



Our 2019 compilation of research and stories explains what's key to a healthier internet across five issues, from personal experience to global concerns.



## 04 Readme

### 2019 Spotlights

- 06 Let's ask more of AI
- 10 Rethinking digital ads
- 14 The power of cities

### Privacy and Security

- 18 How safe is it?

### Openness

- 29 Is it open?

### Digital Inclusion

- 40 Who is welcome?

### Web Literacy

- 52 Who can succeed?

### Decentralization

- 63 Who controls it?

### Participate

- 78 10 minutes to a healthier internet
- 79 Join the movement

Rights and Permissions: This work is available under a Creative Commons Attribution 4.0 International license (<https://creativecommons.org/licenses/by/4.0/>), excluding portions of content attributed to third parties. Under this license, you are free to copy, redistribute, and adapt the material, even commercially, under the following terms:

Attribution — Please cite this work as follows: Mozilla, Internet Health Report v.1.0 2018. CC BY 4.0  
[link: <https://creativecommons.org/licenses/by/4.0/>]

Adaptations — If you remix, transform, or build upon this work, please add the following disclaimer along with the attribution: "This is an adaptation of an original work by Mozilla. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by Mozilla."

# Readme

Is the internet unhealthy? We planted this question in your mind with the title of this report and in the questions we ask throughout. But you will not be getting a simple yes or no answer.

As you may have gathered, this publication is neither a country-level index nor a doomsday clock. We invite you to join us in assessing what it means for the internet to be healthy, and to participate in setting an agenda for how we can work together to create an internet that truly puts people first.

Our intention with this compilation of research, interviews and analysis (designed with input from hundreds of readers in collaboration with over 200 experts) is to show that while the worldwide consequences of getting things wrong with the internet could be huge – for peace and security, for political and individual freedoms, for human equality – the problems are never so great that nothing can be done. More people than you imagine are working to make the internet healthier, and getting things right, by applying their skills, creativity, and even personal bravery, to business, technology, activism, policy and regulation, education and community development.

This annual report is a call to action to recognize the things that are having an impact on the internet today through research and analysis, and to embrace the notion that we as humans can change how we make money, govern societies, and interact with one another online.

Part of the trouble in explaining how to make the internet ‘healthier’ is that so much goes unseen. As internet users, we tend not to think about fibre optic cables beneath the seas, or

the men and women who assemble our electronic devices, let alone about the decision processes coded into “intelligent” machines. Many of us don’t even know how our favorite internet companies profit, or how our personal desires and traits are tracked as we go about our lives.

If we’re completely honest, a lot of us would probably prefer *not* to know. Why ruin the magic of the instant gratification we get at the push of a button, hiding all technological processes behind the scenes. The downside is that we often don’t recognize the things in need of systemic change before the dramatic news headlines assault us. We prefer to imagine that we are protected: by high tech internet companies, by governments, by other more savvy users.

We make choices all the time: about what software to use, what security risks to take, what steps to take to protect the privacy of our children and genetic relatives. As advocates for a healthier internet, let’s now make *better* choices. Let’s fight to change what is wrong and join with others to make things right. In reading the Internet Health Report, let’s cast a glance at the seen *and* unseen opportunities of the internet, and consider this rich, diverse, complex ecosystem as one that adapts to our collective actions and changes over time.

Our “spotlights” this year invite you to consider three topics that in each their way are ‘hidden in

plain sight' and deserve special attention if we are to improve the health of the internet.

Our societies and economies will soon undergo incredible transformations because of the expanding capabilities of machines to “learn” and “make decisions”. How do we begin to make tougher demands of artificial intelligence to meet our *human* needs above all others?

By now, you've surely heard that targeted advertising ads and personal data collection are at the heart of so much that is wrong with the

internet. What are promising efforts to make things right?

More than half of the world's population lives in a city now. You had better believe that officials face tough challenges (and divergent interests) when it comes to putting ideals for a healthier internet into practice. No, this is not about “smart cities”, but about the untapped power of city governments and civil society to work together to make the internet healthier worldwide.

## Credits

So many researchers, fellows, writers and allies of Mozilla generously contributed data and ideas alongside countless readers who participated.

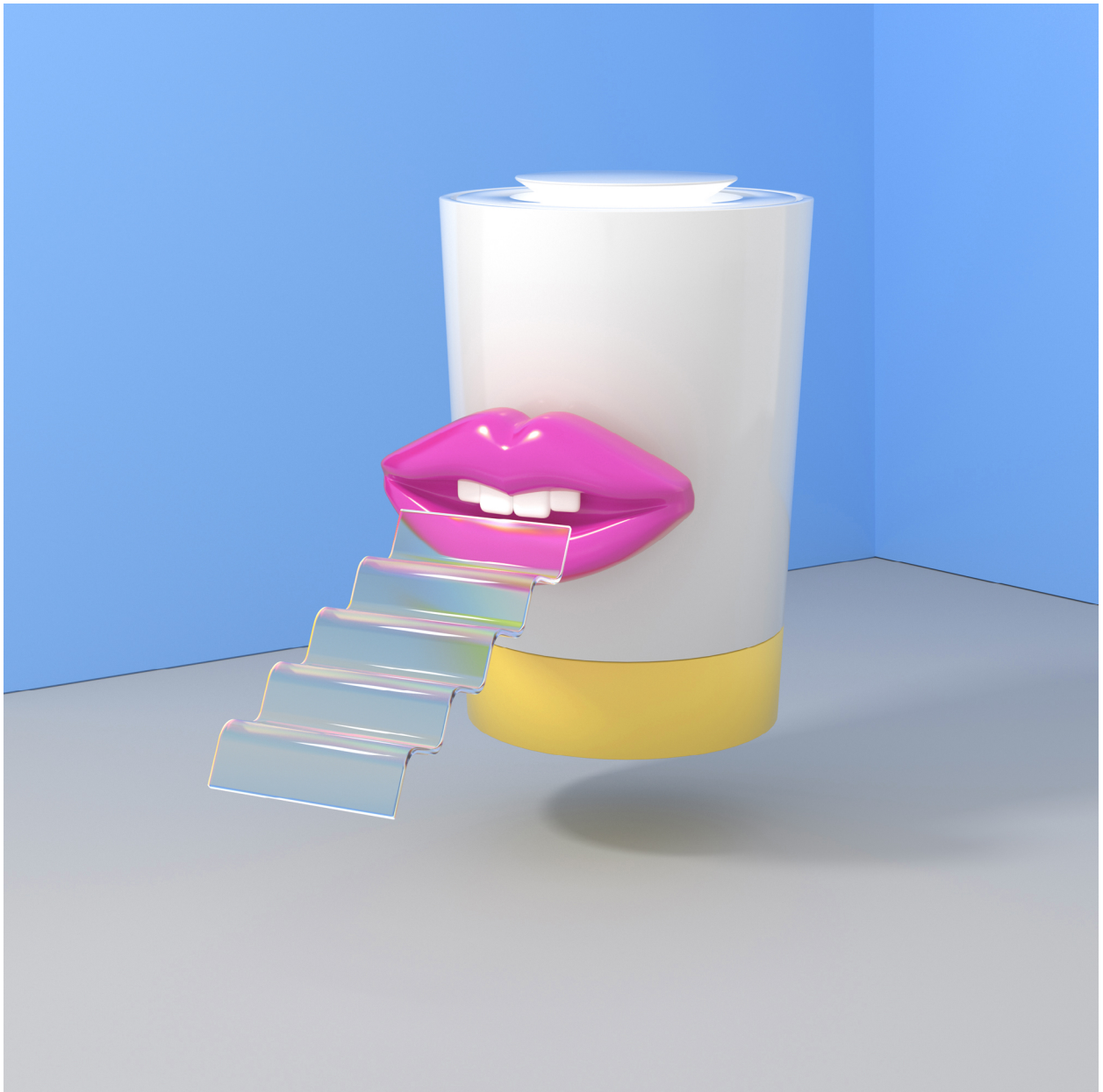
See the full list of contributors in the online version of the report

Solana Larsen is the editor of this report.  
Kasia Odrozek is the project manager.  
Jairus Khan is the outreach coordinator.  
Stefan Baack is the data and research analyst.  
Eeva Moore is the editorial assistant.

Contact us:  
[internethealth@mozillafoundation.org](mailto:internethealth@mozillafoundation.org)

For press inquiries visit:  
[internethealthreport.org/press](http://internethealthreport.org/press)

The creative studio and digital agency Rainbow Unicorn in Berlin, Germany developed the visual design and code, Christian Laesser developed the data visualizations and Julian Braun produced the 3D artwork. The entire report will be translated by Global Voices from English to French, Spanish and German (with staggered launch dates).



Openness

Spotlight

## Let's ask more of AI

Stefania Druga from Romania teaches artificial intelligence (AI) programming to children. As a researcher, she has also studied how 450 children in seven countries interact with and perceive connected toys and home assistants, like Amazon Alexa or Google Home.

Children can understand more than parents think, she says — including that machine learning is limited by what training data you have to work with.

