveillance-based business model undermines the very essence of the right to privacy and poses a serious risk to a range of other rights, the companies are not taking a holistic approach, nor are they questioning whether their current business models themselves can be compliant with their responsibility to respect human rights.

Amnesty International gave both Google and Facebook an opportunity to respond to the findings of this report in advance of publication. Facebook's letter in response is appended in the annex below. Amnesty International had a conversation with senior Google staff, who subsequently provided information around its relevant policies and practices. Both responses are incorporated throughout the report.

Ultimately, it is now evident that the era of self-regulation in the tech sector is coming to an end: further state-based regulation will be necessary, but it is vital that whatever form future regulation of the technology sector takes, governments follow a human rights-based approach. In the short-term, there is an immediate need for stronger enforcement of existing regulation. Governments must take positive steps to reduce the harms of the surveillance-based business model—to adopt digital public policies that have the objective of universal access and enjoyment of human rights at their core, to reduce or eliminate pervasive private surveillance, and to enact reforms, including structural ones, sufficient to restore confidence and trust in the internet.

1. THE BUSINESS OF SURVEILLANCE

> ***"We don't monetize the things we create…we monetize users."***
>
> Andy Rubin, co-founder of Android, 2013[1]

Every time we interact with the online world, we leave behind a data trace, a digital record of our activity. When we send an email, the content of the message, the time it was sent, who it was sent to, from where, and a host of other information, is recorded and stored in servers and data centres. A similar process happens when we browse the internet, use an app on our phone, or buy something with a credit card. As more and more aspects of our lives are carried out online, and more and more devices, services and infrastructure are connected to the internet - from cars to toasters to factories - the volume of data logged is continuing to grow exponentially.

1. Steven Levy, Wired, *The Inside Story of the Moto X: The Reason Google Bought Motorola*, 8 January 2013

In part, the creation of these data trails is simply a by-product of the functioning of computational technology, which relies on processing digital information. But technology companies have long since known the importance of data, finding that this 'data exhaust' is in fact an extremely valuable resource of information. Often data is described as "the new oil", and while this analogy is flawed,[2] it is certainly the case that Big Tech firms have replaced Big Oil as the world's most valuable companies.[3] The mass harvesting and monetisation of data – primarily for the purpose of advertising – has meant that surveillance has become the "business model of the internet".[4]

'Data' can also sound like an abstract, intangible concept. But simply put, data includes raw facts about our lives and our behaviours, and when processed and organised increasingly reveals a huge amount about our innermost thoughts, behaviours and identities. The protection of personal data has long been recognised as being of fundamental importance to our enjoyment of our right to privacy,[5] a right which in turn protects a space in which we freely express our identity.[6] Unwarranted and undue interference with our personal data is an intrusion into our private lives. It also threatens our ability to freely and independently develop and express thoughts and ideas and leaves us vulnerable to outside influence and control.

This report outlines the human rights implications of the surveillance-based business model that underpins the internet, with a focus on two companies – Google and Facebook. Firstly, this chapter sets out how two companies have pioneered a business model that is predicated on harvesting, analysing and profiting from people's data, often described as "surveillance capitalism".[7] In doing so they have between them established near-total dominance over the primary channels through which people connect and engage with the online world, and access and share information online, making them gatekeepers to the "public square" for much of humanity. This gives them unprecedented corporate power to affect the enjoyment of human rights.

THE BUSINESS MODEL OF GOOGLE AND FACEBOOK

The services provided by Google and Facebook derive revenue from the accumulation and analysis of data about people.[8] Instead of charging a fee for their products or services, these businesses require anyone who wishes to use them to give up their personal data instead.

Facebook and Google (a subsidiary of holding company Alphabet Inc) are multinational conglomerates, and as such their operations vary significantly across a wide array of subsidiaries, products and services. However, both companies share the same core business model, namely to:

---

2. See for example, Bernard Marr, *Here's Why Data Is Not The New Oil,* Forbes, 5 March 2018; Jocelyn Goldfein, Ivy Nguyen, Data is Not the New Oil, Tech Crunch, 27 March 2018

3. Statista, *The 100 largest companies in the world by market value in 2019*, August 2019 https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/

4. Bruce Schneier, *Surveillance is the Business Model of the Internet,* April 2014, https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html

5. *S and Marper v UK, Applications nos. 30562/04 and 30566/04,* European Court of Human Rights, 4 December 2008; and in 1988 in General Comment 16 on the right to privacy (HRI/GEN/1/Rev.9 (Vol. I), the Human Rights Committee (HR Committee) states that "[t]he gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant." (para.10)

6. HR Committee, *Coeriel and Aurik v the Netherlands* (1994), Communication No453/1991, para. 10.2

7. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* 2018 (Zuboff, 2018)

8. Facebook states that its business is not driven by the collection of data about people, and data collection is not an end in itself for the company, but that Facebook is supported through the sale of advertising. See Annex below.

a. develop digital products and services that people find useful and then collect extensive data about people who use or interact with these platforms. However, as outlined in Section 2 below, this includes not only people signed up to their platforms but anyone who encounters the companies' pervasive data tracking across the web.

b. use algorithmic systems to analyse this vast amount of aggregated data, assign detailed profiles to individuals and groups, and predict people's interests and behaviour;

c. sell access to the information to anyone who wishes to target a defined group of people. The primary aim of the companies' business is to sell advertising placements enabling marketers and advertisers to target people online.[9] Importantly, the companies do not sell personal data itself.

Google and Facebook's total revenues come almost entirely from advertising, at 84% and 98% respectively.[10] Their information is so attractive to advertisers that the two companies are often described as having a "duopoly" over the market in online advertising.[11] But it isn't "just ads": the information in their data vaults – as well as the computational insights that Google and Facebook derive from that data – is of intense interest to a host of actors, from companies who set insurance rates to law enforcement agencies.

The rise of "Big Data" and continuous tracking of people's lives online has created a "golden age of surveillance" for states, providing authorities access to detailed information on people's activities that would have been unthinkable in the pre-digital age.[12] At the same time, the surveillance-based business model of Google and Facebook has thrived from a largely hands-off approach to the regulation of the technology industry in key countries such as the United States of America (USA), the companies' home state (see section 4 below).[13] As such, since at least 2001, both public and private surveillance have rapidly expanded in parallel.[14]

DOMINANT POWER OF GOOGLE AND FACEBOOK

The data ecosystem is vast and complex, and composed of an inter-connected network of many different actors across sectors. Among the 'Big Five' tech companies – typically identified as Facebook, Amazon, Apple, Microsoft, and Alphabet's Google – Amazon and Microsoft have to a degree also adopted a version of the business model outlined above.[15] Amazon also dominates the world of e-commerce, and Amazon and Microsoft are the world's leading providers of cloud infrastructure, hosting much of the world's data on their servers.[16] Beyond the well-known brands, there is an extensive network of companies that generate revenue through exploiting data, including 'data brokers' that accumulate and trade data from a variety of sources, and the 'ad-tech' industry that provides

9. Alphabet, *Annual Report on Form 10-K*, 2018, part 1, item 1 available at https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm ; Facebook, *Annual Report on Form 10-K*, 2018, part 1, item 1 available at https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm

10. Reuters, *Google parent Alphabet's revenue misses estimates, rises at slowest pace in 3 years*, 29 April 2019; Facebook, *Second Quarter 2019 Results,* 24 July 2019

11. Shoshana Wodinsky, *The Digital Duopoly Still Reigns the Ad World,* 22 March, 2019

12. Both companies pointed to their policies and transparency reports relating to responding government requests for data in accordance with human rights standards. Google, *Legal process for user data requests FAQs,* https://support.google.com/transparencyreport/answer/7381738; Facebook, *Government Requests for User Data,* https://transparency.facebook.com/government-data-requests

13. Cybersecurity expert Bruce Schneier states "governments don't really want to limit their own access to data by crippling the corporate hand that feeds them". Bruce Schneier, *Data And Goliath,* 2015 (Schneier 2015)

14. Zuboff, 2018, p 115

15. Apple's revenue comes largely from selling technology hardware and consumer services.

16. ZDNet, *Top cloud providers 2019,* August 2019 https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/

the analytics and tools behind digital advertising.[17] Telecoms companies have also pivoted towards adopting targeted advertising technology. Increasingly, companies across a whole range of industries have adopted similar data-driven business models.

However, Google and Facebook, have unparalleled power over people's lives online through having established control over the primary channels that most of the world relies on to engage with the internet. Google and Facebook, and the various companies they own such as YouTube and WhatsApp, mediate the ways people seek and share information, engage in debate, and participate in society. The companies' platforms have become fundamental to the modern world and how people interact with each other.

There are some exceptions across different countries, most notably China. The Chinese government operates an internet "firewall," a technical set of controls that determine what applications Chinese users can access and which websites they can see, that sets it apart from the wider internet economy – and enables the government to maintain a repressive internet censorship and surveillance regime.[18] This means China has a largely separate ecosystem of Chinese internet services, with WeChat and Weibo serving many of the functions of Facebook, and Baidu as the leading search engine in place of Google.

Outside of China, the dominance of Google and Facebook is starkly evident in each of the following areas:

- **Social media:** Facebook dominates social media, with 2.45 billion active users on its main platform each month, accounting for around 70% of social media users, dwarfing its closest rivals.[19]
- **Messaging:** WhatsApp, the messaging app owned by Facebook, together with Facebook Messenger, account for 75% market share in mobile messaging outside China.[20]
- **Search:** Google is by far and away the dominant search engine, with over 90% of all internet searches conducted through Google's platforms.[21] Its corporate name is a synonym for search.
- **Video:** Google-owned YouTube is the second biggest search engine in the world *and* the world's largest video platform.[22]
- **Web browsing:** Google Chrome is the world's dominant browser—making Google the gateway to the entire web.[23]
- **Mobile platforms:** Google's Android is the world's biggest mobile operating system.[24] There are over 2.5 billion monthly active Android devices.[25] This makes Google a constant presence on the single most revealing object in a modern person's life - the smartphone.

---

17. Privacy International, *How do data companies get our data?* 25 May 2018 https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

18. see e.g. Amnesty International, *Annual Report: China Country Profile*, 2017/2018 https://www.amnesty.org/en/countries/asia-and-the-pacific/china/report-china/

19. Facebook, *Company Info,* citing user stats as of 30 September 2019; StatCounter, *Social Media Stats Worldwide*, Oct 2018 - Oct 2019 https://gs.statcounter.com/social-media-stats

20. Statista, *Most popular global mobile messenger apps 2019,* as of July 2019 https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

21. Visual Capitalist, *This Chart Reveals Google's True Dominance Over the Web,* April 2018 https://www.visualcapitalist.com/this-chart-reveals-googles-true-dominance-over-the-web/

22. Mushroom Networks, *YouTube: The 2nd Largest Search Engine,* 2018 https://www.mushroomnetworks.com/infographics/youtube---the-2nd-largest-search-engine-infographic/.

23. Statista, *Global market share held by internet browsers 2012-2019,* as of September 2019, https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/ .

24. StatCounter, *Mobile Operating System Market Share Worldwide,* October 2018- October 2019 https://gs.statcounter.com/os-market-share/mobile/worldwide

25. VentureBeat, *Android passes 2.5 billion monthly active devices,* May 2019 https://venturebeat.com/2019/05/07/android-passes-2-5-billion-monthly-active-devices/

- **Advertising:** Together, Google and Facebook account for more than 60% of online ad revenues worldwide,[26] as well as 90% of growth in the digital ad market.[27]

The power of Google and Facebook over the core platforms of the internet poses unique risks for human rights, as explained in the subsequent sections. As the statistics above show, for most people it is simply not feasible to use the internet while avoiding all Google and Facebook services.[28] The dominant internet platforms are no longer 'optional' in many societies, and using them is a necessary part of participating in modern life.

DATA EXTRACTION AND ACCUMULATION

As we have seen, the business model of Google and Facebook is predicated first and foremost on the extraction and accumulation of vast amounts of data about people. The companies are not only collecting our data, but they are using that data to infer and create new information about us. The platforms are underpinned by state-of-the-art artificial intelligence (AI) and machine learning tools which can infer incredibly detailed characteristics about people and aggregate them into highly specific groupings.

To increase their revenue from advertisers, Google and Facebook compete to offer the best predictions about the most people. To achieve this, they need to expand their data vaults and refine their predictive algorithms. This incentivises the companies to seek more data on more people to expand their operations across the internet, into physical space and, ultimately, across the globe.

This expansionist approach to data extraction takes several forms. Firstly, the companies collect and store extensive data about people.[29] For instance, as a default Google stores search history across all of an individual's devices, information on every app and extension they use, and *all* of their YouTube history,[30] while Facebook collects data about people even if they don't have a Facebook account.[31]

Originally, any data that was created as a by-product of providing an internet service was seen as waste or 'data exhaust'; the discovery that this data in fact revealed significant behavioural insights – and so could be monetised – was a key step in the development of Google and Facebook's surveillance-based business model.[32] This discovery was coupled with the rapid reduction in the cost of storing data, meaning that companies became able to grow their data vaults as a default practice.[33]

Google and Facebook's surveillance-based business model also incentivises "datafication" – rendering into data many aspects of the world that have never been quantified before.[34] As such,

---

26. eMarketer, *Digital Ad Spending 2019, March 2019* https://www.emarketer.com/content/global-digital-ad-spending-2019

27. AdExchanger, *Digital Ad Market Soars To $88 Billion, Facebook And Google Contribute 90% Of Growth*, May 2018 https://adexchanger.com/online-advertising/digital-ad-market-soars-to-88-billion-facebook-and-google-contribute-90-of-growth/.

28. Kashmir Hill, *Goodbye Big Five,* Gizmodo, January 2019, https://gizmodo.com/c/goodbye-big-five

29. Facebook's response (see Annex below) states that the only personal information it requires people to provide when they sign up to Facebook is their "name, age, gender and contact information". However, Facebook also collects a vast amount of data about users after they sign up, such as the content of information people share on Facebook, information about who people are connected to or interact with, and details of people's activities on the platform. See Facebook's Data Policy, https://www.facebook.com/policy.php

30. Dylan Curran, Guardian, *Are you ready? Here is all the data Facebook and Google have on you*, March 2018

31. Facebook, Hard Questions: *What Data Does Facebook Collect When I'm Not Using Facebook, and Why?*, April 2018, https://newsroom.fb.com/news/2018/04/data-off-facebook. Facebook states that it does not build profiles on non-users – see Annex below.

32. Zuboff cites a patent submitted by Google in 2003 to illustrate the company's pivot towards a behavioural targeting model. The patent states "the present invention may involve novel methods, apparatus, message formats, and/or data structures for determining user profile information and using such determined user profile information for ad serving". Shoshana Zuboff, *How Google Discovered the Value of Surveillance*, 2019 https://longreads.com/2019/09/05/how-google-discovered-the-value-of-surveillance/

33. Schneier 2015, p 27

34. Kenneth Neil Cukier and Viktor Mayer-Schoenberger, *The Rise of Big Data: How It's Changing the Way We Think About the World,* Foreign Affairs, May/June 2013, https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data

tracking has begun to include the physical world itself, as the expansion of the 'Internet of Things'[35] creates a physical world studded with ambient sensors. This includes the inside of people's homes through the use of Home Assistants like Google's Assistant and Facebook's Portal, and smart home systems connecting multiple devices such as phones, TVs, and heating systems.[36] Increasingly, data extraction is also stretching to public spaces through 'smart city' infrastructure designed to collect data throughout an urban area.[37] Facebook is even developing technology that would enable tracking the inside of the human brain.[38]

The companies also continuously seek to expand to new international markets (see box below). The starkest example involves Facebook's 'free' internet service, Free Basics, in which Facebook partners with mobile operators in over 65 countries to bring people online. In several countries in the Global South, Free Basics is the internet.[39] An example of Google's expansion drive is Project Dragonfly, the company's attempt to re-enter China's search market - and access data on more than 800 million internet users[40] - until protests by its own employees and human rights groups forced it to terminate the programme.[41]

HARVESTING DATA IN THE GLOBAL SOUTH

Both Facebook and Google have sought to expand their reach in developing countries in the Global South.[42] These emerging markets present Facebook and Google with lucrative opportunities for growth, largely through the potential for expanded access to data.

The Free Basics service is another way in which Facebook can collect masses of data from people in developing countries. According to a recent UN report, "For advertising platforms, such as Google and Facebook, more (local) data would mean opportunities for providing better, targeted advertising...With Facebook's Free Basics, traffic is effectively channelled through a portal, reflecting the reliance of Facebook's business model on a more closed platform."[43] In its response to this report (see Annex), Facebook asserts that "Free Basics does not store information about the things people do or the content they view within any third-party app."

35. The Internet of Things can be described as an expanding network of devices connected via the internet, from smart fridges to smart heating systems, allowing them to communicate to users and developers, applications and each other through collecting and exchanging data from their monitored environment.

36. CNet, *Google calls Nest's hidden microphone an 'error'*, February 2019

37. Real-world surveillance is also the purpose of another Alphabet subsidiary, Sidewalk Labs, which designs 'smart city' technologies and provides them to municipalities. See Ellen P. Goodman, Julia Powles, *Urbanism Under Google: Lessons from Sidewalk Toronto*, Fordham Law Review, May 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3390610

38. TechCrunch, *Facebook is exploring brain control for AR wearables*, July 2019 https://techcrunch.com/2019/07/30/facebook-is-exploring-brain-control-for-ar-wearables/

39. Those in the developing world who can afford to pay for internet service are overwhelmingly likely to be using an Android phone, putting them also under Google's surveillance.