The philosophy behind the software she developed for teaching is that if children are given the opportunity for agency in their relationship with “smart” technologies, they can actively decide how they would like them to behave. Children gather data and teach their computers.

This simple approach is what we urgently need to replicate in other realms of society.

In order to navigate what implications AI has for humanity, we need to understand it — and then decide what we want it to do. Use of AI is skyrocketing (for fun, as well as for governance, military and business) and not nearly enough attention is paid to the associated risks.

“Yup, it’s probably AI,” says Karen Hao’s back of the-envelope-explainer about any technologies that can listen, speak, read, move and reason. Without necessarily being aware of it, anybody who uses the internet today is already interacting with some form of AI automation.

Thought of simply, machine learning and AI technologies are just the next generation of computing. They enable more powerful automation, prediction and personalization.

These technologies represent such a fundamental shift in what is possible with networked computers that they will soon likely make even more headway into our lives.

Whether search engine results, music playlists, or map navigation routes, these processes are far from magical. Humans code “algorithms” which are basically formulas that decide how decisions should be automated based on whatever data is fed into them.

Where it begins to feel magical is when it makes new things possible. This Person Does Not Exist is a good example. If you visit the website and refresh the page, you will be shown an endless array of faces of people who never existed. They are images that are generated at random by a machine learning algorithm composite based on a database of faces that do exist.

Look closely, and you will spot the errors — ears that are crooked, hair that doesn’t fall naturally, backgrounds that are blurred. This Cat Does Not Exist is less convincing. The potential exists for either photo generator to improve with additional data and guidance. And the risks that such photos could be used to misrepresent reality also exists, even for such whimsical creations.

In recognition of the dangers of malicious applications of a similar technology, researchers from OpenAI sparked a media storm by announcing they would not release the full version of an AI technology that can automatically write realistic texts, based partly on the content of 8 million web pages. “Due to our concerns about malicious applications of the technology, we are not releasing the trained model,” they wrote, calling it an experiment in “responsible disclosure”.

Such recognition of the faultlines and risks for abuse of AI technologies is too rare. Over the last 10 years, the same large tech companies that control social media and e-commerce, in both the United States and China, have helped shape the AI agenda. Through their ability to gather huge quantities of training data, they can develop even more powerful technology. And they do it at a breakneck pace that seems incompatible with real care for the potential harms and externalities

Amazon, Microsoft and others have forged ahead with direct sales of facial recognition technology to law enforcement and immigration

authorities, even though troubling inaccuracies and serious risks to people of color in the United States have been rigorously documented and defended. Within major internet companies that develop AI technologies, including Amazon and Google, employees have sounded alarms over ethical concerns more urgently.

Company leaders deflect with confidence in their business models, hubris about their accuracy, and what appears to be ignorance or lack of care for the huge risks. Several companies, including Axxon, Salesforce, and Facebook, have sought to allay concerns over controversies by creating ethics boards that are meant to oversee decisions.

Co-founder of the research institute, AI Now, Meredith Whittaker, calls this “ethics theater” and says there is no evidence that product decisions are run by them, or that they have any actual veto power. In an interview with Recode, Whittaker asked of the companies, “Are you going to harm humanity and, specifically, historically marginalized populations, or are you going to sort of get your act together and make some significant structural changes to ensure that what you create is safe and not harmful?”

As it happens, Google’s announcement of an ethics board backfired spectacularly in April 2019 and was dismantled after employee protests and public outrage about who had (and hadn’t) been asked to join. While the company has been vocal about establishing principles for AI, and has engaged in social good projects, it also has competing priorities across its many ventures.

What are real world ethical challenges these boards could tackle if they took Whittaker’s advice? One idea would be to question an everyday function billions of people are affected by. Google’s video platform, YouTube, is often said to be a “rabbit hole” -- endless tunnels leading

from one video to another. Though YouTube denies it, research shows that content recommendation algorithms are fueling a crisis of disinformation and cultish behavior about vaccines, cancer, gender discrimination, terrorism, conspiracy theories and [add your topic].

Similarly, Pinterest and Amazon are also platforms that drive engagement by learning and suggesting new and engaging content. They experience variations of the same problem. In response to public scandals, they have each announced efforts to stop anti-vaccine content, but there is little evidence of any real change in the basic intention or function of these systems.

But it’s not just technology companies that need to be interrogating the ethics of how they use AI. It’s everyone, from city and government agencies to banks and insurers.

At the borders of nine European Union countries, an AI lie detector was tested to screen travelers. Systems to determine creditworthiness are being rolled out to populations in emerging markets in Africa and Asia. In the United States, health insurers are accessing social media data to help inform decisions about who should have access to what health care. AI has even been used to decide who should and shouldn’t be kept in prison in the United States.

Are these implementations of AI ethical? Do they respect human rights? China, famously, has begun scoring citizens through a social credit system. Chinese authorities are now also systematically targeting an oppressed minority through surveillance with facial recognition systems.

Where do we draw the line?

There are basically two distinct challenges for the world right now. We need to fix what we know we are doing wrong. And we need to decide what it even means for AI to be good.



Cutting humans out of government and business processes can make them more efficient and save costs, but sometimes too much is lost in the bargain.

Too rarely, do people ask, should we do this? Does it even work? It's worth questioning whether AI should ever be used to make predictions, or whether we should so freely allow it into our homes.

Some of the most worst missteps have involved training data that is faulty or simply used with no recognition of the serious biases that influenced its collection and analysis.

For instance, some automated systems that screen job applicants consistently give women negative scores, because the data shows it's a field currently dominated by men.

"The categories of data collection matter deeply, especially when dividing people into groups," say the authors of the book Data Feminism, which explores how data-driven decisions will only amplify inequality unless conscious steps are taken to mitigate the risks.

It seems that if we leave it up to the nine big companies that dominate the field of AI alone, we raise the spectre of a corporate controlled world of surveillance and conformity — especially so long as gender, ethnic and global diversity is also lacking among their ranks of employees at all levels of a company. Having engineers, ethicists and human rights experts address collaboratively how AI *should* work increases the chance for better outcomes for humanity.

We are merely at the beginning of articulating a clear and compelling narrative of the future we want.

Over the past years, a movement to better understand the challenges that AI presents to the world has begun to take root. Digital rights specialists, technologists, journalists and researchers around the globe have in different ways urged companies, governments, military and law enforcement agencies to acknowledge the ethical quandaries, inaccuracies and risks.

Each and everyone of us who cares about the health of the internet — we need to scale up our understanding of AI. It is being woven into nearly every kind of digital product and is being applied to more and more decisions that affect people around the world. For our common understanding to evolve, we need to share what we learn. In classrooms, Stefania Druga is making a small dent by working with groups of children. In Finland, a grand initiative sought to train 1% of the country's population (55,000 people) in the elements of AI. What will you do?

#### **Further reading:**

Situating Methods in the Magic of Big Data and Artificial Intelligence, danah boyd, M.C. Elish, Communication Monographs, 2017

AI Now 2018 Report, AI Now Institute, December 2018

Data Feminism, Catherine D'Ignazio, Lauren Klein, MIT Press Open, January 2019

Anatomy of an AI system, Kate Crawford and Vladan Joler, SHARE Lab and AI Now Institute, 2018



Privacy and Security

Spotlight

# Rethinking digital ads

When dozens of people fell gravely ill from eating romaine lettuce in 2018, public health authorities in the United States and Canada could not figure out where the E. coli contaminated leaves were farmed.

The lettuce had changed hands so many times from washing, chopping, packing to shelving that they couldn't retrace the steps. The only option was to temporarily declare *all* romaine lettuce, from any source, unsafe.

It's a stretch of the imagination, but let's compare that to what we are experiencing in the world of "personalised" or "targeted" digital ads.

We have absolutely no idea of the ingredients that go into the daily bread of the internet. The ads we are served as we use mobile apps and browse the Web are like lettuce leaves scattered over the planet — they can be healthy — but information about the supply chain is muddled and we have no way to understand what is happening.

Pretty much everything we do when we interact with the internet can be tracked by someone (or something) without our knowledge. From the websites we visit, to the apps on our phones, to the things we write in emails or say to voice assistants. We have no way of knowing how this big salad of data may be combined by different companies with information that uniquely identifies us.

It appears that collecting data about everything and anything we do is of commercial interest to *someone*, whether app developers, insurance agents, data brokers, hackers or scammers. The lines have been blurred between what's public and private information. Your credit card may share a list of what you buy in stores with Google. Your online dating profile has perhaps been copied and resold. Why *is* this?

Not all data about you is used to sell ads, but it is primarily because of the ad-driven internet economy that data has become such a hot commodity. It is why people now speak of surveillance capitalism and the attention economy. The phrase "You are the product" precedes the

internet, but has gained new currency as a way to explain how so much online can be "free". Personal data may seem like a small price to pay. But the added social tax is now mounting threats to freedom and human rights.

To talk about the positives: Digital ads have been a boon to the global economy. Free online services have driven the uptake of mobile internet around the world. Ads have helped publishers and startups monetize their online content and services.

For some of the most powerful companies of the internet, Google, Facebook and Baidu, ads are a primary source of revenue even as they have expanded their business into multiple directions and geographies. For Google and Facebook, especially, access to data is a source of global market power and leverage for business negotiations. For the first time, in the United States, digital ad spending is bigger than for print and television.

The ad-tech industry is vast, but by some estimates Facebook and Google alone controlled around 84% of the global digital ad market in 2018 outside of China. To succeed, they have developed product design practices which are centered on holding the user's attention and maximizing engagement to drive revenue from ads.

Targeted ads for the most part promote run of the mill products and services, but these same tools can just as easily be exploited by people with criminal or hateful intentions. In a few minutes, you can place content on videos in YouTube, news feeds of Twitter and Facebook, and search results of Google. By selecting what demographic to target, advertisers on some platforms have been spotted excluding people of a certain race or gender from housing or job ads. Or in the case of Facebook, even directly

targeting “affinity groups” like “Jew Haters” (yes, really). Facebook said its categories are created by algorithms, and when confronted said it would make changes, but it begs the question of how much data should be collected and what it should ever be used for.

Your data profile is a sandwich of data that you knowingly or unknowingly share, which is interpreted by secret algorithms that make use of statistical correlations. For instance, searching online for “loan payment” might say something about your finances. And if you “like” articles or join Facebook groups that could help define your affinities.

“Ads can be done in a more privacy friendly way. But publicly-traded corporations have a duty to maximize shareholder profits, which for some companies means squeezing every drop of data out of their users,” says Casey Oppenheim, the CEO of Disconnect, an online privacy tool that blocks trackers and helps guard personal information from prying technologies.

The journey to a comparison with a public health crisis (remember the lettuce?) is in no small part due to the fact that the ad-tech industry, despite a focus on “better ads”, has neglected privacy for years and still faces accusations of skirting privacy and consent today. Even the supposed accuracy with which the value of an ad purchase can be seen is a myth. It’s an open secret that a huge portion of the internet traffic directed to ads is actually from bots and not humans. An estimated \$6.5 billion USD are lost to fraud by advertisers globally in 2017 because of websites that cash in from using bots to inflate numbers.

Many advertisers are angry and have demanded more transparency in the supply chain. “Silicon Valley has created a fetish around automation,” says Rory Sutherland. He is the vice chairman of the advertising agency Ogilvy in the United

Kingdom, and says an obsession with measuring results of targeting has led to a decline in the quality of ads compared with traditional mass media marketing. “The obsession with targeting means what you are rewarding is your algorithm’s facility at identifying a customer,” he says. He compares it to walking into a pub with a piece of paper that says, “Drink beer!” Most people are already there to drink beer, he says. “What about the people outside?”

In 2017, a number of major marketers stopped placing ads on YouTube after a slew of scandals over ads on violent and inappropriate videos. For the general global public it can be jarring to see such content monetized. It adds to the sneaking sense of discomfort that is growing among many internet users for every report of breached data, security flaws, and too-far-reaching data sharing agreements with other companies. Can we really trust these companies with our data?

As internet users we may have more ‘awareness’ about privacy, but still no clear sense of what to do. We are deeply dependent on companies we wish would protect us.

In a restaurant, a food and safety inspector has a checklist of things to look for that may be a danger to public health. The Corporate Accountability Index of the organization Ranking Digital Rights is a kind of checklist too — but a complex one that ranks what the biggest internet and telecom companies disclose about how they protect the privacy and freedom of expression of users. By publicly scoring companies — and none scores high — the small but influential organization creates an incentive for companies to improve year over year, and a method to track noticeable progress and setbacks over time.

Natalie Maréchal is a senior research analyst with Ranking Digital Rights in Washington D.C.

She is leading an open consultation process to create entirely new indicators for the index related to targeted advertising. “We need to decide together, what standards for disclosure and good practice should be used to hold these companies accountable,” she says. Ranking Digital Rights’ current ideas for best practices will sound familiar to many internet researchers and digital rights organizations. Among other things, they suggest companies should allow third-party oversight of the parameters for ads (eg. “affinities”) and of who is paying for them. And that companies should state rules for prohibited content and use of bots — and publish data regularly to show how they are enforced.

Such tools and practices *have* begun to emerge out of companies already. Not of their own initiative, but compelled either by regulations or public pressure. This year, Facebook says they will roll out political ad transparency tools globally by June. In 2018, Google say they killed over two billion “bad ads”. And Facebook took steps to remove 5,000 ad categories to prevent discrimination. Twitter began collecting more personal data in 2017, but now also gives you to control to change how they categorize you.

Data privacy regulations are improving in numerous countries and states, and courts and civil society are taking companies to task around the world on matters of data collection and consent for targeted advertising. Regulation helps!

And so does technology. To protect the security of users, most major browsers have introduced different variations of tracking protection (and sometimes also ad blocking). Total or partial ad blocking by different companies in different configurations has gone fully mainstream with hundreds of millions of users. It makes the Web faster, and batteries last longer.

Coming back to the lettuce. What would the equivalent of “farm to table” in food activism be for digital ads? Perhaps we would see who paid for ads, understand why we are targeted, and have control over who is collecting our data for what.

What really needs rethinking today is the notion that digital ads can only be effective when they are targeted, and when companies know everything about everyone. Many brands and marketers are backing away from this idea for lack of evidence. Unless internet companies are able to regain our trust by changing practices (or perhaps be legally compelled to protect our secrets and interests, like doctors and lawyers), we can invest some hope in a new generation of software initiatives that explore decentralized solutions to give people personal control over who has access to their data.

“I spent 10 years working with an environmental health organization and I have always seen parallels to the privacy world,” says Oppenheim. “Just like we can connect people to the values of the food they eat, we can also connect them to the value of their data.”

#### **Further reading:**

A Grand Bargain to Make Tech Companies Trustworthy, Jack M. Balkin, Jonathan Zittrain, The Atlantic, 2016

It’s time for a Bill of Data Rights, Martin Tisne, MIT Technology Review, 2018

Corporate Accountability Index, Ranking Digital Rights



Decentralization

Spotlight

# The power of cities

When the Amazon Kindle was released, their ebooks didn't work with commonly used screen readers, making accessibility difficult for the blind community.

The National Federation of the Blind (NFB) in the United States campaigned to change this for years, in vain. Then Amazon won a \$30 million USD contract with the New York City Department of Education in 2015 to create an ebook store for educators in 1,800 schools. City schools delayed a final vote until Amazon and the NFB came to an understanding. Since then, the Kindle now has a built in screen reader and Amazon has improved accessibility across many products.

This is an example of how cities have huge potential power to improve the health of the internet ecosystem. In this case, it was a win for children and educators in New York, but also for people around the world. Where consumers may have a hard time persuading giant corporations to do something that they perceive as going against their business interests, a million dollar procurement contract and a commitment to serving the public interest can help.

More than half of the people in the world now live in cities and by 2050 that number is expected to rise to 68%. Cities are where wealth and power is concentrated in most countries, and also where many technology initiatives are rolled out and tested in communities. What we may think of as local decisions today, may be of global consequence in the future.

When the Federal Communications Commission (FCC) of the United States backed away from protecting net neutrality in 2018, a network of city mayors formed to use their combined purchasing power to support internet providers who continued upholding net neutrality.

“In NYC alone, we spend over \$600 million annually to provide internet service to city employees and to offer city services. So, we convened an ad hoc coalition, starting with eight cities committed to only purchasing from broadband

providers that honor net neutrality principles. Now, this coalition is over 130 cities,” says Max Sevilla, the Director of External Affairs for the NYC Mayor’s Office of the Chief Technology Officer.

This story and many others are highlighted in a publication called the New York City Internet Health Report. Its creator, Meghan McDermott, adapted the format of the global Internet Health Report as part of a Mozilla fellowship project to explore among other things how cities can be strong advocates for digital rights by nurturing relationships with civic tech communities.

“The core of the digital rights agenda is to re-frame how we think about and deploy technology in cities. The idea is to recapture the dignity and purpose of technology as a public good,” says McDermott, who has worked at the intersection of education and digital rights for years — formerly as director of strategy for Mozilla’s Hive Learning Networks, a peer community for digital literacy.

When the internet and connected devices are applied to solving problems in cities, it tends to be referred to as a ‘smart city’ initiative. These are often projects to improve the efficiency of energy, transportation or any number of government services. For instance, it could be trash cans with sensors that alert waste management authorities when they need emptying, or parking meters that can help people find free parking spaces in crowded streets.

Such futuristic ideas have excited city officials around the world, and the global market for ‘smart city’ technologies is worth hundreds of billions of dollars and growing. But frankly it’s also an industry where corporate interests and techno-utopianism holds high currency — where flying taxis and autonomous helicopters end up described as a solution to traffic

congestion, even though they most likely won't solve anything for people who rely on public transport.

The harshest critics say a hype about 'smart cities' has led to massive investments in what is essentially surveillance technology under the guise of technological progress. In both resource rich and poor cities, there are cameras, sensors, microphones, and huge multi-year procurement contracts with companies that have questionable data practices. In this way, with scant attention to data privacy, the internet has arrived to cities worldwide, for better or worse.