40. China Internet Watch, *China internet users snapshot 2019*, April 2019, citing number of Chinese internet users as of December 2018. Leaked comments by Google's search engine chief Ben Gomes made clear that the Dragonfly project was part of the company's "Next Billion Users" initiative to expand its user base globally. See Ryan Gallagher, *Leaked Transcript Of Private Meeting Contradicts Google's Official Story On China,* The Intercept, 9 October 2018

41. Amnesty International, *Google must fully commit to never censor search in China*, July 2019

42. Wired, *Facebook and Google's race to connect the world is heating up,* 26 July 2018, https://www.wired.co.uk/article/google-project-loon-balloon-facebook-aquila-internet-africa

43. United Nations Conference on Trade and Development, *Digital Economy Report 2019*, September 2019, at: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

According to the Free Basics Privacy Policy, however, they do collect data on use of third-party services to help offer more personalized services, and store information about the services accessed – along with users phone numbers – for ninety days.[44] Free Basics is presented by Facebook as a philanthropic initiative providing an "onramp to the broader internet" for those in the global south who would otherwise lack internet access, Free Basics instead appears to be an "onramp" for increasing data mining in the Global South.[45]

An investigation by Privacy International found that a low-cost mobile phone produced for the Philippines market and using Google's Android operating system lacked adequate security, particularly through the apps pre-installed by the manufacturer, exposing users' data to potential exploitation by scammers, political parties and government agencies.[46] Users in the Global South, for whom such cheaper devices may be the only way to access the internet, are potentially therefore additionally vulnerable to mass surveillance and exploitative data practices.

Google and Facebook are also expanding into new areas that extend the reach of their data collection. Facebook is leading the establishment of a new global cryptocurrency, Libra, a decision which prompted a group of data protection regulators from around the world to raise privacy concerns around combining vast reserves of personal information with financial information.[47] Meanwhile, Google's access to patient data from the UK's National Health Service, first by its DeepMind subsidiary and now directly through its Health division, has been an ongoing source of controversy over the risk that such data could be merged with Google's data vaults.[48] Google also recently acquired fitness tracking company Fitbit, giving it access to one of the world's largest databases of activity, exercise and sleep data".[49]

The drive to expand their data vaults also incentivises the companies to merge and aggregate data across their different platforms, in turn enhancing the platform's power and dominance. In 2012, Google introduced a sweeping change to its privacy policy allowing the company to combine data across its services, prompting a backlash among privacy advocates and regulators.[50] Similarly, when Facebook acquired WhatsApp in 2014, it made public assurances that it would keep the services separate; however, in 2016 the company introduced a controversial privacy policy change allowing it to share data between the two services, including for ad-targeting.[51] Subsequent investigations by

44. Facebook, *Privacy on Free Basics*, at: https://www.facebook.com/legal/internet.org_fbsterms. According to the policy: "In order to make all of this work, we receive and store some limited information - the domain or name of the Third-party Service accessed through Free Basics and the amount of data (e.g. megabytes) used when you access or use that service. This information also helps us improve and personalise your Free Basics experience by enabling us to provide "Most Used" services for easy access. We store this information together with your phone number for only 90 days, after which it is aggregated or otherwise de-identified."

45. Facebook Free Basics https://connectivity.fb.com/free-basics/

46. Privacy International, *Buying a smart phone on the cheap? Privacy might be the price you have to pay*, 20 September 2019, https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay

47. *Joint statement on global privacy expectations of the Libra network*, 5 August 2019 https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf

48. Natasha Lomas, *Google gobbling DeepMind's health app might be the trust shock we need*, TechCrunch, November 2018, https://techcrunch.com/2018/11/14/google-gobbling-deepminds-health-app-might-be-the-trust-shock-we-need/. Google states that NHS Trusts are "in full control of all patient data and we will only use patient data to help improve care, under their oversight and instructions." https://www.blog.google/technology/health/deepmind-health-joins-google-health/

49. Fitbit, *Fitbit to Be Acquired by Google,* 1 November 2019, https://investor.fitbit.com/press/press-releases/press-release-details/2019/Fitbit-to-Be-Acquired-by-Google/default.aspx

50. The Verge, *Google's 2012 privacy policy changes: the backlash and response,* February 2012, https://www.theverge.com/2012/2/1/2763898/google-privacy-policy-changes-terms-of-service-2012

51. Natasha Lomas, *WhatsApp to share user data with Facebook for ad targeting — here's how to opt out*, TechCrunch, August 2016 https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/

European regulators meant Facebook/WhatsApp was forced to backtrack on data sharing between the two services in the EU.[52] Facebook is reportedly planning to integrate Facebook, Messenger, Instagram and WhatsApp even more closely together in future, but the company states that this will not enable the company to aggregate more data about people.[53]

UBIQUITOUS SURVEILLANCE

The wholesale nature of data collection on the internet has been described by cybersecurity expert Bruce Schneier as "ubiquitous surveillance".[54] In practice, this means people are constantly tracked when they go about their day-to-day affairs online, and increasingly in the physical world as well.

The surveillance reaches well beyond the information which users provide when engaging with Google and Facebook, such as email addresses, date of birth and phone numbers, to include location, search history, and app use.

Google and Facebook are the primary trackers of online browsing activity, including search terms, which websites are visited, and from what location. For example, Google collects data via tracking built into the Chrome browser and Android operating system, through any websites that use Google Analytics, and via AdSense, its ubiquitous ad-serving software. Traditionally, Facebook data tracking occurred whenever anybody visits a website containing a Facebook plugin such as the 'Like' button or the 'Share' button, or a hidden piece of code called the Facebook Pixel. In 2018, Facebook stated that "the Like button appeared on 8.4M websites, the Share button appeared on 931K websites, and there were 2.2M Facebook Pixels installed on websites" – and Facebook receives information whenever anybody visits these sites.[55]

In Facebook's response to this report (see Annex), they clarify that "other than for security purposes and guarding against fraud, Facebook no longer stores data from social plugins (such as the Like Button) with user or device identifiers." However, Facebook's Data Policy makes clear that the company at least still receives such data: "Advertisers, app developers and publishers can send us information through Facebook Business Tools that they use, including our social plugins…These partners provide information about your activities off Facebook…whether or not you have a Facebook account or are logged in to Facebook."[56]

Smart phones are increasingly the primary way that people connect to the internet, and offer a rich source of data, including location data as well as data from all the apps and services the phone offers.[57]

---

52. UK Information Commissioner's Office, *A win for the data protection of UK consumers*, March 2018, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/blog-a-win-for-the-data-protection-of-uk-consumers/

53. Mike Isaac, *Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger*, New York Times, 25 January 2019, https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html ; See Facebook letter to Amnesty International, in Annex below.

54. Schneier 2015, p 38

55. Rebecca Stimson, Head of Public Policy, Facebook UK, *Letter to Chair of UK House of Commons Digital, Culture, Media and Sport Committee*, 14 May 2018, p 2 https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/180514-Rebecca-Stimson-Facebook-to-Ctte-Chair-re-oral-ev-follow-up.pdf

56. Facebook Data Policy, https://www.facebook.com/policy.php. Facebook's cookie policy also states that "We may place cookies on your computer or device, and receive information stored in cookies, when you use or visit… Websites and apps provided by other companies that use the Facebook Products…Facebook uses cookies and receives information when you visit those sites and apps, including device information and information about your activity, without any further action from you. This occurs whether or not you have a Facebook account or are logged in." https://www.facebook.com/policies/cookies

57. World Advertising Research Center (WARC), *Almost three quarters of internet users will be mobile-only by 2025*, January 2019; A New York Times study of smartphone location tracking revealed that an extensive quantity of intimate location data is for sale. *See Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, 10 December 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

The vast majority of smart phones use Google's Android operating system - one study found that an idle Android phone sent Google 900 data points over the course of 24 hours, including location data.[58] Sensorvault, Google's database of location data from Android phones, includes "detailed location records involving at least hundreds of millions of devices worldwide and dating back nearly a decade."[59] Facebook also tracks users on Android through its apps, including logging people's call and SMS history - although the company has stated it only does so with user consent.[60] Furthermore, other Android apps also share data with Facebook.[61]

Importantly, the information collected by Facebook and Google includes not only data itself but metadata, or "data about data". This includes for example email recipients, location records, and the timestamp on emails and photos. The growing use of end-to-end encryption for messaging, for example on WhatsApp, means nowadays even the companies themselves are often unable to access the content of communications. However, it is well recognised that metadata constitutes "information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."[62] The Office of the UN High Commissioner for Human Rights (OHCHR) has recognised that when analysed and aggregated, metadata "may give an insight into an individual's behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication."[63]

Moreover, while the content of data is very revealing when targeting an individual or small group of people, when harvested at the scale of Facebook and Google, metadata in fact is far more valuable, enabling complex analytics to predict patterns of behaviour at a population scale[64] and potentially could be used to infer sensitive information about a person, such as their sexual identity, political views, personality traits, or sexual orientation using sophisticated algorithmic models.[65] These inferences can be derived regardless of the data provided by the user and they often control how individuals are viewed and evaluated by third parties: for example, in the past third parties have used such data to control who sees rental ads[66] and to decide on eligibility for loans.[67]

---

58. Professor Douglas C. Schmidt, Vanderbilt University, *Google Data Collection*, Digital Content Next, August 2018, para 24 https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

59. According to Google employees cited in The New York Times, *Tracking Phones, Google Is a Dragnet for the Police,* April 2019 https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

60. UK House of Commons Digital, Culture, Media and Sport Committee, *Final Report on Disinformation and 'fake news'*, February 2019, p 35; Facebook, *Fact Check: Your Call and SMS History,* 25 March 2018 https://newsroom.fb.com/news/2018/03/fact-check-your-call-and-sms-history/

61. Privacy International, *How Apps on Android Share Data with Facebook,* December 2018. The study found that 61 percent of apps tested automatically transfer data to Facebook the moment a user opens the app; subsequently, a number of apps ended the practice. https://privacyinternational.org/appdata

62. *Tele2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970) (*"Watson"*) Court of Justice of the European Union, Joined Cases C-203/15 at para. 99, http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

63. Report of the OHCHR on the right to privacy in the digital age, 30 June 2014, A/HRC/27/37, para.19.

64. This is the reason why WhatsApp is immensely valuable. Unlike Facebook's other platforms, there is no advertising on WhatsApp, and because of end-to-end encryption Facebook cannot access the content of the messages on the platform, but it provides Facebook with a trove of data – including location information, contact lists, and metadata on more than 65 billion messages per day.

65. Privacy International, *Examples of Data Points Used in Profiling,* April 2018, https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf ; Facebook states that it does not infer people's sexual identity, personality traits, or sexual orientation – see Annex below.

66. Julia Angwin, Ariana Tobin and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race,* ProPublica, November 2017. In March 2019, Facebook announced restrictions to targeting options for housing, employment, or credit ads in the USA as part of a settlement with civil right organisations.

67. Astra Taylor and Jathan Sadowski, How Companies Turn Your Facebook Activity Into a Credit Score, The Nation, May 2015, https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/

BUSINESS AND HUMAN RIGHTS

Under international human rights law, states are the primary duty bearers of human rights and have a duty to protect against right abuses by third parties like corporations. The Human Rights Council has affirmed that the same rights people have offline must also be protected online, and that states should create and maintain an "enabling online environment" for the enjoyment of human rights.[68]

Companies have a responsibility to respect all human rights that exists independently of a state's ability or willingness to fulfil its own human rights obligations, and also exists over and above compliance with national laws and regulations.[69] Standards on business and human rights, like the UN Guiding Principles on Business and Human Rights, establish "global standard[s] of expected conduct" that apply throughout a company's operations.[70]

As part of fulfilling this responsibility, companies need to have a policy commitment to respect human rights, and take ongoing, pro-active and reactive steps to ensure that they do not cause or contribute to human rights abuses – a process called human rights due diligence. Human rights due diligence requires companies to identify human rights impacts linked to their operations (both potential and actual), take effective action to prevent and mitigate against them, and be transparent about their efforts in this regard. This includes addressing high-level risks of adverse human rights impacts prevalent within a sector because of characteristics of that sector.[71]

68. UN Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet,* July 2018, UN Doc: A/HRC/38/L.10/Rev.1

69. UN Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, 2011, UN Doc HR/PUB/11/04, (Guiding Principles) www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

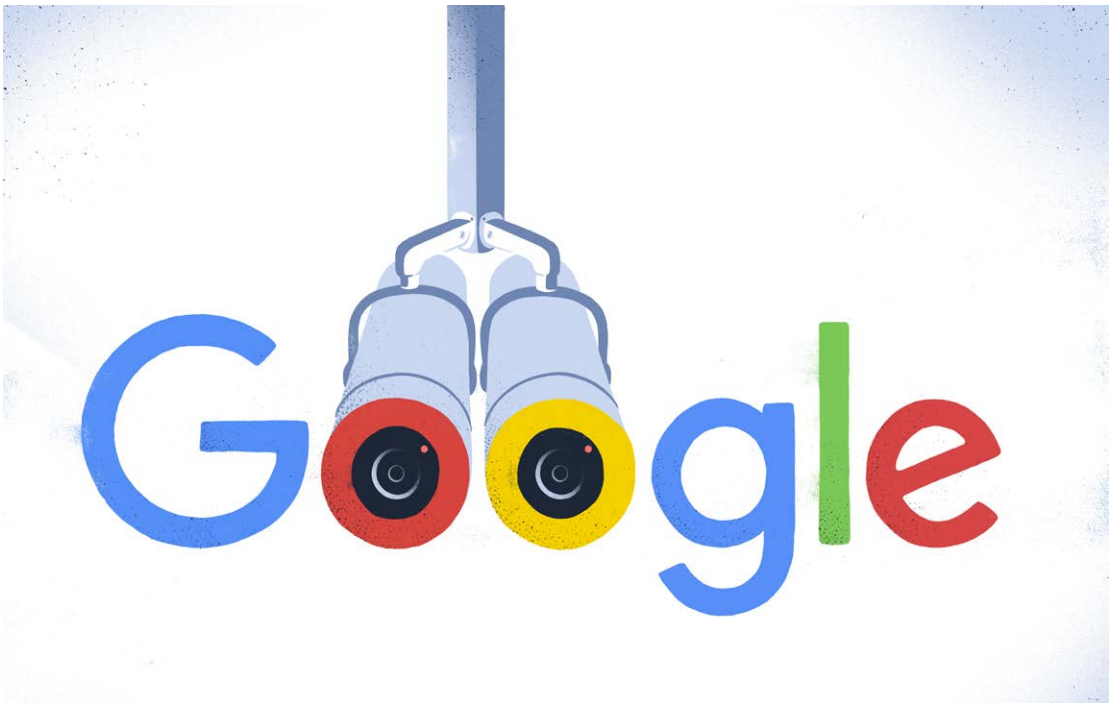
70. Guiding Principles, principle 11

71. OECD Due Diligence Guidance For Responsible Business Conduct, Section II, 2.1, Annex Question 22

2. ASSAULT ON PRIVACY

> ***"We know where you are. We know where you've been. We can more or less know what you're thinking about".***
>
> Eric Schmidt, former Google CEO, 2010[72]

Privacy advocates have been voicing criticism of Google and Facebook for years, and over the past two decades the companies have faced multiple privacy scandals related to their use of personal data. Nevertheless, the companies have continued to expand the scope and depth of their data extraction and processing, creating the current architecture of surveillance outlined above.



72. The Atlantic, Google's CEO: *'The Laws Are Written by Lobbyists'*, October 2010, https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/

In 2010 Facebook CEO Mark Zuckerberg famously declared that social media had changed privacy "as a social norm".[73] In fact, the rise of digital technologies has made privacy an even more important right in the modern world; but Google and Facebook's business model undermines the very essence of the right to privacy itself.

Facebook has made clear that it "strongly disagrees" with the characterisation of its business model as "surveillance-based", arguing that the use of its products is entirely voluntary and therefore different from involuntary government surveillance as envisaged under the right to privacy.[74] However, it is well established in international human rights law that the right to privacy must be guaranteed against arbitrary interferences "whether they emanate from State authorities or from natural or legal persons [such as corporations]."[75] This section outlines how Google and Facebook's current business is fundamentally incompatible with this right.

THE SURVEILLANCE-BASED BUSINESS MODEL AND THE RIGHT TO PRIVACY

The right to privacy provides that no one should be subject to "arbitrary or unlawful interference" with their privacy, family, home or correspondence, and this should be protected by law.[76] The Human Rights Committee has long recognised that such protection includes regulating "the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies."[77]

The scope of privacy has always evolved in response to societal change, particularly new technological developments. The OHCHR has stated that "[p]rivacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."[78] This encompasses three inter-related concepts: the freedom from intrusion into our private lives, the right to control information about ourselves, and the right to a space in which we can freely express our identities. The surveillance-based nature of Google and Facebook's business model undermines each of these three elements to such an extent that it has undermined the very essence of privacy.

The UNHCHR has recognised that "even the mere generation and collection of data relating to a person's identity, family or life already affects the right to privacy, as through those steps an individual loses some control over information that could put his or her privacy at risk."[79] The scale of the data collected by Google and Facebook means that these companies are amassing more information on

73. Ann Cavoukian, (then) Information and Privacy Commissioner of Ontario, *Privacy is still a social norm*, The Globe and Mail, March 2010 https://www.theglobeandmail.com/opinion/privacy-is-still-a-social-norm/article1209523/

74. Facebook letter to Amnesty International, November 2019 – see Annex below.

75. UN Human Rights Committee, General Comment No. 16 on the right to privacy, HRI/GEN/1/Rev.9 (Vol. I), 1988, para 1. The UN Guiding Principles on business and human rights also make clear that companies have a responsibility to respect "the entire spectrum of internationally recognized human rights" (Principle 12).

76. Universal Declaration of Human Rights, Article 12; International Covenant on Civil and Political Rights, Article 17

77. UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, https://www.refworld.org/docid/453883f922.html

78. UN High Commissioner for Human Rights, *The right to privacy in the digital age*, 3 August 2018, A/HRC/39/29, para.5.