Where some see an opportunity to entirely rethink how cities collect data about neighborhoods to improve services, others see a lack of transparency and a recipe for a civil rights disaster spurred on by corporate interests. Where some see energy efficient LED streetlights that help gather data about pedestrians with cameras, others see a surveillance dragnet encroaching on freedom in public space and putting vulnerable populations at risk. Time and again, there are design choices that could be made to minimize the risk of abuse. For instance, when could it be preferable for privacy to use a thermal sensor to collect crowd data instead of a camera?

Digital rights advocates are cast as enemies to progress in such conflicts, but it really boils down to a core difference in opinion about whose interests technology should serve, how to seed social innovation, and what data should be used (or not) in the public interest.

Consider the electronic sensors in the garbage cans. To some, that's a great example of how technology can help cities operate more efficiently. To others, like Tamas Erkelens who is the program manager of data innovation in the mayor's office of the City of Amsterdam, it's

evidence of a wasteful approach that characterizes many 'smart city' innovations.

"We wouldn't need sensors in every trash can if cities could have Google Map data to see where crowds are," says Erkelens. "Wherever people are convening is a good enough indicator of where there is likely to be more trash. We can then use sensors just to train the models, rather than to create new data by machines with batteries that need to be changed," he says.

Many city governments and open data advocates worldwide peer enviously at the wealth of data held by internet companies like Google, Uber, Apple and Airbnb knowing that it could help them understand crucial things about traffic, housing and employment. In 2018, the Open Data Institute in the United Kingdom published a report suggesting that mapping data companies should be compelled to share geospatial data with rival firms and the public sector, to stop "data monopolies" from forming and to create better opportunities for innovation.

Some companies do share aggregated data with city planners, including Uber, but cities are also getting smarter about requesting things like usage data of electric scooters upfront as a condition of doing business. The city of Barcelona is one of very few cities that operates under the principle that all data collected in the duty of local government in public space must be available in a data commons platform. Erkelens says Amsterdam is using its annual procurement budget of €2.1 billion to help guarantee good terms for data privacy too, and that Barcelona and Amsterdam together are experimenting with partners in the European Union to develop new technologies that also give citizens more direct control over their own data.

At the Smart Cities Expo World Congress in Barcelona in November 2018, the chief technology



officers of Amsterdam, Barcelona and New York together launched the Cities Coalition for Digital Rights in partnership with UN-Habitat, a United Nations program to support urban development. Cities who join the coalition agree to a declaration of just five principles that center on respect for privacy and human rights in use of the internet. They pledged to see 100 cities join in 100 days (before July) and 35 cities have joined so far. Declarations may come and go, but these cities aim to sow the seeds of a movement whereby cities decisively claim digital rights. By working together and establishing best practices they will attempt to win a race against technological progress that is not centered on principles of human dignity and inclusivity.

Despite the strong stances taken in New York, Barcelona and Amsterdam, people who do digital rights work at the city level describe an uphill battle of culture change within large and in some parts traditional institutions with multiple agencies and divergent interests. Creating the policies and processes by which all agencies can make better decisions about privacy, data and transparency — and opening up key parts of the work to civil society — is a key part of the challenge.

This is where the civic tech community has blossomed in countless cities. Diverse groups of public interest startups, technical students, officials, and engaged citizens team up to hack bureaucracy and code in an attempt to make cities more responsive to their residents. They work from the inside with willing partners, and from the outside through advocacy groups, research, and live prototypes that reimagine how more responsive systems could work.

Cities worldwide are on the frontline of decisions that affect the health of the internet for all people. At the local level, whether in rural or

urban communities, there are opportunities for civic engagement regarding the internet that can be more direct than at the national level. We should seize opportunities to influence how technology is used (or isn't) in our own communities, and encourage elected officials to be champions of digital rights. The more engaged we are locally, the more empowered cities will be to cast themselves as opponents to internet policies at the national or international level when they go against the interests of people.

The challenge for cities is to advance the intentional adoption of digital tools that advance values of diversity, inclusion and fairness that they already hold, rather than jumping on the latest 'smart city' trend.

When he helped facilitate conversations between Amazon and The National Federation of the Blind over ebooks, Walei Sabry in New York already worked in the Mayor's Office of People with Disabilities. Since then he has also become New York City's first official digital accessibility coordinator. About 'smart cities' he says, "These initiatives can go really well or really wrong depending on who's at the table — people with disabilities must be involved at all stages of the process... because what works for us makes products better for everyone."



Privacy and Security

Introduction

# Is it safe?

The internet is where we could live, love, learn and communicate freely. To be ourselves, we need to be able to trust the systems that protect us.

A tectonic shift in public awareness about privacy and security in the digital world has occurred in the past year. Some are even calling it “the great privacy awakening.”

In 2018, news broke that data analytics firm Cambridge Analytica had harvested data of millions of Facebook users, without their knowledge, and used it for political purposes — including attempts to influence elections in the United Kingdom and the United States.

Public outrage was swift and widespread. Campaigns to make Facebook private by default and to ask users to delete the platform outright took off. Nearly three-quarters of Americans and Canadians reported tightening their Facebook security or distancing themselves from the site altogether. Facebook was grilled in the U.S. Congress and the Canadian House of Commons, fined by the U.K. and sued by the District of Columbia. The company’s stock plummeted.

All this was a symptom of a much larger, systemic issue: the dominant business model and currency of today’s digital world is based on gathering and selling data about us.

Our data-rich digital age has some benefits. Streaming music services recommend songs, based on what we’ve listened to. Voice recognition technology lowers barriers to access to the internet. City planners have access to more data. Yet, as devices on our streets and in our homes gather more data, a fundamental question remains: Are we too exposed?

Does our awareness extend to making informed choices about commercial DNA tests? Or the privacy settings for apps and online services. We should know the risks of ransomware attacks, why strong passwords are vital and how to judge the security of devices we buy.

We can also support products and services that

protect and respect our privacy — like the Tor and Firefox browsers — and demand that other companies do better.

But the responsibility for a healthy internet cannot rest on the shoulders of individuals alone. Just in 2018, millions of people were affected by breaches at Google, Facebook, Quora, Marriott and many others. Over 1 billion Indian citizens were put at risk by a vulnerability in Aadhaar, the government’s biometric ID system. Telecommunications providers, including Telus, AT&T and Sprint, were caught selling customers’ location data. We need more protection from companies and governments.

There were also bright spots in the last year. Europe’s General Data Protection Regulation (GDPR) came into effect, and digital rights organizations are collaborating to ensure it is enforced. Public pressure caused several hackable toys to be pulled off the shelves.

Mark Zuckerberg recently stated that he is committed to “a privacy-focused vision for social networking.” But Facebook is also under criminal investigation for data sharing deals with companies including Amazon, Apple, Microsoft and Sony. It’s going to take more than words to rebuild the trust that’s been lost, not only with Facebook but in the internet overall.

Calls for more privacy regulation are on the rise around the world, some inspired by the idea that companies should treat our data with the same care that a bank would treat our money.

The debate about the dominant business model of the internet — and its implications for the privacy and security of our digital lives — will undoubtedly continue in the years to come. As it does, it’s important that we remember the current reality is a human creation, not a technological inevitability. We built this digital world, and we have the power to change it.

# Ransomware payments add up

We don't know who is making the payments, or who is receiving them. But by looking at the public protocols of Bitcoin accounts associated with ransomware we can see the trail of money paid.

How much would you pay to regain access to your computer files? This is a question victims of ransomware are faced with when they least expect it. A threatening message appears promising to delete all files unless a payment is made before a certain time.

"My first reaction was panic. My second reaction was to get on another computer and figure out exactly how much 1.71 Bitcoin was worth in US dollars," said John, a lawyer in Chicago, describing a ransomware attack that temporarily crippled his legal practice in 2016.

A malicious link clicked or a file attachment arriving by email can unleash ransomware on networked computers or mobile phones. It can take down healthcare providers and threaten the aviation industry. Estimates of how many people and companies are affected by ransomware vary, but it's a big crime business. Software to unleash an attack can be easily bought and customized. Network security company SonicWall counted more than 200 million attacks globally in 2018. Cisco estimates that every 40 seconds a business falls victim.

In recent years, international law enforcement and security firms have collaborated on The No

More Ransom Initiative to freely share decryption tools. This has helped people worldwide. Creating frequent backups of files and keeping operating system software updated is the best fix to keeping your own devices healthy and free of malware that can infect others too.

Secrecy clouds what we know about the economic impact of ransomware. A 2018 study about ransomware payments via Bitcoin offers a glimpse of how many people fall prey, and suggests a new counting method to better estimate the millions of dollars of payments.