79. A/HRC/39/29, para.7; see also A/HRC/27/37, para.20; and European Court of Human Rights, *Weber and Saravia v. Germany,* para. 78; *Malone v. UK,* para. 64.

human beings and human activity than previously imaginable. The aggregation of so much data, combined with the use of sophisticated data analysis tools, can reveal very intimate and detailed information; in effect, the companies can know virtually everything about an individual.[80]

Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful. Human rights mechanisms have consistently interpreted those words as pointing to the overarching principles of legality, necessity and proportionality.[81] Indiscriminate corporate surveillance on such a scale is inherently unnecessary and disproportionate and can never be a permissible interference with the right to privacy. As a comparison, where States have claimed that indiscriminate mass surveillance is necessary to protect national security, human rights mechanisms have stated that this practice "is not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures."[82]

The second component of privacy provides that people have the right to control their personal information, or the right to "informational self-determination",[83] to be able to decide when and how our personal data can be shared with others.[84] This forms the foundation for data protection, which has become increasingly important since the rise of large-scale databases and the advancement of computational technologies. The European Court of Human Rights has recognised that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to privacy,[85] and that privacy provides for the right to a form of informational self-determination.[86] The surveillance-based business model directly conflicts with the fundamental principles underpinning this second component and thereby undermines people's ability to exercise control over their personal information, including having a free choice as to the ways and reasons for which their personal data is used (see inset box below).

DATA PROTECTION

The EU's General Data Protection Regulation (GDPR), which came into force in May 2018, has become a global benchmark for data protection and privacy regulation. Google and Facebook are bound by the GDPR, which applies to all organisations located within the EU and also to those outside if they offer services to, or monitor the behaviour of, individuals who are located in the EU.

80. Privacy International, *A Snapshot of Corporate Profiling,* April 2018, https://privacyinternational.org/long-read/1721/snapshot-corporate-profiling

81. A/HRC/27/37, paras.21-27.

82. Report of the OHCHR on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism, 21 July 2016, A/HRC/33/29, para.58; see also Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 23 September 2014, A/69/397, para.47; and A/HRC/27/37, para.25

83. The term "informational self-determination" was first used in the context of a German constitutional ruling relating to personal information collecting during the 1983 census: Bundesverfassungsgericht [BVerfG], Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1. It was understood by the Court as the authority of the individual to decide when and within what restrictions information about their private life should be communicated to others.

84. Alan Westin, Privacy and Freedom, 1967

85. *S and Marper v UK*, Applications nos. 30562/04 and 30566/04, European Court of Human Rights (ECtHR), 4 December 2008 available at http://hudoc.echr.coe.int/eng?i=001-90051.

86. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application no. 931/13, ECtHR, 27 June 2017, at para.137, available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175121%22]}.

Importantly, the regulation defines personal data broadly as 'any information relating to an identified or identifiable natural person'.[87] The definition includes data relating to an individual who can be identified directly or indirectly from the data in question.[88] The GDPR makes clear that personal data which has been pseudonymised, which could however be attributed to an individual by the use of additional information should be considered information on an identifiable person.[89] Inferred and predicted data similarly count as "personal data" if they are linked to unique identifiers or are otherwise attributable to an identifiable natural person.

One of the key principles in the GDPR is that of "purpose limitation", which requires that companies collecting and processing personal data are clear about their purpose of processing from the start, that they record these purposes and specify them in their privacy information for individuals, and that they only use personal data for a new purpose if this is compatible with their original purpose, they obtain the individual's consent, or they have another clear basis in law.[90]

The GDPR also sets a high standard for consent – it means a freely given, specific, informed and unambiguous indication of an individual's wishes by which they, by a clear affirmative action, signifies agreement to the processing of personal data relating to them.[91] The GDPR makes clear that when the processing has multiple purposes, consent should be given for all of them,[92] and that to ensure that consent is freely given, it should not provide a valid legal ground for the processing of personal data where there is a clear imbalance between a controller and the individual.[93] In contradiction with the requirement that consent is freely given, the surveillance-based business model makes use of services conditional on individuals giving consent for the processing and sharing of their personal data for marketing and advertising, which means that an individual is unable to refuse or withdraw consent without being excluded from these spaces.[94]

Finally, there is a broad consensus that privacy is also fundamental in creating and protecting the space necessary to construct our own identities.[95] The UN Human Rights Committee (HRC) has defined privacy as "a sphere of a person's life in which he or she can freely express his or her identity".[96] This reflects an understanding that our sense of identity is both socially constructed and dynamic: we display different sides of ourselves in different contexts, whether it is with our friends, at work or in public, and this is constantly shifting and adapting. Privacy enables us to decide for ourselves how others see us – and we behave differently when we are subjected to unwanted observation. In this sense, privacy is essential for autonomy and the ability to determine our own identity.

87. GDPR, article 4(1).

88. *Ibid.*

89. GDPR, Recital 26.

90. See GDPR, articles 5(1)(b), 6(4) and 30, and Recitals 39 and 50.

91. GDPR, article 4(11).

92. See GDPR, articles 6(1)(a), 7, and Recital 32.

93. GDPR Recital 43

94. Such 'forced consent' is currently subject to legal challenge under the European General Data Protection Regulation brought against Google and Facebook by consumer rights organisation Noyb: https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.

95. See for example, Agre and Rotenburg (eds), *Technology and Privacy: The New Landscape*, 1998; Julie E. Cohen, 2013

96. Human Rights Committee, *Coeriel and Aurik v the Netherlands* (1994), Communication No453/1991, para. 10.2

People who are under constant surveillance face pressure to conform. Privacy's key role in shaping different identities encourages a diversity of culture. Having layered identities is often the core condition of any minority group seeking to live, work, and subsist in a dominant culture. It can be true, for example, of LGBTI people living in a culture where same-sex intimate conduct is stigmatised or illegal; it can also be true of LGBTI people who do not live in those cultures but with extended family who do.[97] It can also be the characteristic of someone engaged in a vulnerable part of the irregular economy, such as sex work.[98]

The sheer scale of the intrusion of Google and Facebook's business model into our private lives through ubiquitous and constant surveillance has massively shrunk the space necessary for us to define who we are. Privacy protects against "the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable".[99] But the very nature of targeting, using data to infer detailed characteristics about people, means that Google and Facebook are defining our identity to the outside world, often in a host of rights-impacting contexts. This intrudes into our private lives and directly contradicts our right to informational self-determination, to define our own identities within a sphere of privacy.

Put simply, surveillance on such a scale represents an unprecedented interference with the right to privacy, that cannot be compatible with the companies' responsibility to respect human rights. This goes beyond an intrusion into every aspect of our lives online, and in fact threatens our right to shape and define who we are as autonomous individuals in society.

PRIOR PROMISES OF PRIVACY; PRIOR FAILURES TO RESPECT PRIVACY

Recently, the executives at the head of Google and Facebook acknowledged the right to privacy in public statements. In May, Google CEO Sundar Pichai published an op-ed about privacy.[100] In March, Facebook CEO Mark Zuckerberg announced that Facebook would pivot to privacy,[101] and in May gave his main annual speech in front of a sign that read "the future is private."[102]

As part of this drive, both companies have announced new measures with the aim of giving users greater control over their privacy on the platforms.[103] In November, Google announced it would put in place greater restrictions on the data that it shares with advertisers through its ad auction platform, following the launch of an inquiry by the Irish Data protection authority into the processing of personal data in the context of Google's online Ad Exchange.[104] Google has also launched a new feature allowing

97. *See* Alexander Dhoest and Lukasz Szulc, *Navigating online selves: social, cultural, and material contexts of social media use by diasporic gay men*, Social Media + Society, 2016, http://eprints.lse.ac.uk/87145/1/Szulc_Navigating%20online%20selves_2018.pdf

98. Kashmir Hill, *How Facebook Outs Sex Workers,* Gizmodo, November 2017, https://gizmodo.com/how-facebook-outs-sex-workers-1818861596

99. Julie E. Cohen, 2013

100. Sundar Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, New York Times, 7 May 2019

101. Facebook, *A Privacy-Focused Vision for Social Networking*, 6 March 2019, https://newsroom.fb.com/news/2019/03/vision-for-social-networking/

102. Kurt Wagner and Selina Wang, *Facebook's Zuckerberg Preaches Privacy, But Evidence Is Elusive*, Bloomberg, 1 May 2019

103. Both companies also pointed to the tools that they offer users to control their ad preferences. See Google, *Control the ads you see,* https://support.google.com/accounts/answer/2662856; Facebook https://facebook.com/help/247395082112892

104. Google, *Additional steps to safeguard user privacy,* 14 November 2019, https://www.blog.google/products/admanager/additional-steps-safeguard-user-privacy; Irish Data Protection Commission, *Data Protection Commission opens statutory inquiry into Google Ireland Limited,* 22 May 2019

users to delete location data (although only after being kept for a minimum of three months).[105] Facebook started rolling out a tool enabling people to see information other apps and websites share with Facebook, and disconnect the data from their account (but not delete it entirely).[106]

While this may be a positive augur of better privacy practices, many commentators have expressed scepticism at the idea that Google and Facebook will fundamentally change when their business model and position as two of the world's biggest public companies are predicated on surveillance.[107] In July 2019, the US Federal Trade Commission reached a settlement with Facebook over privacy violations that force the company to restructure its approach to privacy and submit to a range of new privacy requirements and oversight.[108] However, as outlined further in Section 4 below, these changes fail to challenge the company's underlying business model or fully address its inherent impacts on privacy.

The companies' long history of privacy scandals and broken promises around privacy starkly illustrate the impacts of the surveillance-based business model on privacy and raises questions about their promises to change that model.

Both Google and Facebook have faced public criticism for their privacy practices dating back over a decade. In 2007, Facebook's first effort to install invasive advertising on its platform, called Beacon, was so unpopular it had to be withdrawn.[109] There have been similar public outcries over Gmail ad targeting for many years, and the company announced in 2017 it would no longer scan emails to target advertisements.[110] When sufficient numbers of people are aware of this surveillance, they have complained, and the companies have tended to apologise—but meanwhile, the business model has trended inexorably toward maximal surveillance, as outlined above.

Google and Facebook have also previously engaged in practices that mislead users about privacy and their advertisement targeting practices. A few examples:

Google and Facebook have also previously engaged in practices that mislead users about privacy and their advertisement targeting practices. A few examples:

- During the development of Google Street View in 2010, Google's photography cars secretly captured private email messages and passwords from unsecured wireless networks.[111]
- In 2018 journalists discovered that Google keeps location tracking on even when you have disabled it. Google subsequently revised the description of this function after the news story but has not disabled location tracking even after users turn off Location History.[112] Google now faces legal action by Australia's competition watchdog over the issue.[113]

---

105. Google, *Introducing auto-delete controls for your Location History and activity data,* 1 May 2019, https://www.blog.google/technology/safety-security/automatically-delete-data . Google also pointed to its work to develop federated learning technology, see https://federated.withgoogle.com/.

106. Facebook, *Now You Can See and Control the Data That Apps and Websites Share With Facebook,* 20 August 2019, https://about.fb.com/news/2019/08/off-facebook-activity/

107. As Shoshana Zuboff puts it, "How can we expect companies whose economic existence depends upon behavioral surplus to cease capturing behavioral data voluntarily? It's like asking for suicide." Zuboff, *The Secrets of Surveillance Capitalism,* Frankfurter Allgemeine, March 2016; See also e.g. Bruce Schneier, *A New Privacy Constitution for Facebook,* 8 March 2019; Casey Johnston, *Facebook is trying to make the word "private" meaningless,* The Outline, 1 May 2019; Julia Carrie Wong, *My data security is better than yours: tech CEOs throw shade in privacy wars*, 9 May 2019

108. Facebook, *A New Framework for Protecting Privacy,* 24 July 2019, https://about.fb.com/news/2019/07/ftc-agreement/

109. The Register, *Facebook turns out light on Beacon,* 23 September 2009

110. Google, *As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align,* 23 June 2017

111. Guardian (UK), *Google admits collecting Wi-Fi data through Street View cars*, 15 May 2010, https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data

112. Associated Press, *Google clarifies location-tracking policy,* August 2018, https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211

113. Australian Competition and Consumer Commission, *Google allegedly misled consumers on collection and use of location data*, 29 October 2019, https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data

- In early 2019 journalists discovered that Google's Nest 'smart home' devices contained a microphone they failed to inform the public about.[114]
- Facebook has acknowledged that it knew about the data abuses of political micro-targeting firm Cambridge Analytica months before the scandal broke (see box in Section 3 below).[115]
- Facebook, through an app called Facebook Research, previously paid teenagers to download an app that tracked everything they do on their phones.[116]
- Facebook has also acknowledged performing behavioural experiments on groups of people—nudging groups of voters to vote, for example, or lifting (or depressing) users' moods by showing them different posts on their feed.[117]

It is difficult not to draw the conclusion that the companies' numerous privacy abuses are not aberrations, but in fact demonstrate exactly how Google and Facebook's surveillance-based model is predicated on their ability to harvest, analyse and sell huge amounts of data while disregarding the right to privacy.

STATES' ACCESS TO GOOGLE AND FACEBOOK'S DATA VAULTS

"You must assume that any personal data that Facebook or Android keeps are data that governments around the world will try to get or that thieves will try to steal."

Tim Wu, 2019[118]

In addition to the direct impacts that the surveillance-based business model has on privacy, there is also a risk of indirect impacts through the relationship between corporate surveillance and state surveillance programmes. State authorities, such as intelligence agencies, law enforcement and immigration agencies, are increasingly seeking to gain access to data held by technology companies.[119] The vast vaults of data that Google and Facebook hold about people represent a centralized 'honeypot' – an opportunity for state authorities to access highly valuable personal data that would otherwise be very difficult to assemble.

As such, the model poses an inherent risk that Google and Facebook could contribute to invasive and unlawful digital surveillance by states or their targeting of people in a way that amounts to rights abuses. Although this risk exists for all companies that amass large vaults of personal data, the surveillance-based business model of Google and Facebook incentivises the companies to collect and hold as much data as possible in order to increase their revenues, greatly increasing the risk.

---

114. The Verge, *Google claims built-in Nest mic was 'never intended to be a secret',* February 2019 https://www.theverge.com/circuitbreaker/2019/2/20/18232960/google-nest-secure-microphone-google-assistant-built-in-security-privacy

115. Guardian (UK), *Facebook acknowledges concerns over Cambridge Analytica emerged earlier than reported,* 22 March 2019, https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing

116. Josh Constine, *Facebook admits 18% of Research spyware users were teens, not <5%,* TechCrunch, 28 February 2019, https://techcrunch.com/2019/02/28/facebook-research-teens/

117. Christian Science Monitor, *Facebook 'I Voted' button experiment: praiseworthy or propaganda?*, November 2014; Guardian (UK), *Facebook reveals news feed experiment to control emotions,* June 2014

118. Tim Wu, author of 'The Attention Merchants', *How Capitalism Betrayed Privacy*, New York Times, 10 April 2019, https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html

119. see for example, CNBC, *US, UK sign first-ever deal to access data from tech companies like Facebook and Google,* October 2019, https://www.cnbc.com/2019/10/04/us-uk-sign-agreement-to-access-data-from-tech-companies-like-facebook.html ; Jennifer Lynch, EFF, *Google's Sensorvault Can Tell Police Where You've Been*, April 2018, https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been

The revelations of mass surveillance exposed by former US National Security Agency (NSA) whistle-blower Edward Snowden demonstrated the ways that intelligence agencies had been able to access tech companies' data. US intelligence documents disclosed by Snowden in 2013 exposed how US and UK intelligence agencies conducted indiscriminate surveillance on a vast scale – and how companies including Yahoo, Google and Microsoft faced secret legal orders to hand over their customers' data.[120] The NSA was also able to circumvent security protections of Google and Yahoo to gain access to the companies' data centres.[121]

In the wake of the Snowden revelations, technology companies have expanded their use of encryption to protect user data and have mounted legal challenges against state requests for user data, such as the US Government's use of secrecy orders preventing companies from disclosing certain types of legal demands for information.[122] Both Google and Facebook are members of the Reform Government Surveillance Coalition (RGS), advocating reform of the laws and practices regulating government surveillance.[123] These are welcome measures, but they do not address the underlying source of the problem, which is that the surveillance-based business model incentivises large scale data harvesting and processing in a way that hugely expands the opportunities for state surveillance.

HUMAN RIGHTS AT GOOGLE AND FACEBOOK

In line with international human rights standards, Google and Facebook should be carrying out due diligence to identify and address the potential and actual impacts of their business model on specific human rights, including the rights to privacy and freedom of expression.[124] However, the fact that the harvesting, analysis and monetisation of data is so core to their business model, has such a fundamental and widespread impact on the right to privacy, and is so inherently at odds with the enjoyment of this right, means that the companies should also be assessing whether their surveillance-based business model can ever be compatible with their responsibility to respect human rights.

Google and Facebook have both made a longstanding commitment to the rights to privacy and freedom of expression through participation in the Global Network Initiative (GNI).[125] However, the scope of the GNI means it does not address risks to other rights beyond freedom of expression and privacy; it is also primarily focused on how companies respond to government requests for data.

Through the GNI, both companies are subject to independent assessments every two years of their relevant internal systems, policies and procedures. The most recent assessment published in July

120. Ewen MacAskill and Dominic Rushe, *Snowden document reveals key role of companies in NSA data collection*, Guardian (UK), November 2013 https://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms

121. Barton Gellman and Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say,* The Washington Post, October 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

122. Washington Post, *Google challenges U.S. gag order, citing First Amendment,* 18 June 2013

123. Reform Government Surveillance, *RGS Principles,* https://www.reformgovernmentsurveillance.com/principles/

124. Ranking Digital Rights conducts a detailed evaluation of leading internet, mobile, and telecommunications companies on their disclosed commitments and policies affecting freedom of expression and privacy of internet users across the world. *See 2019 Ranking Digital Rights Corporate Accountability Index*, https://rankingdigitalrights.org/index2019. RDR is currently expanding its methodology to address harms associated with companies' targeted advertising policies and practices, and their use and development of algorithmic decision-making systems.

125. See also Google's Artificial Intelligence (AI) principles https://ai.google/principles and human rights statement https://about.google/human-rights/

2016 concluded both companies were in compliance with the GNI Principles, which are based on internationally recognized laws and standards for human rights.[126]

Amnesty International is unable to verify this assessment given that the process is confidential. However, GNI states that the scope of the GNI process covers an examination of a company's systems, policies, and procedures, together with an assessment of a number of specific cases agreed by the company itself.[127] The focus on specific case studies may indicate that the process does not include a holistic assessment of whether the company is effectively implementing these policies and procedures in practice, including by identifying and addressing human rights impacts throughout its business, or whether companies like Google and Facebook are undertaking due diligence to identify and address the human rights impacts of their business model as a whole. It would therefore appear not to cover the issue at the heart of this paper, which is whether a surveillance-based business model can ever be compatible with the responsibility to respect human rights on the basis that it is inherently at odds with the three core elements of the right to privacy.[127]

Amnesty International asked Google and Facebook whether the companies' human rights due diligence processes take into account the systemic and widespread human rights impacts of their business model as a whole, in particular the right to privacy, as outlined above. In a meeting with Amnesty International, Google stated that it does conduct human rights due diligence across its business. Facebook sent a detailed letter in response (see Annex) but did not answer this specific question.

126. GNI, *2015/2016 Company Assessments,* July 2016, https://globalnetworkinitiative.org/2015-2016-company-assessments/

127. GNI, *Company Assessments,* https://globalnetworkinitiative.org/company-assessments/

128. The process review questions for the current GNI assessment cycle asks what due diligence the company does to identify potential risks to freedom of expression and privacy connected to specific products, markets, acquisitions or business relationships; but not the company's business model as a whole. See: GNI, *2018/2019 Company Assessments*, Appendix I: Process Review Questions, https://globalnetworkinitiative.org/wp-content/uploads/2019/03/GNI-2018-Appendix-I.pdf

3. DATA ANALYTICS AT SCALE: HUMAN RIGHTS RISKS BEYOND PRIVACY

> ***"Surveillance is just the act of watching, but what has it done to the society, right? …. What does it do when there're no pockets where you can have dissident views, or experiment with self-presentation in different ways? What does that look like? That's really just a form of social control…a move towards conformity…. [S]urveillance itself is not quite an aggressive enough word to describe it.***
>
> Julia Angwin, 2018[129]

Google and Facebook's platforms are underpinned by a set of advanced data analytics systems. Their algorithmic models are designed to serve a user 'relevant' content (relevancy that is inferred by the companies on the basis of collected data) - both 'organic' posts and adverts. For example, the algorithms powering Google Search and Facebook Newsfeed are continuously trained on vast amounts of user data to serve many different purposes, such as ad targeting and delivery, serving search results, recommending new content, and prompting users to create new content and engage with existing content. To do this, the systems "optimize" to best deliver a specific outcome using highly complex and iterative algorithmic processes that draw correlations and inferences from user data.[130]

Increasingly, these algorithmic systems have been shown to have knock-on effects that can result in serious negative impacts on human rights, including privacy, freedom of expression and the right to

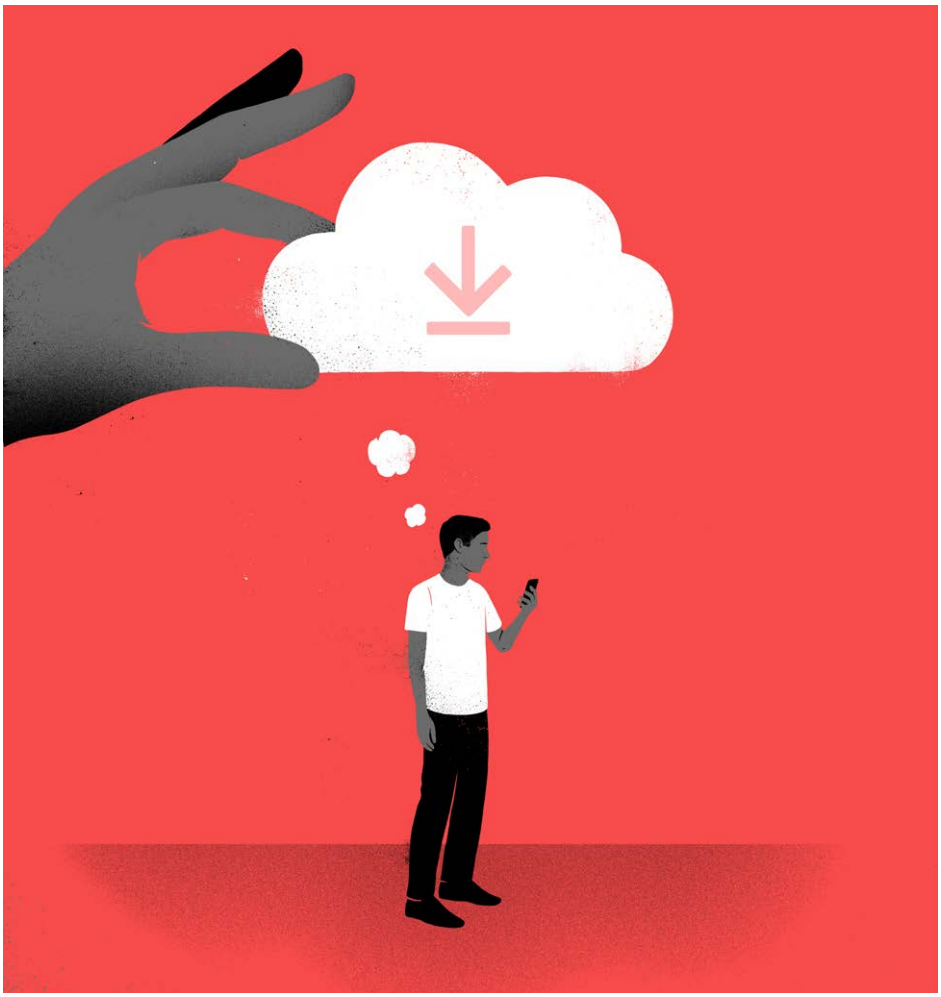
129. Julia Angwin in conversation with Trevlor Paglen, *The End of Trust,* Issue 54, McSweeney's Quarterly Concern and the Electronic Frontier Foundation, p. 55, https://www.eff.org/document/end-trust-0.

130. "Optimization systems apply a logic of operational control that focuses on outcomes rather than the process… We call optimization systems those systems that capture and manipulate user behaviour and environments under the logic of optimization." Rebekah Overdorf, Bogdan Kulynych, Ero Balsa, Carmela Troncoso, Seda Gürses, *POTs: Protective Optimization Technologies,* August 2018, https://arxiv.org/abs/1806.02711.

equality and non-discrimination.[131] In some cases, such impacts are directly caused by the company's technology itself; in other cases, these tools can be exploited by other actors in ways that harm rights. These impacts are significantly amplified and multiplied by the sheer scale of Facebook and Google's operations and the dominance of their platforms.

As a result, the initial harm caused by the surveillance-based model's assault on privacy boomerangs back on people in a host of unforeseen ways. For example, at an individual level, a person may only give up some seemingly innocuous data such as what they 'like' on Facebook. But once aggregated, that data can be repurposed to deliver highly targeted advertising, political messages and propaganda, or to grab people's attention and keep them on the platform.

OHCHR has stated that the analytical power of data-driven technology has created an environment that "carries risks for individuals and societies that can hardly be overestimated."[132]



131. See various examples cited in Ranking Digital Rights, *Human Rights Risk Scenarios:* Targeted Advertising, February 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf; and Algorithms, machine learning and automated decision-making, July 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf

132. OHCHR, *Right to privacy in the digital age*, 3 August 2018, A/HRC/39/29, para 16.

GREATER PERSONALISATION, PROFILING AND MICROTARGETING

Advanced data analytics are core to the surveillance-based business model and have propelled the economic power of Facebook and Google. In 2018, Facebook stated that one of the machine learning frameworks behind its platform was delivering 200 trillion predictions per day.[133] Algorithmic systems serve the incentives of the business model in two primary ways: firstly, to deliver targeted advertising, and secondly, maximising user engagement. As outlined in the following sections, both these purposes have troubling side-effects that threaten human rights.[134]

The accumulation of data enables Facebook and Google to deliver highly targeted advertisements to people based on a complex combination of their profile characteristics including location, demographics, interests, and behaviour. As noted in Section 1, these characteristics are inferred and predicted by the companies' sophisticated algorithmic models. The ability of Google and Facebook to offer advertisers finely tuned prediction and 'microtargeting' tools driven advertising revenues for the companies.

There are a huge number of companies and other actors that make up the complex ecosystem of targeted advertising. However, the uniquely self-reinforcing combination of their vast data vaults, the reach of their platforms and control over the primary flows of data, and consequent ability to develop the most advanced machine learning tools and prediction models mean that Google and Facebook completely dominate the market in digital advertising.

Alongside deploying data analytics for advertising, Facebook and Google also use algorithms to personalise user experience and 'maximise engagement' with their products, keeping users on their platforms for as long as possible.[135] The platforms are designed, in short, to be addictive.[136] This is intimately linked to the companies' business model and revenue, because more time on the platform means more advertisements can be served, and more people will see and click on the ads, thus generating more data. Furthermore, it reinforces the model by ensuring continued access to people's data and maintaining the dominance of the platforms.

INFLUENCING OPINION AND BELIEFS

As outlined in section 2 above, privacy is intimately connected with the concept of autonomy, the ability to shape and express our identity without unwarranted observation and undue influence.

However, the combination of algorithmically-driven ad targeting and personalised content means Google and Facebook's platforms play an enormous role in shaping people's online experience and determining the information we see. This can influence, shape and modify opinions and thoughts, which risks affecting our ability to make autonomous choices. Moreover, the algorithms are designed

133. Facebook, *Announcing PyTorch 1.0 for both research and production*, May 2018, https://engineering.fb.com/ai-research/announcing-pytorch-1-0-for-both-research-and-production

134. Ranking Digital Rights, *Human Rights Risk Scenarios:* Targeted Advertising, February 2019; and Algorithms, machine learning and automated decision-making, July 2019

135. Facebook denies that its News Feed algorithm is designed to maximise engagement, and that "the actual goal is to connect people with the content that is most interesting and relevant to them." See Facebook response, in annex below.

136. ABC News, *Book excerpt: Jaron Lanier's 'Ten Arguments for Deleting Your Social Media Accounts Right Now'*, June 2018, https://abcnews.go.com/Technology/book-excerpt-jaron-laniers-ten-arguments-deleting-social/story?id=56009512.

to find the best ways to nudge people towards particular outcomes based on an individual's unique personal characteristics. As such, techno-sociologist Zeynep Tufecki has described the platforms as "persuasion architectures" that can manipulate and influence people at the scale of billions.[137] Similarly, former Google advertising strategist James Williams has called it the "industrialisation of persuasion", arguing that this "attentional capture and exploitation" distracts us to the point that it limits our ability to think clearly and pursue our own goals.

These capabilities mean there is a high risk that the companies could directly harm the rights to freedom of thought, conscience and religion and freedom of opinion and expression through their use of algorithmic systems.[138] Furthermore, they risk contributing to abuses of these rights by other actors who are able to access or utilise their models.

International human rights law does not permit any limitations whatsoever on the freedom of thought and conscience or on the freedom to have or adopt a religion or belief of one's choice. These freedoms are protected unconditionally, as is the right of everyone to hold opinions without interference.[139] The HR Committee has concluded that the right to freedom of opinion requires freedom from undue coercion in the development of an individual's beliefs, ideologies, reactions and positions.[140] The UN Special Rapporteur on the promotion and protection of the right to freedom of expression has highlighted that "[t]he intersection of technology and content curation raises novel questions about the types of coercion or inducement that may be considered an interference with the right to form an opinion"[141] and has noted that "[c]ompanies should, at the very least, provide meaningful information about how they develop and implement criteria for curating and personalizing content on their platforms, including policies and processes for detecting social, cultural or political biases in the design and development of relevant artificial intelligence systems."[142] The Council of Europe's Committee of Ministers has also warned that "fine grained, sub-conscious and personalised levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions."[143]

There are numerous examples that show how the platforms can be used to target people at a granular level and to influence their opinion and beliefs. Such targeting is made possible by the surveillance-based business model of Facebook and Google. Academic research has demonstrated that machine learning is now able to scan Instagram posts for signs of depression more reliably than human reviewers.[144] Facebook also told advertisers it could judge when teenagers were feeling "insecure", "worthless", or needed a "confidence boost".[145] In response, Facebook said it does not allow targeting

137. Zeynep Tufekci, *We're building a dystopia just to make people click on ads,* TEDGlobal, September 2017, https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads/transcript?language=en

138. Rights guaranteed by UDHR Articles 18, 19; ICCPR Articles 18, 19.

139. See Human Rights Council, 'General Comment No.22: The right to freedom of thought, conscience and religion (Art. 18), 30 July 1993, CCPR/C/21/Rev/1/Add/4, para.3; and Human Rights Committee, 'General Comment No.34, Article 19: Freedoms of opinion and expression', CCPR/C/GC/43, 12 September 2011, para.3.

140. Y*ong Joo-Kang v. Republic of Korea*, HR Committee communication No. 878/1999, 16 July 2003 (CCPR/C/78/D/878/1999).

141. David Kaye, Special Rapporteur on the Promotion and protection of the right to freedom of opinion and expression report to the UN General Assembly, 29 August 2018, A/73/348, para.24. (David Kaye, 2018)

142. David Kaye, 2018, para.26. As noted above, Facebook has taken some steps in this direction, including introducing tools that give users "more information about and control over what they see on Facebook." See Facebook response in the annex below.

143. Council of Europe's Committee of Ministers, *Declaration on the Manipulative Capabilities of Algorithmic Processes*, February 2019, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

144. Johannes C. Eichstaedt, Robert J. Smith, Raina M. Merchant, Lyle H. Ungar, Patrick Crutchley, Daniel Preoțiuc-Pietro, David A. Asch, and H. Andrew Schwartz, *Facebook language predicts depression in medical records,* October 2018, https://www.pnas.org/content/115/44/11203.

145. The Australian, *Facebook targets 'insecure' kids*, May 2017, https://www.theaustralian.com.au/business/media/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

based on people's emotional states;[146] however, the case highlights the capabilities of the platform, and how it could be misused to intrusively target people when they are at their most vulnerable.

Another example is Google's Redirect Method, a project that uses the company's AdWords platform (now called Google Ads) to deradicalize potential supporters of Islamic terrorism.[147] One commentator successfully used the same tool – which is freely available online – to nudge suicidal people to call a helpline.[148] This demonstrates that such "social engineering" could easily be used to manipulate people's opinions and beliefs, either by the companies directly or by other actors. Although in the latter examples, such influence was used for a purportedly positive objective, these tools could easily be (mis)used in ways that harm our rights, particularly if deployed at scale.

HIDDEN MANIPULATION AT SCALE

The right to privacy is "an essential requirement for the realization of the right to freedom of expression"[149] and therefore Google and Facebook's erosion of the "private sphere" has corresponding direct and indirect impacts on the free development and exchange of ideas.

Freedom of expression is a collective right, enabling people to seek and receive information as a social group and to "voice their collective views".[150] By their very nature, algorithmic systems impact people as a group as well as at an individual level.[151] When the capabilities of influence and persuasion are deployed at the scale of the platforms controlled by Facebook and Google, the companies have the capability to affect opinion for large groups or segments of a population, and this can also be exploited by other actors.

The surveillance-based business model has created an architecture that has not only drastically shrunk and restricted the "private sphere", but at the same time isolated people from one another, as each individual engages with their own highly personalised experience of the internet, uniquely tailored to them based on algorithmically-driven inferences and profiling.[152] This leaves the door wide open to abuse by manipulating people at scale.

The starkest and most visible example of how Facebook and Google's capabilities to target people at a granular level can be misused is in the context of political campaigning – the most high-profile case being the Cambridge Analytica scandal (see inset box). The same mechanisms and tools of persuasion used for the purposes of advertising can be deployed to influence and manipulate people's political opinions.[153] The use of microtargeting for political messaging can also limit people's freedom of expression by "creating a curated worldview inhospitable to pluralistic political discourse".[154]

---

146. Facebook, *Comments on Research and Ad Targeting,* April 2017, https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting/

147. The Redirect Method, https://redirectmethod.org/

148. Patrick Berlinquette, *I Used Google Ads for Social Engineering.* It Worked. New York Times, July 2019 https://www.nytimes.com/2019/07/07/opinion/google-ads.html

149. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, A/HRC/23/40, para.24.

150. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 20 April 2010, A/HRC/14/23, para. 29.

151. "A profile does not simply identify the characteristics of individual data subjects, rather they are constructed by contrast with the other data subjects in the dataset." Lilian Edwards and Michael Veale, *Slave to the Algorithm? Why A 'Right To An Explanation' Is Probably Not The Remedy You Are Looking For,* 16 Duke Law & Technology Review 18, 2017, p 35, https://ssrn.com/abstract=2972855 (Edwards and Veale, 2017)

152. For example, a study by the Web Foundation into curation on Facebook's central News Feed feature found that "The algorithm places each user into a separate and individualised version of what should be an open public square for information." See the Web Foundation, *The Invisible Curation of Content*, 2018, p 5 http://webfoundation.org/docs/2018/04/WF_InvisibleCurationContent_Screen_AW.pdf

153. Tactical Tech has researched and mapped out the tools and techniques of the political data industry. See Tactical Tech, *Tools of the Influence Industry* https://ourdataourselves.tacticaltech.org/posts/influence-industry

154. David Kaye, 2018, para 18

The use of microtargeting for political campaigning is particularly problematic because of a lack of transparency or oversight over the messages that are sent and who is sending them. This leaves open the ability for campaigns to use "dark" political ads, in which people receive highly tailored messages that are only visible to them, and where it may not be clear what organisation or individual is behind them – or what information other people are seeing and receiving.