## Further reading:

The No More Ransom Initiative

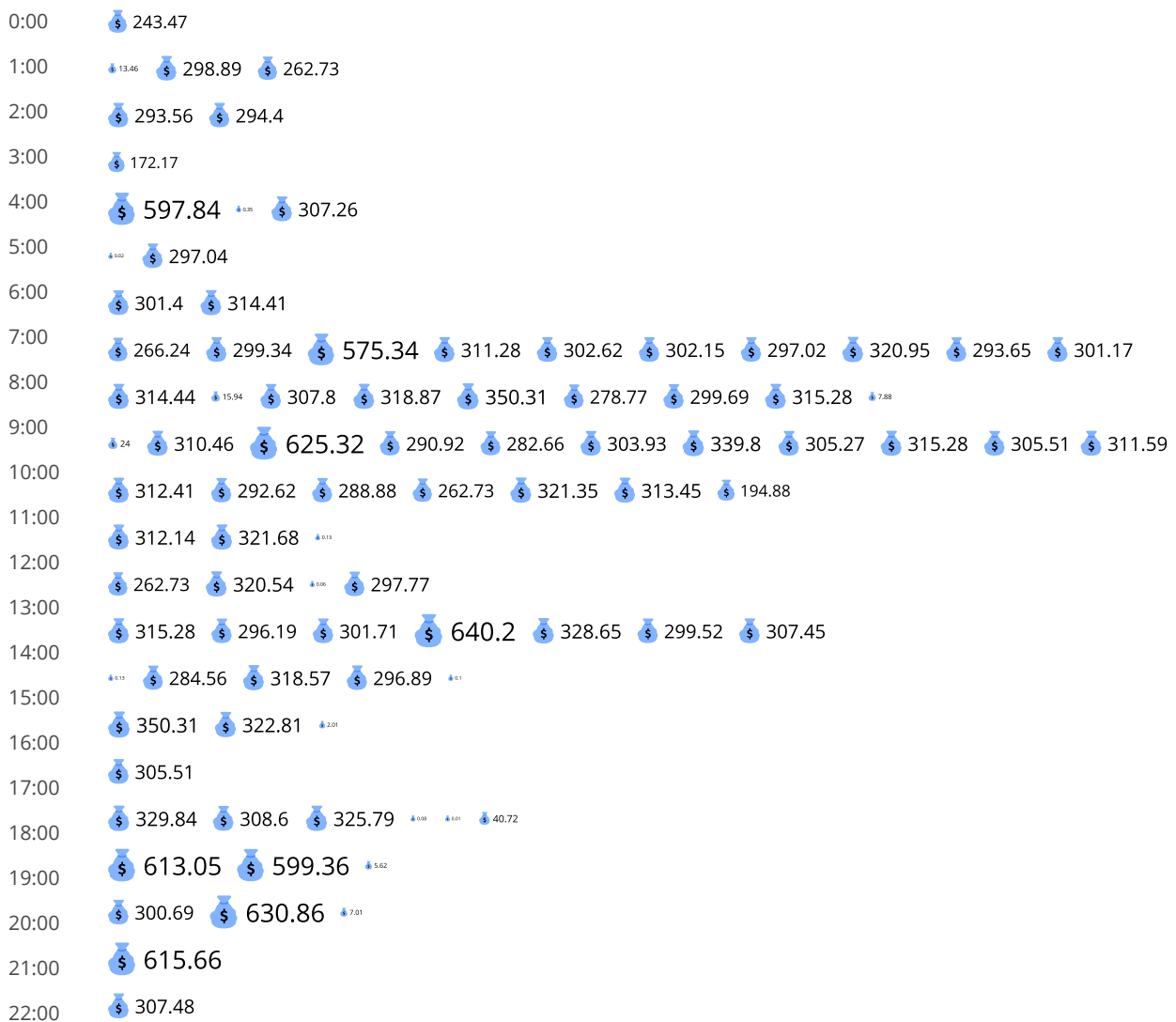
On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective; Mauro Conti, Ankit Gangwal and Sushmita Ruj, 2018

With Ransomware, It's Pay and Embolden Perpetrators, or Lose Precious Data, The New York Times, May 2017

# One day of WannaCry ransom payments

On May 15, 2017 the equivalent of \$24,246.51 USD in ransom payments were transferred to WannaCry ransomware attackers. In few days, an estimated 300,000 businesses in 150 countries were hit. There are still new WannaCry victims today.

Hour of the day      Sum of ransom payments  
**23:59      \$24246.51 USD**



On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective by Mauro Conti, Ankit Gangwal and Sushmita Ruj. In: arXiv:1804.01341 [cs], 2018. Data provided by Ankit Gangwal. Bitcoin values in USD were calculated according to May 15, 2017 rates

# In defense of anonymity

When bad things happen over the internet, anonymity often gets the blame.

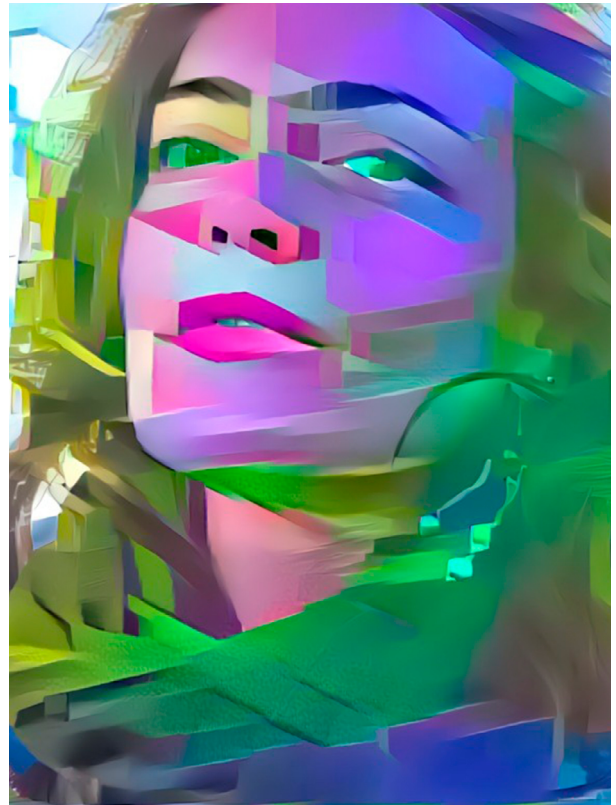
It may seem logical to think that if we could identify each and every person online, we could prevent crime. In every part of the world, there are authorities who argue that encryption should be banned or that anonymous sites should be eradicated. The reality is that anonymity often protects victims of crime, in a wide range of areas, from human rights, to banking security, military defense, or personal safety from stalking and domestic violence.

Constant surveillance facilitated by digital technology, whether by corporations or governments, is harmful to society and chilling to civil liberties. Our ability to communicate, work, and learn on the internet free from the glare of others enables very good things to happen.

Being untraceable on the internet takes effort. For that, Tor is one of the most important anonymity and censorship circumvention tools. An estimated 2 million daily users use it to hide the origin and destination of internet traffic as they browse the Web and communicate around the world.

In the context of concerns over terror and crime on the internet, Tor is often vilified. In the daily position of defending anonymity is Stephanie Ann Whited, the communications director of the Tor Project.

Q: What are questions you get from journalists that frustrate you?



Stephanie A. Whited, 2019 (CC-BY-SA 4.0).

A: It's frustrating to be asked questions based on the misunderstanding that Tor "is the dark web."

Tor onion services can be used to publish and share information online with a high degree of privacy and security without being indexed by search engines. You can't just visit them in any browser. Calling this "the dark web" and assuming everything published anonymously

online is bad, is a huge disservice to an under-appreciated technology that saves lives.

With onion services, women can share and access women's health resources in countries where it is outlawed. Activists can organize with less fear of surveillance when there may be life or death consequences. Whistleblowers reporting corruption can communicate securely. Onion services have also been used to create a more secure way to access popular sites like The New York Times, Facebook, or ProPublica. They all have .onion addresses.

Q: What makes your work feel most meaningful?

A: Internet freedom is in decline around the world, and being part of a force for good that allows people to have private access to the open Web is hugely important to me. Millions of people around the world rely on Tor Browser and onion services for private and secure communication in their day-to-day lives.

Some people rightly just want to limit the amount of data big corporations and advertisers can collect about them. For others, Tor is a vital tool against government oppression.

During protests in Sudan this year, when social media was blocked, Tor Browser usage spiked. It's also actively used in Uganda where a tax on social media was introduced.

Q: When you hear about the serious crimes that really do happen on onion sites (the so-called "darknet") does it make you doubt your sense of purpose?

A: It can be upsetting to hear Tor was used in a serious crime, but it doesn't make me doubt the software or the good that is only possible with anonymity tools like Tor. The reality is that

criminal activity exists on all kinds of sites, whether they were configured using onion services or not. Getting rid of Tor, or even getting rid of the internet, wouldn't make crime go away.

Q: Has press coverage about Tor changed over time?

A: Yes, and I think it's because we've improved the consistency and frequency of our communications and made Tor more user-friendly. Also, a lot more people are coming to understand how their daily online activities are exploited by tech giants. Even when other browsers offer more privacy protections than they used to, the full benefits of Tor Browser are unmatched. The press is beginning to highlight that more often without caveats.

Q: What are exciting things that are happening in the world of Tor?

A: Tor is more user-friendly and faster than ever. A decentralized network of over 7,000 volunteer-run servers around the world make up the backbone of our software, and we just surpassed over 40 GiB/s total bandwidth thanks to our community of volunteer relay operators.