THE CAMBRIDGE ANALYTICA SCANDAL

Cambridge Analytica was a political data analytics firm that claimed the ability to influence target populations by creating uniquely detailed personality profiles and then tailoring political messaging based on these profiles (a technique known as psychographic targeting).[155] Cambridge Analytica's own marketing stated that the company had profiles on up to 240 million Americans and that it had 4,000 to 5,000 data points on each voter.[156]

In 2014, Cambridge Analytica gained access to Facebook profile data that was obtained via an app called "thisisyourdigitallife", created by Dr. Aleksander Kogan, a psychology professor at Cambridge University. When Facebook users downloaded the app, they consented for the app to access their personal information.[157] Dr. Kogan's company entered into a contract with a Cambridge Analytica affiliate, premised on harvesting Facebook data.[158]

Under Facebook's policies at the time, apps could access data not only about users who directly consented, but also personal data from people in those users' social network (i.e. their Facebook friends).[159] This meant that even though only 270,000 users consented to share their data through Kogan's app, information from up to 87 million Facebook profiles was subsequently improperly shared with Cambridge Analytica, as Facebook later confirmed.[160]

In late 2015, the Guardian reported that Cambridge Analytica was improperly using personal Facebook data for the campaign of US Presidential candidate Ted Cruz.[161] In response, Facebook demanded that Kogan and Cambridge Analytica delete the data.[162] Cambridge Analytica certified that it would do so, but in fact still had access to the data or models based on the data.[163]

155. Sue Halpern, *Cambridge Analytica and the Perils of Psychographics,* The New Yorker, https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics

156. BBC News, *Cambridge Analytica parent firm SCL Elections fined over data refusal,* January 2019

157. Facebook, *Suspending Cambridge Analytica and SCL Group From Facebook,* March 2018 https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/

158. Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,* Guardian (UK), 17 March 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

159. UK House of Commons Digital, Culture, Media and Sport Committee, *Interim Report into Disinformation and 'fake news',* July 2018, para 120

160. Facebook, *An Update on Our Plans to Restrict Data Access on Facebook,* 4 April 2018, https://newsroom.fb.com/news/2018/04/restricting-data-access/

161. Harry Davies, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users,* Guardian (UK), 11 December 2015, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

162. Facebook, *Hard Questions: Update on Cambridge Analytica,* 21 March 2018, https://newsroom.fb.com/news/2018/03/hard-questions-cambridge-analytica

163. Paul Lewis, David Pegg and Alex Hern, *Cambridge Analytica kept Facebook data models through US election*, Guardian (UK), May 2018, https://www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election

In 2016, the Donald Trump US Presidential campaign hired Cambridge Analytica, which used these psychographic profiles to help the campaign identify target audiences for digital ads and model voter turnout. Only in April 2018, after the Observer and the New York Times broke the story over Cambridge Analytica's use of Facebook data, did Facebook begin to contact the 87 million users affected by the data breach.[164]

There are three key aspects of the scandal with regards to Facebook. First was Facebook's notoriously lax data privacy policies at the time, under which Kogan was allowed to access personal information, not only from Facebook users who accessed the app, but from their entire social networks as well. Facebook subsequently had to suspend tens of thousands of apps from around 400 developers that had been able to access user data before the company reduced developer access in 2014.[165] Facebook has since further restricted the extent to which app developers are able to access user data.[166] Second, even though Facebook requested that Cambridge Analytica delete the data, they had no way of verifying if Cambridge Analytica complied, showing how difficult it is to enforce those policies that do exist. Third was the fact that, even though Facebook had been aware of the problem since at least December 2015, it did not alert users whose data had been compromised until much later - and then only following a media investigation and major public scandal.

In the wake of the Cambridge Analytica scandal, Google and Facebook have both tightened their policies around political advertising,[167] including measures to increase transparency around who's paying for the advertising, and 'Ad Libraries' disclosing political advert. However, an analysis by Privacy International found that to date these measures have been inadequate, and inconsistently applied in different countries, so that most users around the world "lack meaningful insight into how ads are being targeted through these platforms".[168] A separate analysis by Mozilla researchers also found Facebook's tool to be inadequate.[169]

Fundamentally, the business model's dependence on profiling and targeting for advertising means that these capabilities will continue to be exploited by third parties, including political campaigns.

164. Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *2016 the Donald Trump Presidential campaign hired Cambridge Analytica,* New York Times, 17 March 2018; Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, Guardian (UK), 17 March 2018; CNBC, Facebook now lets you know if your data was shared with Cambridge Analytica, 9 April 2018

165. Facebook, *An Update on Our App Developer Investigation,* 20 September 2019, https://newsroom.fb.com/news/2019/09/an-update-on-our-app-developer-investigation/. According to Facebook's response letter to Amnesty, included at the end of this report: "Suspension is not necessarily an indication that these apps were posing a threat to people."

166. Facebook, *API Updates and Important Changes*, 25 April 2019, https://developers.facebook.com/blog/post/2019/04/25/api-updates/

167. Google, *Introducing a new transparency report for political ads,* 15 August 2018, https://www.blog.google/technology/ads/introducing-new-transparency-report-political-ads/; Facebook, *A Better Way to Learn About Ads on Facebook,* 28 March 2019, https://newsroom.fb.com/news/2019/03/a-better-way-to-learn-about-ads/

168. Privacy International, *Social media companies have failed to provide adequate advertising transparency to users globally,* 3 October 2019, https://privacyinternational.org/long-read/3244/social-media-companies-have-failed-provide-adequate-advertising-transparency-users

169. Mozilla, *Facebook's Ad Archive API is Inadequate,* 29 April 2019, https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadequate/

MAXIMISING ENGAGEMENT

Companies have a responsibility to respect free expression, which encompasses expression which may be offensive or disturbing.[170] The International Covenant on Civil and Political Rights, for example, requires states to prohibit only "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence." Many other forms of expression, even those which shock or offend, may not lawfully be restricted.

However, the use of algorithms to curate social media content and encourage people to remain on the platform can result in Google and Facebook actively promoting or amplifying abusive, discriminatory or hateful content. The platforms recommend and promote new content based on opaque algorithmic processes to determine what will best engage users.[171] Because people are more likely to click on sensationalist or incendiary material, the so-called 'recommendation engines' of these platforms can send their users down what some have called a 'rabbit hole' of toxic content.[172]

Former Google Chief Technology Officer Nicole Wong now recognises this problem, stating that "Personalization, engagement ... what keeps you here, which today we now know very clearly. It's the most outrageous thing you can find."[173] Mark Zuckerberg acknowledges that "our research suggests that no matter where we draw the lines for what is allowed, as a piece of content gets close to that line, people will engage with it more on average -- even when they tell us afterwards they don't like the content."[174]

Facebook argue that "our focus is on the quality of time spent on Facebook, not the amount... Facebook's algorithms prioritize posts that are predicted to spark *meaningful conversations*".[175] Yet even Facebook insiders admit the intentionally addictive nature of the product. For instance, Roger McNamee, an early investor in Facebook and advisor to Mark Zuckerberg, wrote earlier this year: "The business model depends on advertising, which in turn depends on manipulating the attention of users so they see more ads. One of the best ways to manipulate attention is to appeal to outrage and fear, emotions that increase engagement."[176]

The UN Special Rapporteur on the promotion and protection of the right to freedom of expression has noted that "the artificial intelligence applications for search have enormous influence over the dissemination of knowledge. Content aggregators and news sites… choose which information to display to an individual based not on recent or important developments, but on artificial intelligence applications that predict users' interests and news patterns based on extensive datasets. Consequently, artificial intelligence plays a large but usually hidden role in shaping what information individuals consume or even know to consume."[177] The Special Rapporteur has also stated that "[i]n an artificial

170. Human Rights Committee, 'General Comment No.34, Article 19: Freedoms of opinion and expression', CCPR/C/GC/43, 12 September 2011, para.11.

171. For example, Alex Madrigal, The Atlantic, *How YouTube's Algorithm Really Works,* November 2018 https://www.theatlantic.com/technology/archive/2018/11/how-youtubes-algorithm-really-works/575212/

172. Kevin Roose, T*he Making of a YouTube Radical,* The New York Times, June 2019 https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html

173. Recode Decode, *Full Q&A: Former Google lawyer and deputy U.S. CTO Nicole Wong*, September 2018 https://www.vox.com/2018/9/12/17848384/nicole-wong-cto-lawyer-google-twitter-kara-swisher-decode-podcast-full-transcript

174. Mark Zuckerberg, *A Blueprint for Content Governance and Enforcement*, November 2018, https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/

175. Facebook letter to Amnesty International – see Annex. The company also points to its efforts to reduce the virality of hate speech and other content moderation measures.

176. Roger McNamee, *I Mentored Mark Zuckerberg. I Loved Facebook. But I Can't Stay Silent About What's Happening,* Time, 17 January 2019, https://time.com/5505441/mark-zuckerberg-mentor-facebook-downfall/

177. David Kaye 2018, para 11

intelligence-governed system, the dissemination of information and ideas is governed by opaque forces with priorities that may be at odds with an enabling environment for media diversity and independent voices."[178]

Sensationalism in mass media is, of course, not a new phenomenon, and is not limited to the internet. But the recommendation engines of social media go well beyond the adage "if it bleeds, it leads": they can systematically privilege extreme content including conspiracy theories, misogyny, and racism to keep people on their platforms for as long as possible. For example, one academic study into the spread of anti-refugee sentiment on Facebook found that "anti-refugee hate crimes increase disproportionally in areas with higher Facebook usage during periods of high anti-refugee sentiment online".[179] Similarly, the algorithms behind Google's YouTube platform have been shown to have various harmful consequences (see box below).

As well as privileging harmful content, the platforms' algorithms can also undermine freedom of expression or lead to discrimination by suppressing certain forms of content. For example, LGBTI communities have alleged that YouTube's algorithm blocks or suppresses videos containing LGBTI content by automatically enforcing age restrictions and by "demonetising" the videos – meaning that they deny the producers ad revenue.[180] YouTube denies this, saying the company does "not automatically demonetize LGBTQ content."[11]

CASE STUDY: YOUTUBE'S RADICALISATION ECOSYSTEM

Numerous studies of YouTube—by scholar Zeynep Tufecki,[182] ex-YouTube engineer Guillaume Chaslot,[183] the New York Times[184] and others—have documented how the YouTube recommendation algorithm privileges false and incendiary content.

In theory, both harassment and hate speech violate YouTube's policies. In practice, material that closely treads (or crosses) this line stays up because it garners a lot of attention and is profitable for YouTube because it means people stay on the platform for longer, during which they see more ads, which in turn is more profitable for YouTube as it earns money from advertisers based on the number of views an ad gets. According to the company itself, their system for algorithmically recommending new material drives 70 percent of the total time people spend on the platform.[185]

178. David Kaye 2018, para 30

179. Karsten Müller and Carlo Schwarz, *Fanning the Flames of Hate: Social Media and Hate Crime,* University of Warwick, May 2018, https://warwick.ac.uk/fac/soc/economics/research/centres/cage/manage/publications/373-2018_schwarz.pdf; Amanda Taub and Max Fisher, *Facebook Fueled Anti-Refugee Attacks in Germany, New Research Suggests,* New York Times, 21 August 2018

180. Julia Alexander, *LGBTQ YouTubers are suing YouTube over alleged discrimination*, The Verge, August 2019 https://www.theverge.com/2019/8/14/20805283/lgbtq-youtuber-lawsuit-discrimination-alleged-video-recommendations-demonetization

181. Ibid.

182. Zeynep Tufekci, *YouTube, The Great Radicalizer,* The New York Times, March 2018 https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.

183. Chaslot's site, "Daily YouTube Recommendations," seeks to track YouTube's recommendations for over a thousand channels. See https://algotransparency.org/. *See also How an ex-YouTube insider investigated its secret algorithm,* Guardian (UK), https://www.theguardian.com/technology/2018/feb/02/youtube-algorithm-election-clinton-trump-guillaume-chaslot.

184. Max Fisher and Amanda Taub, *How YouTube Radicalized Brazil,* New York Times, 11 August 2019, https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html

185. Max Fisher and Amanda Taub, *How YouTube Radicalized Brazil,* New York Times, 11 August 2019

One 2018 report by a researcher with the Data & Society thinktank, Becca Lewis, describes how YouTube's recommendation engine monetizes reach and 'influence' for even those who regularly profess harmful and racist views.[186] In her 2018 study, "Alternative Influence: Broadcasting the Reactionary Right on YouTube," Lewis maps the network of far-right influencers on the US who use YouTube's algorithm to profit from disinformation and hate speech. She charts how a combination of YouTube's recommendation algorithm and the social practices of far-right YouTubers creates a radicalization ecosystem that makes it "remarkably easy for viewers to be exposed to incrementally more extremist content."[187] This is particularly problematic, she writes, given YouTube's popularity as a news source for the young.[188] Her conclusion: "A giant network of influencers on YouTube is broadcasting reactionary ideas to young viewers - and radicalizing them in the process."[189]

The algorithm also helps reinforce false information and rumours. By automatically joining together different videos that all repeat the same false narrative, YouTube creates the illusion that there are multiple sources for the same idea. In reality, this seeming consensus is entirely manufactured by the algorithm: according to Debora Diniz, a women's rights activist who became the target of a coordinated conspiracy campaign in Brazil, "it feels like the connection is made by the viewer, but the connection is made by the system".[190] These problems of confirmation bias and popularity bias have been documented across social media platforms.[191]

In response to some of this reporting, YouTube announced—not for the first time—changes in the ways algorithms would recommend content on the platform, but to date these changes only apply only to a small set of videos in the USA.[192] The company continues to be subject to intense public criticism for allowing the monetisation of abusive content on their platform.[193] However, YouTube's CEO denies the allegation "that we hesitate to take action on problematic content because it benefits our business".[194] Google stated that YouTube is continuing to improve its recommendations function.[195]

186. Rebecca Lewis, *Alternative Influence: Broadcasting the Reactionary Right on YouTube*, Data & Society, September 2018, https://datasociety.net/output/alternative-influence/

187. Ibid, p 36.

188. The report cites a Pew Research Center study showing over 90% of adults 18-24 use YouTube: http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/pi_2018-03-01_social-media_0-01/.

189. Rebecca Lewis, https://twitter.com/beccalew/status/1042054175201185792

190. Max Fisher and Amanda Taub, *How YouTube Radicalized Brazil,* New York Times, 11 August 2019

191. Giovanni Luca Ciampaglia, Filippo Menczer, *Biases Make People Vulnerable to Misinformation Spread by Social Media,* The Conversation, 21 June 2018 https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/

192. YouTube, *Continuing our work to improve recommendations on YouTube*, 25 January 2019, https://youtube.googleblog.com/2019/01/continuing-our-work-to-improve.html

193. YouTube, *Taking a harder look at harassment,* 5 June 2019 https://youtube.googleblog.com/2019/06/taking-harder-look-at-harassment.html

194. YouTube, *Susan Wojcicki: Preserving openness through responsibility*, August 2019, https://youtube-creators.googleblog.com/2019/08/preserving-openness-through-responsibility.html

195. YouTube, *The Four Rs of Responsibility, Part 1: Removing harmful content,* 3 September 2019, https://youtube.googleblog.com/2019/09/the-four-rs-of-responsibility-remove.html

DISCRIMINATION

Another major rights risk of targeted advertising and profiling, which forms the basis of Facebook and Google's business model, is that serving targeted content to selected people or groups of people can fuel discrimination by private entities, or directly by the platforms themselves, undermining the critical principle that all people should enjoy equal access to their human rights.[196] Non-discrimination, together with equality before the law and equal protection of the law without any discrimination, constitute a basic and general principle relating to the protection of human rights.[197]

Profiling inherently seeks to differentiate between people based on personal characteristics, beliefs and behaviours. Targeting by advertisers and political parties using Facebook and Google's platforms (i.e. deciding to include or exclude certain groups) has in the past been shown to include profiling people in sensitive ways including across protected characteristics – examples of categories include 'under 18,'[198] 'multicultural affinity',[199] 'interested in treason',[200] 'interested in [former Nazi leader] Joseph Goebbels',[201] 'lower 50% income bracket,'[202] 'interested in addiction treatment centres,'[203] 'interested in abortion,'[204] 'interested in white genocide'[205] or 'sexual orientation'.[206]

Individual instances of targeting do not necessarily imply a rights violation: often when advertisers target consumers to sell them products based on their interests, it will not impair any rights or freedoms. However, when deployed in contexts that touch directly on people's rights, including economic, social and cultural rights, Facebook and Google's enabling of granular targeting by advertisers inherently poses a high risk of discrimination.

Facebook's advertising policies have long prohibited discrimination.[207] Investigative journalists, however, showed that for years, Facebook permitted advertisers (for housing, jobs, or even more worryingly, political ads) to target – and exclude – groups by protected categories including ethnicity and age.[208] Earlier this year, Facebook was forced to heavily restrict the use of targeting for housing,

196. Chris Gillard, Friction-Free Racism, Real Life magazine, 15 October 2018, https://reallifemag.com/friction-free-racism/

197. Human Rights Committee, General Comment No.18: Non-discrimination, 10 November 1989, para.1.

198. Facebook, About age-based targeting, https://www.facebook.com/help/103928676365132 ("The minimum age on Facebook is 13, so all ads will be targeted only to people who are at least 13 years of age.")

199. ProPublica, *Facebook Promises to Bar Advertisers from Targeting Ads by Race or Ethnicity. Again.*, July 2018 https://www.propublica.org/article/facebook-promises-to-bar-advertisers-from-targeting-ads-by-race-or-ethnicity-again

200. Guardian (UK), *Facebook labels Russian users as 'interested in treason,* July 2018, https://www.theguardian.com/technology/2018/jul/11/facebook-labels-russian-users-as-interested-in-treason

201. Los Angeles Times, *Facebook decided which users are interested in Nazis — and let advertisers target them directly*, February 2019, https://www.latimes.com/business/technology/la-fi-tn-facebook-nazi-metal-ads-20190221-story.html

202. Google, *About demographic targeting,* https://support.google.com/google-ads/answer/2580383

203. In 2018, Facebook started to restrict addiction treatment centre advertising to certified organisations – but only in the USA. See Facebook, *Restricting Ads for Addiction Treatment Centers and Bail Bonds,* 9 August 2018, https://www.facebook.com/business/news/restricting-ads-for-addiction-treatment-centers-and-bail-bonds

204. Google Advertising Policies, Healthcare and Medicines, https://support.google.com/adspolicy/answer/176031 (this category is not available in a number of countries.)

205. The Intercept, "Facebook Allowed Advertisers to Target Users Interested in "White Genocide" — Even in Wake of Pittsburgh Massacre," *available at* https://theintercept.com/2018/11/02/facebook-ads-white-supremacy-pittsburgh-shooting/ . This category has since been disabled.

206. The ability to target users by sexual orientation on Facebook was available up until February 2019. Buzzfeed, *Facebook Has Blocked Ad Targeting By Sexual Orientation*, 21 March 2018 https://www.buzzfeednews.com/article/alexkantrowitz/facebook-has-blocked-ad-targeting-by-sexual-orientation.

207. Facebook Ad Policy, *Prohibited Content: Discriminatory Practices*, https://www.facebook.com/policies/ads/prohibited_content/discriminatory_practices

208. Julia Angwin and Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race,* 28 October 2016 https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

employment and credit advertisements in the United States, after a legal settlement with civil rights groups.[209] For instance, advertisers can no longer target housing, employment and credit opportunity ads to people based on their age, gender, ZIP code or any interests describing or appearing to relate to protected characteristics. However, these measures only apply to advertisers based in the USA or targeting people in the USA, meaning people in the rest of the world are still at risk of discrimination in those areas.

Importantly, in addition to the risks of discrimination by third party use of the companies' ad targeting capabilities, the algorithmic systems determining how ads are actually *delivered* on the platforms can lead to discriminatory outcomes – even when the ads are targeted in a neutral way by the advertisers themselves.[210] This raises the risk that the companies could directly cause discrimination themselves through the way that their algorithmic systems optimize to deliver ads, e.g. on the basis of "relevance" or to more "valuable" users. In March 2019, the US Department of Housing and Urban Development (HUD) sued Facebook over housing discrimination, including through its own ad delivery system, stating that Facebook's mechanisms "function just like an advertiser who intentionally targets or excludes users based on their protected class".[211] In response, Facebook disputed this allegation, saying "HUD had no evidence and finding that our AI systems discriminate against people."[212] HUD is reportedly also investigating Google and Twitter's advertising practices.[213]

209. Facebook, *Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising,* 19 March 2019, https://newsroom.fb.com/news/2019/03/protecting-against-discrimination-in-ads; ACLU, Summary Of Settlements Between Civil Rights Advocates And Facebook, 19 March 2019, https://www.aclu.org/other/summary-settlements-between-civil-rights-advocates-and-facebook

210. Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, Aaron Rieke, *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*, April 2019, https://arxiv.org/abs/1904.02095; Carnegie Mellon University, *Questioning the Fairness of Targeting Ads Online,* July 2015, https://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html

211. United States Department of Housing and Urban Development v Facebook, Charge of Discrimination, 28 March 2019, https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf

212. Facebook statement in ProPublica, *HUD Sues Facebook Over Housing Discrimination and Says the Company's Algorithms Have Made the Problem Worse,* March 2019, https://www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms

213. Washington Post, *HUD is reviewing Twitter's and Google's ad practices as part of housing discrimination probe*, 28 March 2019, https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/

4. CONCENTRATION OF POWER OBSTRUCTS ACCOUNTABILITY

> ***"In the software world, particularly for platforms, these are winner-take-all markets."***
>
> Bill Gates, Microsoft co-founder.[214]

The surveillance-based business model of Google and Facebook has enabled them to establish near-total control over the primary channels that most people rely on to engage with the digital world and the global "public square", in the process becoming powers of historic proportions. Never before has any entity been able to mediate and prioritise the transmission of information to over two billion users in multiple nations.

The concentrated power of the companies is multifaceted. Paul Nemitz, Principal Adviser in the European Commission, has set out that the unique concentration of power into the hands of the Big Tech companies has four key elements, which should be seen together and in cumulation: the power of money, enabling them to influence politics and markets; the power over infrastructures for democracy and discourse; the power over individuals based on profiling, and the ability to leverage that knowledge for their own interests; and the dominance in AI innovation.[215]

This concentrated power goes hand in hand with the business model's human rights impacts – indeed, the one has symbiotically propelled the other. The evisceration of the right to privacy online has taken place largely because essential internet services came to be controlled by companies dependent on surveillance. At the same time, the companies were able to establish such dominance precisely because they prioritised advertising revenues over privacy and other rights.

This power of the platforms has not only exacerbated and magnified their rights impacts but has also created a situation in which it is very difficult to hold the companies to account, or for those affected to access an effective remedy.

---

214. The Verge, *Bill Gates says his 'greatest mistake ever' was Microsoft losing to Android*, June 2019

215. Paul Nemitz, Principal Adviser in the European Commission (writing in his personal capacity), *Constitutional democracy and technology in the age of artificial intelligence*, October 2018. The analysis refers to the power of Google, Facebook, Microsoft, Apple and Amazon.

INTERNET ACCESS AT THE COST OF SURVEILLANCE

Access to the internet has long been recognised as a critical enabler of human rights in the digital age. In 2011, the UN Special Rapporteur on Freedom of Expression acknowledged the "unique and transformative nature of the internet not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights, and to promote the progress of society as a whole."[216] In 2016, the UN Human Rights Council stressed the importance of "applying a comprehensive human rights-based approach when providing and expanding access to the internet and for the internet to be open, accessible and nurtured".[217]

The role of Google and Facebook as "gatekeepers" to the digital world (as outlined in Section 1 above) means that they have significant influence over people's enjoyment of human rights online; indeed, the large majority of internet users are reliant on the services the companies provide. As such, the platforms have become fundamental to how people are able to exercise their human rights online, and are used every day in ways that facilitate freedom of expression, the rights of peaceful assembly and association, and other rights.[218]

At the same time, the dominance of the companies' platforms means it is now effectively impossible to engage with the internet without "consenting" to their surveillance-based business model. "Network effects" (as outlined below) mean it is not realistic for people to leave social networks where all their friends and family are. People who signed up for platforms when they were far more privacy-respecting (see below) – or before they were acquired by Google or Facebook – now face a false choice to leave a service they depend on or submit to surveillance. In some countries in the world, Facebook has become synonymous with the internet; and worldwide, the vast majority of smartphones run on Google's Android. Even for people who have not signed up for any of the companies' services, it is extremely difficult to use the internet without being subject to data harvesting by the two companies.[219]

This has created a paradoxical situation in which, in order to access the internet and enjoy their human rights online, people are forced to submit to a system predicated on interference with the right to privacy on an unprecedented scale, with corresponding impacts on a range of other human rights, including the right to freedom of expression and non-discrimination. Such a situation stands in sharp contradiction to the Human Rights Council's affirmation of the importance of "a human rights-based approach when providing and expanding access to the internet".[220] In June 2019, a group of UN experts further articulated that "Digital space is not neutral space. At the levels of its physical architecture, regulation and use, different groups exert their interests over it. The principles of international human rights law, however, should be at the centre of its development."[221]

---

216. Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report to the Human Rights Council, 16 May 2011, UN Doc A/HRC/17/27

217. UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, June 2016, UN Doc A/HRC/32/L.20

218. "In the digital age, the exercise of the rights of peaceful assembly and association has become largely dependent on business enterprises, whose legal obligations, policies, technical standards, financial models and algorithms can affect these freedoms." Clément Nyaletsossi Voule, Special Rapporteur on the rights to freedom of peaceful assembly and of association,

219. Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2014; Kashmir Hill, *Goodbye Big Five,* Gizmodo, January 2019

220. UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, June 2016, UN Doc. A/HRC/32/L.20

221. OHCHR, *UN experts stress links between digital space and human rights at RightsCon, Tunis,* 13 June 2019 www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24696

CONCENTRATED POWER EXACERBATES HARMS

The increasing power of Google and Facebook as gatekeepers to the ways people engage with the digital world has been a key driver of the erosion of privacy online. Various analyses charting the rise to dominance of Google and Facebook show that the companies were able to incrementally increase the breadth and depth of their surveillance in parallel with their control over the primary channels of the internet and the decline in any meaningful alternatives.[222]

Originally, when operating in highly competitive markets, both Google and Facebook did not condition access to their services on ubiquitous surveillance. Facebook's initial privacy policy stated that "we do not and will not use cookies to collect private information from any user."[223] Google's first privacy policy stated that the company shared information about users with advertisers, but "we only talk about our users in aggregate, not as individuals" – directly contrary to the current model of highly personalised and targeted advertising.[224]

The companies' transformation from their early more privacy-respecting days to the current business model of ubiquitous surveillance has been gradual. Google took the final step to fully embrace the surveillance-based model in 2016, when it changed its privacy policy to enable the company to combine data from its advertising network DoubleClick (since rebranded to Google Marketing Platform) with personal data collected from its other platforms.[225] This meant that the company could directly target advertising to identifiable individuals, based on highly personal information. In response, data privacy journalist Julia Angwin stated Google had "quietly erased that last privacy line in the sand".[226] Facebook had already taken a similar step in 2014, announcing that it would use web-browsing data for targeted advertising.[227]

The companies were able to take this final step because they had already established such a dominant position. As demonstrated by the companies' early business model, in a competitive market, internet users would not tolerate such a high degree of intrusion into their privacy and would move to alternative services. Now, the companies can afford to abuse privacy, because people have no choice but to accept.[228]

HUMAN RIGHTS HARMS FUEL CONCENTRATION OF POWER

At the same time, the surveillance-based business model has in-built tendencies to exponentially increase the platforms' dominance and scale, and as such, the abuse of privacy and other rights has also helped concentrate power towards Google and Facebook. The extraction of more and more data

222. See for example Zuboff, 2018; Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy,* 16 Berkeley Bus. L.J. 39, 2019

223. Facebook, *The Facebook Privacy Policy (2004),* cited in Dr Liza Lovdahl Gormsen & Dr Jose Tomas Llanos, *Facebook's Anticompetitive Lean in Strategies,* June 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3400204 (Gormsen and Llanos, 2019)

224. Google, Privacy Policy, June 1999, https://policies.google.com/privacy/archive/19990609?hl=en&gl=ZZ

225. Google, Privacy Policy, June 2016, https://policies.google.com/privacy/archive/20160325-20160628?hl=en&gl=ZZ

226. Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking,* ProPublica, 21 October 2016, https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking

227. AdAge, *Facebook To Use Web Browsing History For Ad Targeting,* June 2014, https://adage.com/article/digital/facebook-web-browsing-history-ad-targeting/293656

228. "Online communications platforms …can be compared to utilities in the sense that users feel they cannot do without them and so have limited choice but to accept their terms of service. Providers of these services currently have little incentive to address concerns about data misuse or online harms, including harms to society" UK House of Lords Select Committee on Communications, *Regulating in a Digital World,* March 2019, para 45. Facebook challenged this conclusion, stating that "to the contrary, we know that if we do not protect people's data, we will lose their trust". See Facebook response to Amnesty International, in Annex below.

has enabled the companies to gain greater control over the main ways that people engage with the internet, to an extent that likely would not have been possible had the companies stuck to a more privacy-respecting model.

First is an economic phenomenon known as "network effects": the more users a platform has, the more valuable it becomes, both to the users themselves and to others. Online platforms – and the business model behind them – are by their very nature prone to these network effects. Many users join Facebook because their friends are on Facebook; advertisers flock to YouTube because that is where the audience is largest. This has a snowball effect, such that the larger a network or platform becomes, the more reliant people become on it, and the more entrenched its position – making it harder for users to leave the platform or for competitors to establish an alternative.

The business model's extraction and analysis of data also results in specific data-driven network effects.[229] The accumulation of greater amounts of data enables a company to be better able to train the machine learning models and algorithms which produce behavioural predictions. In turn, these predictive functions are deployed to keep people on the platform, generating further data and maintaining control over data flows. Better predictive functions also lead to greater advertising revenue, enhancing the value of the platform and the company's power in the market.

This system of feedback loops, combined with traditional network effects, has been instrumental in rapidly expanding the scale and impact of the platforms, and thereby concentrating the power of Google and Facebook over the digital world. As we transition rapidly to a world where the 'Internet of Things,' data analytics and artificial intelligence sit at the heart of the economy, Google and Facebook's data vaults and control over the most advanced AI and machine learning technology will further entrench their position. Already, the machine learning frameworks backed by Google and Facebook – TensorFlow and PyTorch, respectively – have become the leading tools relied on by AI developers.[230]

The companies have also been able to use their data-driven advantages – and the financial clout that goes with it – to actively prevent the development of alternative services. They do this in several ways: by 'tying' one service to another, leveraging dominance in one area to try to increase dominance in another;[231] by downranking the services offered by would-be competitors on their own platforms (in, e.g., search results);[232] and by stifling companies offering similar or potentially competing services by either copying them or purchasing the company outright.[233] This pattern has become so well known that venture capitalists in Silicon Valley describe Google and Facebook as having a "kill zone:"[234] an economic area in which a competitor cannot take root, and where the only viable business model for a new market entrant is to be acquired by Google or Facebook.

---

229. Gormsen and Llanos, 2019

230. Jeff Hale, *Which Deep Learning Framework is Growing Fastest?*, KDnuggets, April 2019, https://www.kdnuggets.com/2019/05/which-deep-learning-framework-growing-fastest.html

231. European Commission, *Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine,* 18 July 2018, http://europa.eu/rapid/press-release_IP-18-4581_en.htm

232. European Commission, *Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service,* 27 June 2017, http://europa.eu/rapid/press-release_IP-17-1784_en.htm. See also, *The Case Against Google,* The New York Times, 20 Feb 2018, www.nytimes.com/2018/02/20/magazine/the-case-against-google.html

233. See, for example: Wired, If you can't build it, buy it: *Google's biggest acquisitions mapped,* September 2017; Billy Gallagher, *Copycat: How Facebook Tried to Squash Snapchat,* Wired, February 2018; New York Post, *Facebook boasted of buying Instagram to kill the competition: sources,* February 2019

234. The Economist, *American tech giants are making life tough for startups,* 2 June 2018

POWER OBSTRUCTS CORPORATE ACCOUNTABILITY

The imbalance between the multifaceted power of big technology companies like Google and Facebook, as set out above, and the ability of governments to meaningfully regulate them is a striking example of the "governance gaps" between "the scope and impact of economic forces and actors, and the capacity of societies to manage their adverse consequences". Such gaps were identified by UN Special Representative on Business and Human Rights John Ruggie as the "root cause" of the global business and human rights challenge created by globalization.[235]

Google and Facebook's accumulation of so much detailed data through controlling platforms and services that are deeply embedded in virtually all aspects of modern life has created massive information asymmetries between the companies on the one hand, and governments and internet users on the other. Zuboff states that "private surveillance capital has institutionalized asymmetries of knowledge unlike anything ever seen in human history. They know everything about us; we know almost nothing about them."[236]

The speed at which Google and Facebook's platforms have grown to such a vast scale, operating across borders, has meant that state-based regulation has struggled to keep pace with the companies' impacts on people's rights.[237] This gap is now publicly acknowledged by senior figures in Silicon Valley. Microsoft CEO Brad Smith stated, "Almost no technology has gone so entirely unregulated, for so long, as digital technology."[238] Mark Zuckerberg has called for "a more active role for governments and regulators", including in relation to data privacy.[239] In 2014, former Google CEO Eric Schmidt and then head of Google Ideas Jared Cohen declared that "the online world is…the world's largest ungoverned space".[240] Google itself states that it is "axiomatic that international legal frameworks are lagging behind the pace of technological innovation".[241]

Although there have been numerous regulatory actions against the big technology companies by data protection, competition and tax authorities worldwide, to date these have largely failed to disrupt the fundamental drivers of the surveillance-based business model.

To give a recent high-profile example, in June 2019, the US Federal Trade Commission (FTC) levied a record $5bn penalty against Facebook and imposed a range of new privacy requirements on the company, following an investigation in the wake of the Cambridge Analytica scandal.[242] Although the fine is the largest recorded privacy enforcement action in history, it is still relatively insignificant in comparison to the company's annual turnover and profits – illustrated by the fact that after the fine was announced, Facebook's share price went up.[243] More importantly, the settlement did not challenge the underlying model of ubiquitous surveillance and behavioural profiling and targeting. As FTC Commissioner Rohit Chopra stated in a dissenting opinion "The settlement imposes no meaningful

235. John Ruggie, UN Special Representative on the issue of human rights and transnational corporations and other business enterprises, Report to Human Rights Council, April 2008, A/HRC/8/5

236. https://www.democracynow.org/2019/3/1/age_of_surveillance_capitalism_we_thought

237. See e.g. UK House of Lords Select Committee on Communications, *Regulating in a Digital World,* March 2019: "regulation of the digital world has not kept pace with its role in our lives." ; Deloitte Insights, *The future of regulation,* June 2018, https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html; Daniel Malan, *The law can't keep up with new tech. Here's how to close the gap,* World Economic Forum, June 2018, https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up

238. NPR, *Microsoft President: Democracy Is At Stake. Regulate Big Tech*, September 2019

239. Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas,* Washington Post, March 2019

240. Schmidt and Cohen, *The New Digital Age,* 2014,

241. Google, submission to Office of the United High Commissioner for Human Rights on the right to privacy in the digital age, 2018

242. US Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, 24 July 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

243. MIT Technology Review, *Facebook is actually worth more thanks to news of the FTC's $5 billion fine,* 15 July 2019

changes to the company's structure or financial incentives, which led to these violations. Nor does it include any restrictions on the company's mass surveillance or advertising tactics."[244]

However, the tide is turning: there is now a growing appetite among both regulators and legislators in multiple jurisdictions to confront the dominant power of Google and Facebook head on, primarily through competition and data protection laws.