The release of our first official mobile browser, Tor Browser for Android in 2018, is enabling us to reach more people in the parts of the world that need Tor most.

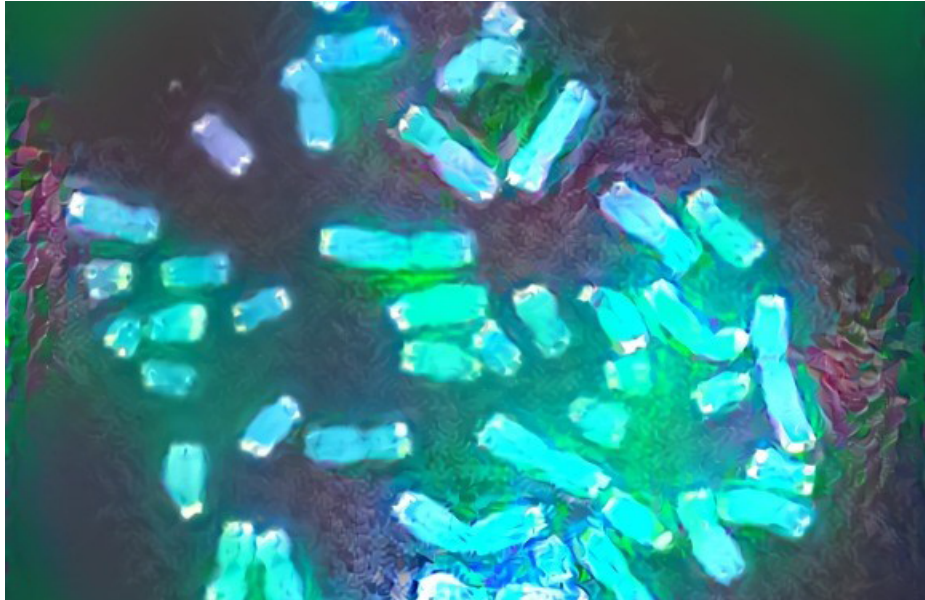
#### **Further reading:**

[Tor Metrics](#)

"Tor is easier than ever. Time to give it a try", WIRED, January 2019

"If anonymity isn't the problem, what is?", Internet Health Report, 2018

# 23 reasons not to reveal your DNA



Karyotype. Photo by Can H. (CC BY-NC 2.0).

DNA testing is a booming global business enabled by the internet. Millions of people have sent samples of their saliva to commercial labs in hopes of learning something new about their personal health or heritage, primarily in the United States and Europe. In some places, commercial tests are banned. In France, you could face a fine of around \$4,000 USD for taking one.

Industry giants Ancestry.com, 23andMe, MyHeritage and FamilyTreeDNA market their services online, share test results on websites, and even offer tutorials on how to search for relatives in phone directories, or share results in social media. They often also claim rights to your genetic data and sell access to their databases to big pharmaceutical and medtech companies.

In terms of internet health, it's part of a worrying trend of corporations to acquire personal data about people and act in their own best interests, not yours. OK, so test results can also lead to important discoveries about your personal health, and can also be shared for non-profit biomedical research in the public interest. But before you give in to your curiosity,



here are 23 reasons not to reveal your DNA – one for each pair of the chromosomes in a human cell.

1. **The results may not be accurate.** Some outputs on personal health and nutrition have been discredited by scientists. One company, Orig3n, misidentified a Labrador Retriever dog's DNA sample as being human in 2018. As Arwa Mahdawi wrote after taking the test, "Nothing I learned was worth the price-tag and privacy risks involved."
2. **Heritage tests are less precise if you don't have European roots.** DNA is analyzed in comparison to samples already on file. Because more people of European descent have taken tests so far, assessments of where your ancestors lived are usually less detailed outside of Europe.
3. **Your DNA says nothing about your culture.** Genetic code can only tell you so much. As Sarah Zhang wrote in 2016, "DNA is not your culture and it certainly isn't guaranteed to tell you anything about the places, history and cultures that shaped you."
4. **Racists are weaponizing the results.** White nationalists have flocked to commercial DNA companies to vie for the highest race-purity points on extremist websites.
5. **DNA tests can't be anonymous.** You could jump through hoops to attempt to mask your name and location, but your DNA is an unique marker of your identity that could be mishandled no matter what.
6. **You will jeopardize the anonymity of family members.** By putting your own DNA in the hands of companies your (known or unknown) relatives could be identifiable to others, possibly against their wishes.
7. **You could become emotionally scarred.** You may discover things you weren't prepared to find out. A fertility watchdog in the United Kingdom called for DNA testing companies to warn consumers of the risks of uncovering traumatic family secrets or disease risks.
8. **Anonymous sperm and egg donors could become a thing of the past.** The likelihood that anonymous donations will remain anonymous decreases with every test taken, which could dissuade donors and negatively affect some families.
9. **Millions are spent on targeted ads to lure you.** DNA companies hand out free kits at sporting events, and create DNA specific music playlists on Spotify. In 2016 alone, Ancestry.com spent \$109 million on ads. An ad by AncestryDNA capitalized on "Brexit" and British identity politics, with the slogan, "The average British person's data is 60% European. We may be leaving Europe, but Europe will never leave us."
10. **A pair of socks is a better gift.** You may be tempted by special offers around holidays such as this one, offering 30% off genetic tests for Father's Day: "What do you share with Dad? This Father's Day, celebrate your DNA connection with Dad". Perhaps the man who has everything would prefer not to become your science experiment.
11. **You will become the product.** Your genetic code is valuable. Once you opt in to sharing, you have no idea what company gets access to it, nor for what purpose.
12. **Big pharma wants your DNA.** 23andMe revealed a \$300 million USD deal with pharmaceutical giant GlaxoSmithKline in 2018 that gives them access to aggregate

customer data. Calico Life Sciences, a med-tech company owned by Google's parent company, Alphabet, is the primary research partner of Ancestry.com.

13. **Companies can change their privacy policies.** You might be asked to give your consent again, but policies of companies can still change in ways you may not like.
14. **A company (and your DNA) can change hands.** Companies are bought, sold, go out of business or change their business models. And then what happens with your genetic info?
15. **Destructing your DNA can be difficult.** An investigation into how to delete your DNA from Ancestry.com found that it is possible to erase your record and allegedly even destroy your physical sample. But they don't make it easy.
16. **You have no idea how long they will keep your sample.** Some companies say they keep samples for 1-10 years. Regulations governing DNA databases differ from country to country. Do you know the rules where you live?
17. **Police can access your DNA.** There's crime solving potential, but also human rights risks. Authorities can seek court approval to access consumer DNA databases, but investigators have also been known to create fake profiles using a suspect's DNA.
18. **Your results could become part of a global database.** Law enforcement in several countries have unrestricted access to genetic profiles. Some scientists argue that creating a "universal genetic forensic database" would be the only way to make unwanted intrusion less likely through regulation.
19. **Your data could be hacked, leaked or breached.** Third party sharing is common practice among companies. The more people have access to your DNA, the more vulnerable it is to being hacked. As companies amass more data, they will become increasingly attractive to criminals and vulnerable to cyber theft.
20. **Genes can be hacked.** Scientists have discovered how to store data and even animated GIFs in DNA, and even believe malware could be placed in DNA to compromise the security of computers holding databases. Still trust them?
21. **You are signing away rights.** When you use services like AncestryDNA the default agreement is to let them transfer your genetic information to others, royalty-free, for product development, personalized product offers, research and more.
22. **Companies profit from your DNA.** Testing isn't the only way companies make money. They profit from data sharing agreements with research institutes and the pharmaceutical industry. If your DNA helps develop a cure for a disease, you'll never know. And you certainly won't earn royalties from any related drug sales.
23. **You may be discriminated against in the future.** In the United States, health insurers and workplaces are not allowed to discriminate based on DNA. But the law does not apply to life insurance or disability insurance. Who knows in your case, where you live? Some day you could be compelled to share genetic information with your own insurer.

If you still decide to submit your DNA for testing, the U.S. Federal Trade Commission offers sound advice to consumers: compare privacy policies

before you pick a company, choose your account options carefully, recognize the risks, and report any concerns to authorities. To counteract the dominance of commercial companies, you can also contribute your data to non-profit research repositories like [All of Us](#) or [DNA.Land](#) that are open to public scrutiny.

If you regret a choice you made in the past, you could have your DNA data deleted and request that your sample be destroyed. Consumer DNA testing is an example of why strong data protection laws are so important. In Europe, the [General Data Protection Regulation \(GDPR\)](#) offers some protections, but elsewhere you have few rights when you hand over sensitive data.