Google and Facebook are facing a raft of complaints filed since the EU's GDPR came into force. The Data Protection Commission in Ireland – where both Google and Facebook have their European headquarters – has multiple ongoing inquiries into both companies, including in relation to behavioural analysis and targeted advertising.[245] In January 2019 France's data protection watchdog imposed a record fine of 50 million euros on Google over breaches including lack of valid consent regarding ad personalization.[246]

In the USA, Google and Facebook are both facing multiple anti-trust investigations, including by the US Department of Justice, the FTC, the House Judiciary subcommittee, and two separate groups of state attorneys general.[247] Meanwhile, in 2018 California passed the US's most progressive privacy act to date, the California Consumer Privacy Act (CCPA), giving California residents new rights to find out what personal information companies are collecting and sharing, and to opt-out of the sale of that information.[248]

In September 2019 the EU's competition commissioner Margrethe Vestager was reappointed with an expanded portfolio over digital policy and regulation,[249] signalling a statement of intent around regulating Big Tech following several significant anti-trust decisions by the Commission against Silicon Valley companies.[250] Beyond the USA and Europe, the Australian competition commission published a major report into addressing the power of Google and Facebook, and competition authorities in four out of the five BRICS countries issued an initial report examining digital markets.[251]

A landmark decision by the German competition authority against Facebook in February 2019 provides an example of how taking a joined-up approach between competition and data protection could challenge the core incentives of the surveillance-based business model. The ruling prohibits Facebook from combining data between its different platforms such as WhatsApp and Instagram without consent, directly challenging the company's ability to leverage its control over these platforms,[252] however a regional court suspended the decision pending Facebook's appeal.[253]

---

244. FTC, *Dissenting Statement Of Commissioner Rohit Chopra,* In re Facebook, Inc. Commission File No. 1823109, July 24, 2019

245. see Data Protection Commission Annual Report 25 May- 31 December 2018, Multinational Technology Companies Statutory Inquiries commenced, p 50; *Data Protection Commission opens statutory inquiry into Google Ireland Limited,* May 2019 https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited

246. Commission Nationale de l'Informatique et des Libertés (CNIL), *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, 21 January 2019. Google has appealed the decision.

247. Marcy Gordon and Matt O'Brien, Associated Press, *As feds loom, states hit Facebook, Google with new probes*, 6 September 2019, https://www.apnews.com/5d4d10e28b4841c8a3a723095d4c0d16

248. California Consumer Privacy Act (CCPA), 2018, https://oag.ca.gov/privacy/ccpa

249. Wall Street Journal, *EU Commissioner Who Targeted Tech Giants Gets Second Term,* 10 September 2019,

250. For example, the Commission fined Google €4.34 billion fine for illegally using its Android mobile operating system to "cement the dominance of its search engine", and €1.49 billion over "misuse of its dominant position" in online search advertising. Google has appealed both rulings.

251. Australian Competition and Consumer Commission, *Holistic, dynamic reforms needed to address dominance of digital platforms,* 26 July 2019, https://www.accc.gov.au/media-release/holistic-dynamic-reforms-needed-to-address-dominance-of-digital-platforms ; Brazil's Administrative Council for Economic Defense (CADE), *Cade releases report on digital economy,* September 2019, http://www.cade.gov.br/cade_english/press-releases/cade-releases-report-on-digital-economy-during-the-vi-brics-competition-conference

252. Germany's Federal Cartel Office (Bundeskartellamt), *Bundeskartellamt prohibits Facebook from combining user data from different sources: Background information,* 7 February 2019, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf

253. Herbert Smith Freehills, *German FCO's landmark Facebook decision suspended on appeal,* 27 August 2019, https://hsfnotes.com/crt/2019/08/27/german-fcos-landmark-facebook-decision-suspended-on-appeal

This trend indicates that the era of self-regulation of Big Tech may be coming to an end, and it is highly likely that a combination of enforcement actions and new legislation will lead to substantially greater government oversight of technology companies. These efforts have the potential to ensure Google and Facebook meet their responsibility to respect human rights. But governments must ensure that future regulation of the technology industry is in line with state's obligation under international law to protect individuals and communities from the harmful activities of corporate actors, including through "effective policies, legislation, regulation and adjudication".[254]

CORPORATE LOBBYING

One of the ways Google and Facebook have sought to weaken regulation is by using their resources for extensive corporate lobbying. It is important to note that the companies lobbying efforts encompass a wide range of other business-related issues and not all of the money that Google and Facebook spend on lobbying has human rights implications. However, the high figures that the companies spend on lobbying serve to illustrate their power and political influence. For example, Google spent over 8 million Euros lobbying the EU in 2018, while Facebook spent over 3.5 million Euros.[255] To put this in perspective, Google spent more money than any other company to lobby the EU that year, followed by Microsoft, Shell and Facebook.[256] Google and Facebook lobbied heavily against Europe's General Data Protection Regulation (GDPR), which became directly applicable in all EU member states in 2018.[257]

The companies spend even more money lobbying the US Government. The Center for Responsive Politics, a non-partisan non-profit which tracks lobby spend in the US, states that Google spent US$21.2 million lobbying the US Government in 2018 (up 17.6% from the year before), while Facebook spent US$12.6 million (up 9.6% from the year before).[258] Technology companies also fund a wide range of think tanks to bolster their arguments.[259] Tech companies are lobbying both to ward off potential anti-trust actions, as well as to promote potential federal legislation to nullify stronger existing state-level privacy laws. Tech companies have also pushed back strongly against these state level initiatives, including the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act.[260]

Finally, this lobbying isn't restricted to Europe and the US. According to The Guardian, a leak of Facebook documents earlier this year revealed "a secretive global lobbying operation targeting

254. UN Guiding Principles on Business and Human Rights, Guiding Principle 1

255. See European Union's Transparency Register: Google profile, http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=03181945560-59; Facebook profile, http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=28666427835-74

256. Statista, *The companies spending the most on EU lobbying,* 29 April 2019, https://www.msn.com/en-us/finance/news/the-companies-spending-the-most-on-eu-lobbying/ar-BBWoSWM

257. See, e.g. Laura Kayali, *Inside Facebook's fight against European regulation,* Politico, 23 January 2019, https://www.politico.eu/article/inside-story-facebook-fight-against-european-regulation/

258. See The Center for Responsive Politics, Lobby Firm Profiles: Google, https://www.opensecrets.org/lobby/firmsum.php?id=D000022008&year=2018; Facebook, https://www.opensecrets.org/lobby/clientsum.php?id=D000033563&year=2018

259. Lee Fang, *Silicon Valley-funded privacy think tanks fight in DC to unravel state-level consumer privacy protections,* The Intercept, 16 April 2019, at: https://theintercept.com/2019/04/16/consumer-privacy-laws-california/

260. See, e.g. Kang and Vogel, *Tech giants amass a lobbying army, NYT and Fang, Silicon Valley-funded privacy think tanks fight in DC,* The Intercept, April 2019

hundreds of legislators and regulators in an attempt to procure influence across the world, including in the UK, US, Canada, India, Vietnam, Argentina, Brazil, Malaysia and all 28 states of the EU."[262]

In its response to this report, Google pointed to its transparency listing for third parties it funds and its lobbying disclosures.[263] Facebook states that it maintains compliance with all relevant laws and guidelines when carrying out lobbying activities.[264]

OBSTACLES TO REMEDY

The scale of platforms like Google and Facebook also creates some unique obstacles with respect to the ability of individuals to access and obtain effective remedy after suffering adverse human rights impacts linked to the surveillance-based business model.[265] In part, this is due to inherent challenges that algorithmic systems pose to obtaining access to remedy.

A significant issue is lack of enforcement of existing data protection regulation. Even in Europe, where there is a comparatively strong data protection regime, regulators lack resources and expertise to properly investigate and prosecute violations.[266] Furthermore, private actions by individuals are rare because of "a lack of knowledge of rights, complicated procedures, costly cases and little financial benefits from pursuing cases individually".[267] Globally, there has been an increase in data protection laws, but proper enforcement remains a challenge.[268]

One of the five basic forms of reparation for human rights harms is restitution – meaning restoring the situation to the way it was before the violation occurred. But in the context of corporate surveillance and mass data extraction, restitution may be virtually impossible. The OHCHR makes clear that "The effect of privacy breaches is difficult to undo…The ease of retaining, sharing, repurposing and fusing data and profiles influences the permanence of digital data, meaning an individual may face new and ongoing risks to their rights into the future."[269]

---

261. For California Consumer Privacy Act, see, e.g. Kartikay Mehrotra, Laura Mahoney and Daniel Stoller, *Google and other tech firms seek to weaken landmark California data-privacy law,* Los Angeles Times, 4 September 2019, https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law. For Illinois Biometric Information Privacy Act, see, e.g. Russell Brandom, *Facebook-backed lawmakers are pushing to gut privacy law,* The Verge, 10 April 2018, https://www.theverge.com/2018/4/10/17218756/facebook-biometric-privacy-lobbying-bipa-illinois

262. Carole Cadwalladr and Duncan Campbell, *Revealed: Facebook's global lobbying against data privacy laws,* The Guardian, 2 March 2019, https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment

263. Google, *Our Principles and Standards of Business Conduct,* https://www.google.com/publicpolicy/transparency/, and *Trade Associations and Membership groups,* https://services.google.com/fh/files/misc/trade_association_and_third_party_groups.pdf

264. Facebook response, see Annex below.

265. The right to an effective remedy has been recognized under various international and regional human rights treaties and instruments and also as a rule of customary international law. See e.g. Article 8, Universal Declaration of Human Rights; Article 2 (3), International Covenant on Civil and Political Rights; Article 2, International Covenant on Economic, Social and Cultural Rights.

266. see for example, Reuters, *European regulators: We're not ready for new privacy law,* May 2018, https://uk.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUKKBN1I915X; European Union Agency for Fundamental Rights (FRA), *Access to data protection remedies in EU Member States,* 2013, p 46, https://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

267. Noyb, *Making Privacy a Reality,* 2017, p 8, https://noyb.eu/wp-content/uploads/2017/11/concept_noyb_public.pdf

268. Consumers International, *The state of data protection rules around the world,* May 2018, p 5 https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf; Privacy International, *The Keys to Data Protection, August 2018,* p 7, https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

269. OHCHR, *Right to Privacy in the Digital Age,* A/HRC/39/29, 2018, para 56

Access to information on how a company's operations impact their rights is vital to enable people to claim their right to an effective remedy in cases of corporate human rights abuse.[270] However, the asymmetry of information between Google and Facebook and internet users, and the opacity of the processes of how data is collected, processed and shared, means individuals are often unable to even find out details of whether and how their rights have been affected.[271] An example is the Facebook data that was harvested by Cambridge Analytica: academic David Carroll has spent two years trying to recover his data from Cambridge Analytica but has been unable to do so; if the incident had not been uncovered by investigative journalists, Carroll would not even know his data had been misused.[272]

The UN Special Rapporteur on Freedom of Expression has highlighted how AI systems in general often interfere with the right to remedy.[273] There is an inherent challenge around informing , as "individuals are not aware of the scope, extent or even existence of algorithmic systems that are affecting their rights". This opacity is exacerbated because companies' algorithms are constantly adapting and changing, such that even the designers of the system may not be able to explain how they reached their outcomes.[274]

Finally, the inherently collective nature of the algorithmic impacts on the scale of Google and Facebook's systems presents challenges to pursuing reparations at an individual level. Remedial systems are often not designed to manage impacts of such a large and diffuse scale.[275] As digital rights and technology experts Lilian Edwards and Michael Veale stress, "data protection remedies are fundamentally based around individual rights…while algorithmic harms typically arise from how systems classify or stigmatise groups."[276]

270. Amnesty International, *Injustice Incorporated: Corporate Human Rights Abuses and the Right to Remedy*, 2014, p 157

271. The Human Rights, Big Data and Technology Project, University of Essex, Submission to OHCHR on The Right to Privacy in the Digital Age, 2018, p 8

272. Wired, One Man's Obsessive Fight to Reclaim His Cambridge Analytica Data, January 2019, https://www.wired.com/story/one-mans-obsessive-fight-to-reclaim-his-cambridge-analytica-data/

273. David Kaye, 2018, para 40

274. AI Now Institute, *Annual Report,* 2017, p 30 https://ainowinstitute.org/AI_Now_2017_Report.pdf

275. Berkman Klein Center for Internet & Society, *Artificial Intelligence & Human Rights: Opportunities & Risks*, p 55 https://cyber.harvard.edu/sites/default/files/2018-09/2018-09_AIHumanRightsSmall.pdf?subscribe=Download+the+Report

276. Edwards and Veale, 2017, p22

CONCLUSION AND RECOMMENDATIONS

The rise of the surveillance-based business model has resulted in two companies – Google and Facebook – controlling an architecture of surveillance that has no basis for comparison in human history. This system spans entire continents and touches at least a third of the world's population. In its current form, the surveillance-based business model is incompatible with the right to privacy and poses a serious threat to a range of other human rights.

In practice, the issues set out in this paper go far beyond Google and Facebook. The surveillance-based business model does not only serve the interests of these companies at the very top of the food chain. It has become the core of so many businesses: from the advertisers, to the data brokers, to the start-ups and non-tech companies looking to grow or pivot their businesses to monetize personal data. The model that has been pioneered by Google and Facebook is now the blueprint for the internet, and it is making its way into our homes, workplaces and streets via the 'Internet of Things'.

And yet, despite what everyday users around the world have been encouraged to believe, the internet does not *need* to depend on surveillance. The serious abuses or privacy, freedom of expression and other human rights are not inherent in the technology behind the internet, but to the business model that has become dominant. Facebook and Google chose their business model precisely because it was the quickest way for them to grow. Now it is clear their choice is having profound and far reaching consequences for human rights.

The scale and complexity of the human rights harms linked to the surveillance-based business will require a 'smart mix' of structural solutions. It will take ongoing investigation, analysis and interdisciplinary thinking from a wide range of actors – technologists, academics, civil society, policy experts and policy makers - to arrive at an appropriate set of solutions. Already there is a significant body of academic research and an active multidisciplinary community working on these questions.

The risks to privacy posed by the business model have long been documented. Twenty years ago, when the foundations of the system were being put in place, privacy advocates warned of the dangers of individualised online profiling and the need for legal safeguards. In 2000, the Director of the Electronic Privacy Information Center, Marc Rotenburg, told the US Senate "We warned [a year ago] that self-regulation would fail to protect privacy and that there would be a public backlash against the company's plan to profile Internet users."[277]

277. Marc Rotenburg, *On Internet Privacy and Profiling,* Testimony to US Senate Commerce Committee, June 2000, https://epic.org/privacy/internet/senate-testimony.html. The company referred to was ad tech company DoubleClick, which was later acquired by Google.

However, there is now a major opportunity to finally tackle the problem. Prevailing public attitudes towards the power of Big Tech in the companies' largest markets mean it is evident that further government regulation of the industry is on the way. The risk is that any regulation over the internet must be implemented extremely carefully in order not to harm freedom of expression and other rights. As such, it is vital that whatever form a new regulatory regime takes, it is grounded in a human-rights based approach and addresses the inherent impacts of the surveillance-based business model on the right to privacy and other human rights. In the short-term, there is an immediate need to strengthen enforcement of existing regulation in the face of pervasive, widespread and systemic breaches of data protection laws.

Human rights law and standards already clearly sets out the obligations of States and responsibilities of private actors to take immediate and effective action to protect and respect (as relevant) the right to privacy. In 2016, the Human Rights Council set out a range of steps governments should take towards promoting and protecting human rights and fundamental freedoms online, including for states "to adopt, implement and, where necessary, reform laws, regulations, policies and other measures concerning personal data and privacy protection online".[278]

No one approach will work on its own. Efforts to set much stricter limits on the tracking and use of personal data won't be enough if they don't address the concentration of data – and power – in the hands of Facebook and Google. At the same time, the increasing chorus of politicians, regulators and public intellectuals who propose that Big Tech should be "broken up", will fail to address the systemic human rights abuses unless they push for measures that holistically tackle the surveillance-based business-model itself.

This report is an effort to introduce a human rights lens into the debate and point to a potential way forward.

RECOMMENDATIONS FOR STATES

- Governments must take measures to ensure that access to and use of essential digital services and infrastructure – including those provided by Google and Facebook – are not made conditional on ubiquitous surveillance. This will require enacting and/or enforcing legislation to guarantee people a right 'not to be tracked' by advertisers and other third parties.
- As a first step, companies must be prevented from making access to their service conditional on individuals "consenting" to the collection, processing or sharing of their personal data for marketing or advertising.
- Governments must enact and enforce strong data protection laws with human rights at the front and centre, in line with long-established data protection principles. These laws should restrict the amount and scope of personal data that can be collected, strictly limit the purpose for which companies process that data, and ensure inferences about individuals drawn from the collection and processing of personal data are protected. They should further require that companies are clear with users about the purpose of collecting their personal data from the start and that they do not further process it in a way incompatible with this purpose or their responsibility to respect human rights.
- Governments must also ensure that truly independent national data protection regulators have adequate resources and expertise to meaningfully investigate and sanction violations by Google,

278. UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, June 2016, UN Doc A/HRC/32/L.20

Facebook and other major technology companies. They must also ensure effective individual and collective redress mechanisms.