**Further reading:**

[How DNA Testing Botched My Family's Heritage, and Probably Yours, Too](#), Gizmodo, 2018

[Ancestry wants your spit, your DNA and your trust. Should you give them all three?](#), McClatchy, 2018

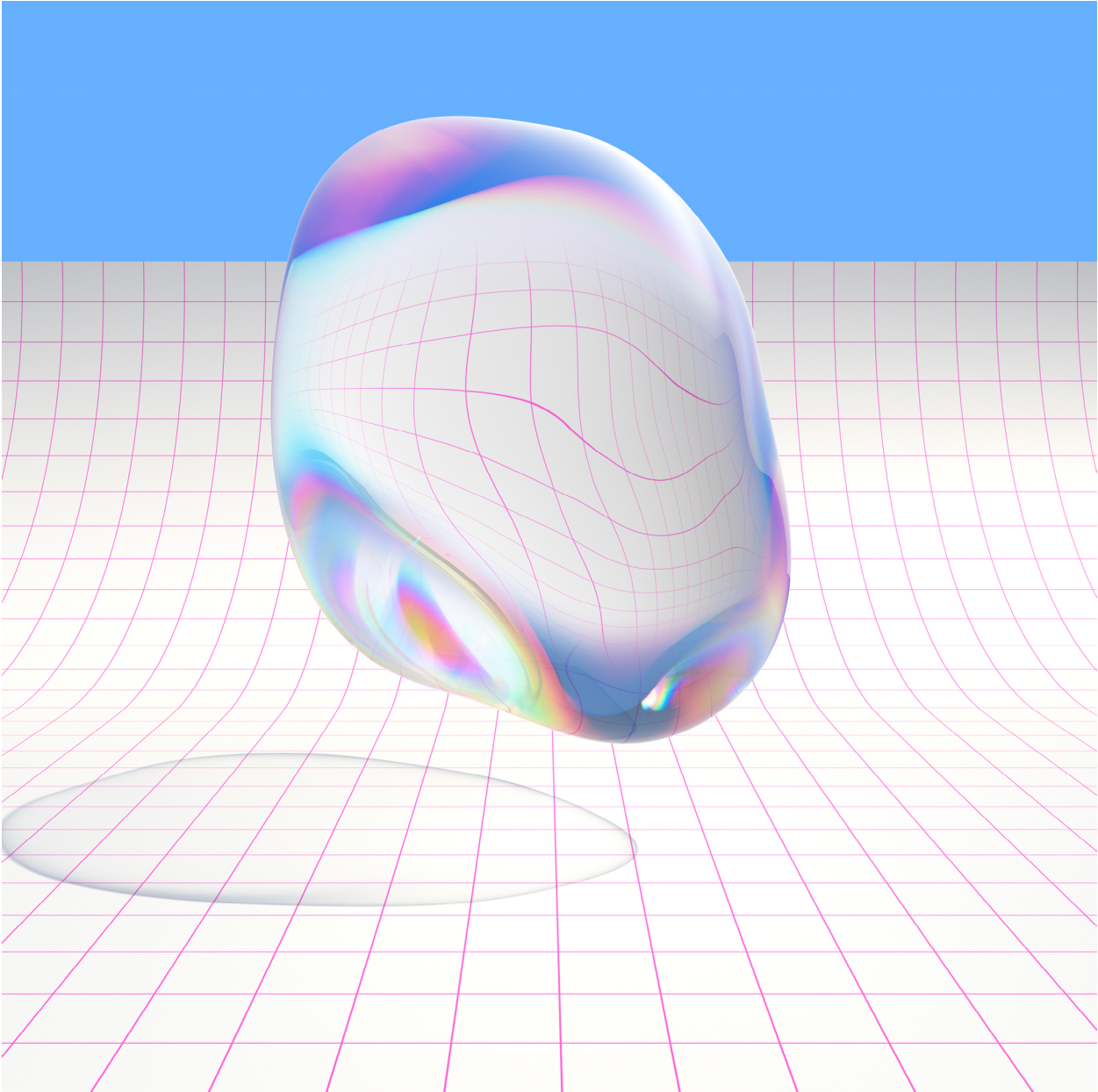
[The Forensic Genetics Policy Initiative](#) – Country Wiki

## Read more online

Coordinating complaints for data privacy in Europe

Your mobile apps are tracking you





Openness

Introduction

# How open is it?

The internet is transformative because it is open: everyone can participate and innovate. But openness is not guaranteed – it's always under attack.

Openness

Introduction

**moz://a** [internethealthreport.org/2019](https://internethealthreport.org/2019)

29

Openness is a foundational pillar of the internet. Today's digital world exists because people don't need permission to create for and on the Web.

Yet in 2019, the internet's openness is as radical — and as threatened — as ever.

Governments worldwide continue to restrict internet access in a multitude of ways, ranging from outright censorship to requiring payment of taxes to use social media, to shutting down or slowing down the internet to silence dissent. Powerful lobbyists are winning fights for more restrictive copyright regimes, and big tech platforms lock us in to proprietary systems

At the same time, the open Web is resilient.

Volunteers of the Wikidata community of Wikimedia have created a data structure that enables content to be read and edited by both humans and machines. Advocates of open data are pushing for more transparency to understand how companies create digital profiles of us and what they do with the data.

But a tension between openness and inclusion persists. Despite many measures taken, hate speech and harassment on online platforms remains an urgent and serious problem.

In Germany, one year after implementation, a law to reduce hate speech online, was neither particularly effective at solving what it set out to do, nor as restrictive as many feared.

Yet the lack of strong evidence isn't stopping similar regulations from being introduced elsewhere. The European Union is currently debating new rules that would require companies of all sizes to take down 'terrorist content' within one hour, or face stiff penalties.

Opponents warn that the law risks undermining people's fundamental rights and stifling competition by setting a bar only the largest companies can meet.

Heightened discussions about artificial intelligence and automated decision making (AI) are also introducing new angles to this debate.

New user-friendly AI tools have made it easier than ever to create deepfakes: media that depict a person saying or doing something they never did. These sort of developments raise a critical question: how do we mitigate the real harms that misuse of a technology could cause, particularly to vulnerable groups, without sacrificing the benefits of the open internet?

Sometimes, the best approach might be to never release it.

OpenAI recently built a language model so good at automatically generating convincing text that they became concerned about it being misused. To mitigate potential harm, the organization decided to release a limited version of the tool. The choice sparked criticism that it was the "opposite of open," while others praised the decision as a "new bar for ethics."

Grappling with the challenge of safeguarding the open internet, while building an inclusive digital world, remains a pivotal task for companies, technologists, policy makers and citizens alike.

This is especially true as a new dimension emerges, centered around an urgent question: how do we decide what technologies to build and use at all?

# Show me my data, and I'll tell you who I am

“Stop manipulating us, and give us real choices,” says Katarzyna Szymielewicz, a technology and human rights expert, lawyer and activist who advocates for people to have more control over how their data is processed and used.

Companies are building digital profiles of us, made up of data collected by thousands of trackers in mobile apps or on the web. They gather information about us practically whenever we are connected to the internet. Data brokers sell this data to whoever is willing to pay the price. It changes hands between countless companies without our knowledge.

Data about us is sorted into categories we often can't see and analyzed by algorithms we often don't know about – and then used to make decisions that could impact our lives, for better or worse.

But what if we could take guessing out of the equation, and just *tell* companies who we are? Would they respect our answers?

Katarzyna Szymielewicz is the co-founder and president of Panoptykon Foundation, a digital rights organization in Poland. In January 2019, Panoptykon filed a complaint against Google under new the European General Data Protection Regulation, alleging the company had violated the regulation's requirements to provide users with access to data held about them.

To help a broader audience visualize how little we're currently able to control our digital profiles, Szymielewicz has developed a metaphor of “three layers” of data: providing examples of what is collected about us, what is observed and what is generated by machines.

Q: Are our data profiles inaccurate?

A: Who knows? Without transparency and access to the full profiles that are generated for us by tech companies we cannot really tell. I am sure users themselves would be the best auditors of these datasets because they have real (often economic) incentives not to be judged on the basis of incorrect or incomplete information. But they are not given the chance to do so.

I came up with this layered metaphor to explain the complexity (and dangers) of how online data profiles work after hearing for the hundredth time: ‘What's the problem if we choose to share and publish our data ourselves?’ The thing is that we do not make these choices ourselves. We are lured into sharing more data than we would accept, observed and qualified by machines in ways we can hardly imagine. Not

surprisingly, they detect sensitive characteristics we may prefer to keep private.

Q: Why should we want to see our data?

A: The only way to regain full control over our profiles, is to convince the companies who do the profiling to change their approach. Instead of hiding our data from us, they should become more transparent. We need to open these opaque systems to the scrutiny of users.

On the other hand – instead of guessing our location, relationships, or hidden desires behind our backs, I think companies could simply start asking us questions, and respecting our answers. I even see this as a real opportunity for marketing companies to build trust and make targeted ads more relevant and fair.

In the European Union, we have a legal framework that facilitates greater openness and access. The General Data Protection Regulation (GDPR) now gives Europeans the right to verify data held by individual companies, including marketing and advertising profiles. Companies can still protect their code and algorithms as business secrets, but in theory they can no longer hide personal data they generate about their users. I say in theory – because in practice companies don't reveal the full picture when confronted with this legal obligation. In particular, they hide behavioural observation data and data generated with proprietary algorithms. This must change, and I am sure it will, once we begin to see the first legal complaints result in fines.

Q: How could we make radical transparency a reality?