- Governments should put in place regulation, in meaningful consultation with independent technical experts and affected groups, to ensure oversight over the design, development and implementation of algorithmic systems to ensure companies are held legally accountable for human rights harms linked to such systems, including negative impacts resulting from the optimization decisions of such systems. This is particularly important for systems of the scale and impact of Google and Facebook's platforms.
- Governments should legally require technology companies to carry out human rights due diligence to identify and address human rights impacts related to their global operations, including risks and abuses linked to their algorithmic systems or arising from their business model as a whole.
- Governments must adopt internet-related public policies that have the objective of universal access and enjoyment of human rights at their core. This includes measures that disrupt the market and incentives for corporate surveillance-based business models.
- Governments must enact or enforce regulatory frameworks to ensure people are able to practically exercise their right to choose privacy-respecting alternatives to surveillance-based business models. This includes measures to ensure interoperability rather than just data portability so that people can move between services without social detriment, and to lessen network effects.
- Governments must guarantee access to effective remedy for human rights harms linked to the impacts of technology companies, wherever those harms may occur, including harms resulting from the operations of their subsidiaries (foreign or domestic).
- Governments must invest in, encourage and promote the implementation of effective digital educational programmes to ensure that individuals understand their rights, including their right to seek an effective remedy against any data protection, privacy, and other human rights abuses, when accessing digital services.

RECOMMENDATIONS FOR COMPANIES

- Google, Facebook and other technology companies that depend on invasive data-driven operations amounting to mass corporate surveillance must find ways to transition to a rights-respecting business model. As a first step, companies must ensure that their human rights due diligence policies and processes address the systemic and widespread human rights impacts of their business models as a whole, in particular the right to privacy, and be transparent about how they identified and addressed these impacts as well as any specific human rights risks or abuses.
- Technology companies must refrain from lobbying for relaxation of data protection and privacy legislation and policies where such a relaxation increases the risk of human rights abuses. In their efforts to respect human rights, companies must not undermine states' abilities to meet their own human rights obligations.
- Technology companies must take action to remediate any human rights abuses to which they have caused or contributed through their business operations.

Dear Tanya and Joe,

Thank you for the opportunity to respond to the summary of your forthcoming report about human rights and Facebook's business model. While we appreciate the opportunity to engage with Amnesty International on these important issues, we respectfully disagree with your conclusion that our practices are inconsistent with human rights principles.

Like many other online companies, Facebook is supported through the sale of advertising. This enables billions of people around the world to connect and express themselves, on an unprecedented scale. Amnesty International itself has benefited from this ability to connect: The organization has relied on Facebook ads and other Facebook products to reach supporters, raise money, and advance your mission.

Our business model is what allows us to offer an important service where people can exercise foundational human rights—to have a voice (freedom of expression) and be able to connect (freedom of association and assembly). That's why we were disappointed to see that Facebook's clear contributions to human rights (and human rights organizations) are not mentioned in the "summary of analysis" you shared with us. There are countless examples of how people have used Facebook to advance human rights around the world. And, as a company, we're committed to respecting human rights, including the right to privacy. Our longstanding membership in the Global Network Initiative (GNI)—and our adherence to the governance, privacy, and freedom of expression standards enshrined in the GNI Principles and Implementation Guidelines—reflect this commitment. As you know, these standards are grounded in the UN Guiding Principles for Business and Human Rights (UNGP), the Universal Declaration of Human Rights (UDHR), and the International Covenant on Civil and Political Rights (ICCPR). We are independently assessed every two years on our implementation of our obligations as a GNI member company.

This is an important moment for human rights at Facebook. We recently updated our staffing and leadership on human rights issues, and have just issued new Community Standards Values that explicitly refer to human rights principles. We're engaged in multiple, major, human rights impact assessments, and are about to launch one of this decade's most exciting rights-related experiments, Facebook's Oversight Board. Accompanied by the recent explicit commitment of our top leadership to freedom of expression, and in the midst of designing a significant new initiative for human rights defenders, you can be confident there is much more rights-related work to come.

It also an important moment for privacy at our company. Our robust privacy review process, which brings together a cross-company group of experts to review new products and privacy-related changes to existing products, is about to become even stronger as we implement our recent settlement with the Federal Trade Commission.The settlement requires an unprecedented level of accountability, imposing controls that have never before been required of a company in our industry.

We appreciate the opportunity to respond to the summary you sent us, but we are deeply concerned that it contains a number of inaccuracies and faulty assumptions, the most serious of which we outline here:

1. **Facebook's Business Model and "Surveillance."** Describing Facebook's business model -- which involves selling ads in order to offer services for free -- as "surveillance-based" elides the crucial difference between services that people voluntarily sign up to use, and the involuntary government surveillance that defines the arbitrary interference with privacy, home, family, or correspondence envisaged under article 17 of the International Covenant on Civil and Political Rights.

2. **Data Collection.** We do not "collect as much data about people as possible" or infer people's sexual identity, personality traits or sexual orientation. In fact, we only require

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

people to provide their name, age, gender, and contact information when they sign up for Facebook. We do not have access to the contents of anyone's email.

3. **Non-users.** Like other companies that provide technologies to other websites and apps, we may receive information about non-users when they use those websites and apps. This is part of the basic function of the Internet. We do not use non-user information to build profiles about people.

4. **Interoperability.** Part of our vision for enabling people to message across our apps is making those messages end-to-end encrypted. This means we will collect **less** data about people -- not more, as the summary suggests.

5. **Social plugins.** We do not store data from social plugins (such as the Like button) in identified form unless that's necessary for safety, fraud prevention or security.

6. **Free Basics.** The purpose of Free Basics was not to "gain access to new sources of data." Free Basics does not store information about the things people do or the content they view within any third-party service available through Free Basics.

7. **Engagement.** Our News Feed algorithm is not designed to "maximise engagement." The goal of News Feed is to connect people with the content that is most interesting and relevant to them. Our focus is on the quality of time spent on Facebook, not the amount.

8. **Discrimination and transparency.** The summary fails to mention the many changes we have made to our ads systems in order to help prevent discrimination -- measures that remain unmatched in the industry. Facebook is far from the only place where advertisers run ads for opportunities like housing, employment and credit and we've made fundamental changes for how these ads run on our services. Many of the interest segments mentioned in the summary have also been removed. Transparency is a significant part of how we're addressing this issue, and we have made it easier to see all the ads running on Facebook, regardless of whether they are shown to you.

9. **App Developers.** The summary similarly fails to mention the work we have done to limit the misuse of people's information that we saw in the Cambridge Analytica matter. The summary's suggestion that we recently suspended 10,000 developers because of suspected data misuse is flatly incorrect.

10. **Law enforcement.** Far from "contributing" to unlawful government surveillance, we actively push back against it, scrutinizing every request we receive to ensure it complies with accordance with our terms of service, applicable law, and international human rights standards.

You will note that our processes far exceed the minimum standards set out in the UN's latest guidance on this issue, *The Right to Privacy in the Digital Age.* We hope these points -- and the additional context below -- will help you revise your arguments on surveillance, privacy, and proportionality as you finish your report.

We fully recognize that Facebook has made mistakes in the past, and are committed to continually improving our services and incorporating feedback from the people who use them. We would welcome the opportunity to engage further with you on your report and the important issues it raises.

Sincerely,

Steve Satterfield

Director, Privacy & Public Policy

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

Facebook's Business Model and Data Practices

Your summary characterizes Facebook's business model as "surveillance-based." We strongly disagree with this suggestion.

First, it is important to note that **no one is obliged to sign up for Facebook.** The decision to use our family of apps is entirely voluntary and personal. A person's choice to use Facebook's services, and the way we collect, receive or use data -- all clearly disclosed and acknowledged by users -- cannot meaningfully be likened to the involuntary (and often unlawful) government surveillance and interception of communications defining the kind of arbitrary interference with home, correspondence, or family life envisaged under article 17 of the International Covenant on Civil and Political Rights.

Second, Facebook's business model is not, as your summary suggests, driven by the collection of data about people. Like many other online companies, Facebook is supported through the sale of advertising. As you correctly note, we do not sell data; we sell ads. Doing so allows us to **offer a service that enables everyone to exercise foundational human rights—to have a voice (freedom of expression) and be able to connect (freedom of association and assembly).**

While using the data we collect and receive is an important part of showing effective ads, it is incorrect to suggest that our business model is driven by the desire to collect "as much data about people as possible." Data collection is not an end in itself for Facebook, but rather is the way we provide relevant and useful services to people and organizations. **The only data we require people to provide when signing up for Facebook are the person's name, age, gender, and contact information.** We also enable people to express their gender identity in ways that go beyond male and female.

Over time, as people use our products, we may receive additional data (e.g., the Pages a person likes, the posts and ads they click on), and this data helps us provide content and services that are more relevant to them, such as determining which posts and ads appear higher up in their News Feeds.

Your summary misstates the nature of the data we collect and receive from people. **We do not read the content of people's emails, nor do we infer people's sexual identity, personality traits or sexual orientation. We also do not use the content of people's messages to other people for ad targeting.**

Third, it is vitally important to note the range of controls we give people over the data we collect, store and use. We provide strong controls to allow people to decide what is right for them. This is why we offer tools such as Access Your Information, Ad Preferences and "Why am I seeing this ad?", all of which we are constantly working to improve. We also recently started rolling out a new way for users to view and control off-Facebook activity, and to disconnect this information from their accounts. **These tools provide unprecedented levels of transparency and control,** and strongly surpass the minimums defined in paragraph 30 the UN's most recent thinking on this topic, The Right to Privacy in the Digital Age. Our steady introduction of privacy-protected tools like these belies the summary's suggestion that "Facebook can afford to abuse privacy." To the contrary, we know that if we do not protect people's data, we will lose their trust.

As noted above, data allows us to make ads more relevant. Not only is this a better experience for people; it also has been crucial for the millions of small businesses who have access to the same powerful tools that large businesses do, allowing them to reach people who are more likely to be interested in their products, services, or causes. The efficiency that data brings to advertising has helped businesses and other organizations around the world to grow and advance important

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

causes, including freedom of assembly and association; rights to freedom of expression and political participation; and of course, the right to development.

The summary's suggestion that our goal of making our services more interoperable will enable us to aggregate *more* data about people is flatly incorrect. As our CEO Mark Zuckerberg explained, our vision for the future operation of our services involves making them end-to-end encrypted — which means we will receive ***less* data about people, not more.** End-to-end encryption means that we'll be unable to access the content of people's messages for advertising—or for any other reason.

It is also worth noting that, other than for security purposes and guarding against fraud, **Facebook no longer stores data from social plugins (such as the Like Button) with user or device identifiers.** The limited data that we do keep for security and fraud investigations is stored in separate, access-controlled tables to help ensure that only the relevant security or integrity employees have access to that information. Once the investigation concludes, the data is deleted unless we determine abusive activity has occurred and further action is necessary to protect our products and users.

Although it is correct that we may receive information about people without Facebook accounts when they use a website or app that includes a social plugin (or other Facebook technology), **we do not build profiles about non-users.**

The report's characterization of our Free Basics service is inaccurate. **The Free Basics privacy statement makes clear that the service is not a "data extraction exercise."** To the contrary, Free Basics safeguards people's privacy through strong protections. **Most importantly, Free Basics does not store information about the things people do or the content they view within any third-party service**. Rather, in order to provide access to those services free of data charges, Free Basics temporarily stores only the domains or names of the third-party services visited, after which this information is aggregated or otherwise de-identified. Free Basics continues to be an important tool for bringing more people online and providing a baseline of connectivity for people around the world.

Improving People's Experiences in News Feed

Amnesty's executive summary incorrectly suggests that our algorithms are designed to promote sensationalist content because people are more likely to engage with that content. **The actual goal of Facebook's News Feed is to connect people with the content that is most interesting and relevant to them. Our focus is on the quality of time spent on Facebook,** not the amount. Because the space in each user's News Feed is limited, Facebook's algorithms prioritize posts that are predicted to spark meaningful conversations — including posts from close friends, family, and pages users interact with frequently. This type of content is prioritized over public content, including posts from businesses, brands, and media.

We have also taken steps to reduce the incidence of content that may be engineered to game engagement on Facebook, but that results in a negative or harmful experience for users. For example, we've introduced systems to detect and reduce the distribution of content such as engagement bait, hoaxes, fake news, and clickbait. And we have worked very hard, and successfully, to reduce the virality of hate speech and other inflammatory content in many countries at risk of violence.

We also believe in giving users more information about and control over what they see on Facebook, including on News Feed. In March 2019, we announced a new transparency initiative called "Why I am seeing this post?" which gives users access, for the first time ever, to ranking information about each post in their Feed. We also have tools that allow users to further

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

personalize how they experience News Feed, such as viewing posts in chronological order or choosing to see posts from a particular Page of person at the top of Feed.

Taking Action to Prevent Discrimination and Improve Transparency

One of our top priorities is protecting people from discrimination on Facebook. Our advertising policies have long prohibited discrimination, and we require all advertisers globally to certify compliance with our non-discrimination policy in order to run ads on Facebook.

We are now making fundamental changes in how U.S. housing, employment and credit opportunity ads can run on Facebook. We will not allow advertisers to target these ads to people based on age, gender, ZIP code or any interests describing or appearing to relate to protected characteristics. These changes will be fully implemented by the end of 2019; they're the result of settlement agreements with leading civil rights organizations and ongoing input from civil rights experts. This settlement also included a **commitment that we work with the civil rights community and other experts to study the potential for bias in connection with the algorithms we (and others in the industry) use to show people relevant content and ad**s.

Even before the settlement, we had made changes to the ads system, which advertisers use to select the audience for their ads. We removed thousands of categories from that could potentially relate to protected characteristics. Our review of these audience selection options is continuous and informed by feedback from outside experts.

We are also **building a new section of our Ad Library** that will give people the ability to search for and view all current housing ads in the U.S. by location chosen by the advertiser, regardless of whether a person is in the intended audience. We'll introduce similar sections for U.S. employment and credit ads next year.

These transparency efforts build on our efforts referenced in the report to bring greater transparency to political and issue ads on Facebook. Among other things, these efforts are intended to address so-called "dark ads" that you refer to. We continue to work on more ways to provide transparency in this space, and we appreciate the feedback we have received from the organizations cited in your report.

Addressing Potential Misuse of Facebook Platform Data by Third-Party App Developers

The Cambridge Analytica matter involved a third-party app developer — Aleksandr Kogan — who violated Facebook's policies by selling users' information to a third party, Cambridge Analytica. When we became aware of this issue, we took action quickly to investigate, and we secured sworn certifications from Kogan, Cambridge and others that they had deleted the relevant data. In 2018, reports surfaced that Cambridge may have not, in fact, deleted the data it received from Kogan.

We recognize that Cambridge involved a breach of trust, and we have taken a number of steps to help prevent something like it from happening again. These steps include:

- Reducing the kinds of data that people may share with app developers;
- Preventing apps that a person has not used for more than 90 days from continuing to access a person's data through Facebook;
- Strengthening our App Review process by requiring more apps to submit to upfront review before being able to ask people to share their data;
- Conducting an investigation of apps that had access to large amounts of user information before we changed our Platform in 2015 to prevent people from sharing their friends' information with apps; and

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

- Suspending — and even suing — developers who fail to cooperate with this investigation.

With respect to this investigation, your report states "ten thousand . . . apps were suspended for potentially misusing data." This is incorrect. As we explained in our most recent update on this investigation (which thus far has addressed millions of apps), we have suspended tens of thousands from around 400 developers. Suspension is not necessarily an indication that these apps were posing a threat to people. Many apps were not live but were still in their testing phase when we suspended them. It is not unusual for developers to have multiple test apps that never get rolled out. And in many cases, the developers did not respond to our request for information so we suspended them.

You are correct that carrying out an investigation of this kind is difficult, but it is not accurate to suggest that we do not have sufficient tools at our disposal to identify and take action against developers we have found to have violated our policies. **We are committed to taking strong action — including by taking developers to court, as we have done recently.**

Finally, our new agreement with the FTC also will bring its own set of requirements for oversight of app developers on our Platform. It will require developers to annually certify compliance with our policies. Any developer that fails to follow these requirements will be held accountable.

Protecting Privacy In Connection with Requests from Law Enforcement

Facebook discloses account records in response to valid legal requests in accordance with our terms of service, applicable law, and international human rights standards. Because we are deeply concerned about protecting our users' data, **we carefully scrutinize every request to ensure it meets those requirements.** When we don't believe those standards have been met, we decline to provide the requested data and, if necessary, challenge the request in court. We've done this, for example, when the requesting government exceeded its authorities in making the data request, or we are concerned the request doesn't comply with international human rights standards.

We openly publish how we enforce our Community Standards, and how we respond to government data requests, in our regular Transparency Reports. They are worth studying.

Engaging With Government Officials on Important Public Policy Issues

As we've said in our annual political engagement statement, public policy decisions can have significant implications for the people who use our services and the future direction of our company. Facebook regularly engages with government officials to discuss a range of policy issues as well as share information about our products and services. In doing so, we maintain compliance with all relevant laws and guidelines. All Facebook Personnel, including external consultants, who engage with government officials to discuss policy issues on our behalf receive training on the ethical standards required in all such interactions.

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US


info@amnesty.org


+44 (0)20 7413 5500

JOIN THE CONVERSATION


www.facebook.com/AmnestyGlobal


@AmnestyOnline

SURVEILLANCE GIANTS:

HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS

Google and Facebook help connect the world and provide crucial services to billions. To participate meaningfully in today's economy and society, and to realize their human rights, people rely on access to the internet—and to the tools Google and Facebook offer.

But despite the real value of the services they provide, Google and Facebook's platforms come at a systemic cost. For people to enjoy their rights online they are forced to submit to being constantly tracked across the web and in the physical world as well, for example, through connected devices. The surveillance-based business model of Facebook and Google is inherently incompatible with the right to privacy and poses a threat to a range of other rights including freedom of opinion and expression, freedom of thought, and the right to equality and non-discrimination.

Governments must take positive steps to reduce the harms of the surveillance-based business model—to adopt digital public policies that have the objective of universal access and enjoyment of human rights at their core, to reduce or eliminate pervasive private surveillance, and to enact structural reforms sufficient to restore confidence and trust in the internet. Google, and Facebook and other technology companies must put an end to ubiquitous surveillance and transition to a rights-respecting business model.

Index: POL 30/1404/2019
Novemeber 2019
amnesty.org

AMNESTY INTERNATIONAL