A: Well, no doubt we have to be prepared for a long march. We need to work together as a movement and test different approaches. Some of us will continue to test legal tools and fight

opponents in courts or in front of Data Protection Authorities. Others will advocate for (still) better legal safeguards, for example in the upcoming European ePrivacy Regulation. Others will build or crowdfund alternative services or push big tech to test new business models, and so on. I am sure it will be a long run, but as a movement, we are at least heading in the right direction. The main challenge for us now is to convince or compel commercial actors to come along.

### Further reading

Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Wolfie Christl and Sarah Spiekermann, 2016

Data Ethics – the new competitive advantage, Gry Hasselbalch and Pernille Tranberg, 2016

The Age of Surveillance Capitalism by Shoshana Zuboff review – we are the pawns, The Guardian, 2019

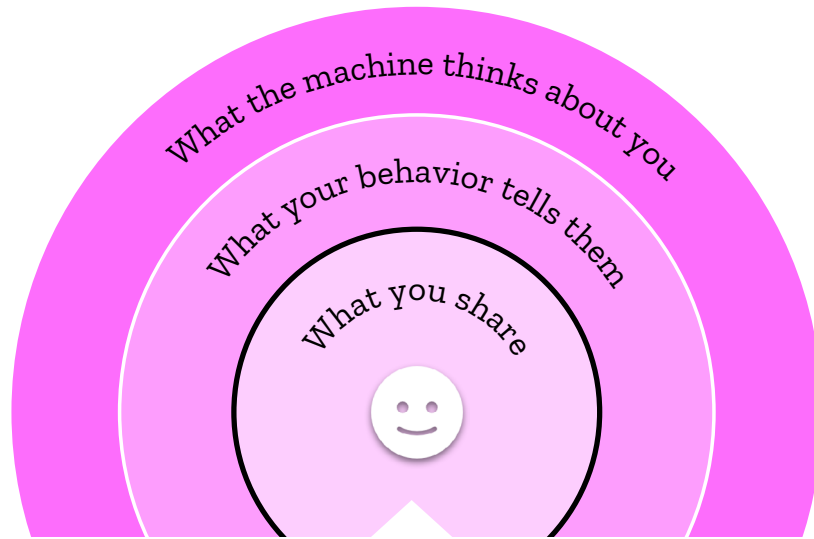
Your digital identity has three layers and you can protect only one of them, Quartz, 2019

### Further listening

All Your Data Are Belong to Us, IRL podcast, S.1 E.1, 2017



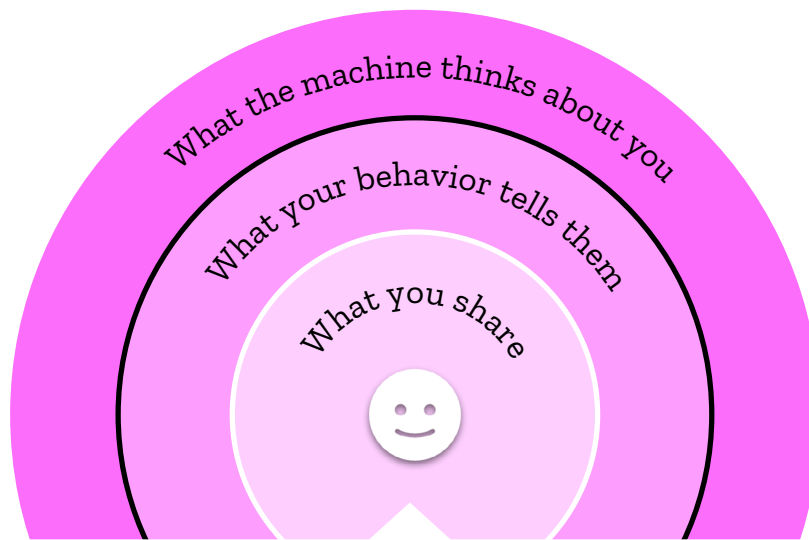
# Three layers of our digital profile



## What you share

The first layer is information we actively feed into social media and mobile applications. We can control this data ourselves if we choose not to share specific information: not to publish certain updates, not to upload photos, avoid sensitive search queries, and so on.

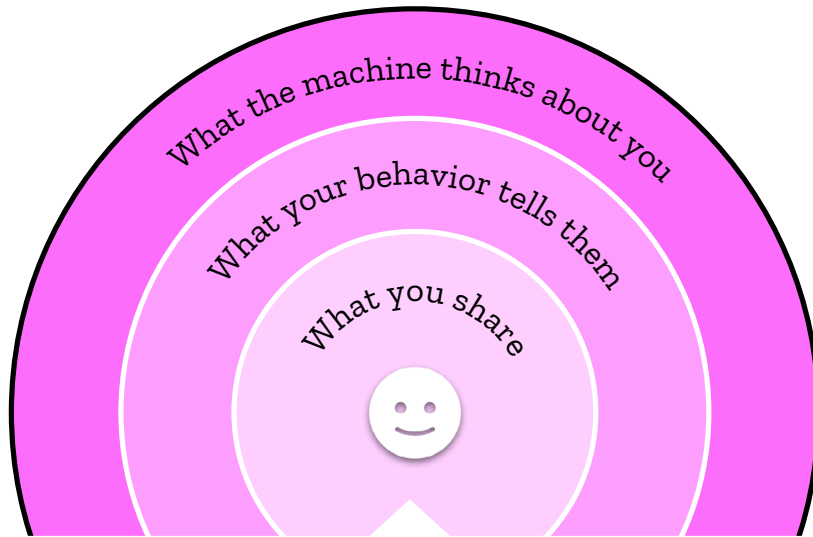
- user name
- real name
- gender
- friends
- groups entered
- blocked contacts
- likes & other reactions
- search terms
- uploaded photos
- fingerprints



## What your behaviour tells them

The second layer is our behavioral data and 'metadata' logged by our devices. For example our current location or who we communicate with. It is possible to control this layer of our digital profile to some extent, but it requires real effort and technical expertise.

- visited websites
- keystroke dynamics (incl. misspelling and typos)
- ads clicked
- ignored content
- device location (GPS)
- articles/posts clicked
- time stamp of any online activity
- number of interactions/posts per day
- shopping patterns (routine)
- typing speed



## What the machine thinks about you

The third layer is interpretations of the data collected in the first and second layers by algorithms that learn who we are based on behaviors and statistical correlations. It is virtually impossible to control. Full access to data generated by algorithms is often not made available to users.

- ethnic affinity
- expecting a baby/pregnant
- professional relationships
- religious views
- political affiliations
- psychometric profile
- high/low esteem
- IQ level
- mental illness
- gambling

Three layers of our digital profile by Katarzyna Szymielewicz, Marcin Antas, Kamil Śliwowski, 2019. Data used in this visualization is based on Panoptykon's research and it is meant as data samples that aren't exhaustive or applicable to every person.

# Taxing social media in Africa



Photo by George Pagan III on Unsplash.

## How much would you pay your government for a day's worth of WhatsApp messaging?

One after another, the governments of three countries in Africa, Uganda, Zambia and Benin have announced or imposed new taxes on mobile internet customers in 2018, leaving millions of Africans struggling to cover the costs of getting online. Only in Benin did protests result in quick abandonment of the tax plan.

Governments have imposed these levies to raise public revenues, and also argue that they are protecting the local telecommunications sector from competition from internet companies from abroad. But in practice, the (intended or unintended) consequence has been to push more people offline, increase barriers to getting online, and vastly limit freedom of expression

and access to information — as well as access to goods and services that are now online.

Uganda imposed the first of these tax schemes in July 2018, forcing residents to pay a daily tax of 200 shillings (\$0.053 USD) to use any one of 58 “over the top” (OTT) mobile communication apps. These include — but are not limited to — social media services like Facebook, Twitter, Instagram, and LinkedIn; instant messaging and voice communication apps WhatsApp, Snapchat, Skype; and dating sites like Tinder and Grindr.

The law in Uganda also placed a 1% tax on the use of mobile money, which is now the required method for airtime top up of SIM cards. With

the average Ugandan already spending 15% of their monthly income for 1GB of broadband data, the new tax puts popular internet services out of reach for most people.

This is not just a matter of chatting with friends. As anyone in the region knows, WhatsApp in particular has become an essential platform for communication and information-sharing in Africa. Millions of people rely on WhatsApp groups to conduct business, communicate about local issues, read the news, and seek help in emergencies.

For many Ugandans, social media like Facebook and WhatsApp are a gateway to the rest of the internet. In an opinion piece for Global Voices, Ugandan blogger Pru Nyamishana wrote:

“The tax ignores a critical lack of digital literacy, particularly among poor Ugandans. When I interviewed women living in Bwaise, a slum in Kampala, I learned that for them, WhatsApp and Facebook are the internet. These are the only platforms they know how to use. So with the new tax, they will be cut off altogether.”

After the tax had been in effect for six months, the Uganda Communications Commission reported national internet usage rates had dropped by from 47.4% to just 35%.

On the heels of Uganda’s initiative, Benin approved a similar tax in September 2018, targeting mobile messaging and ‘Voice over IP’ calls (like Skype). It drove up the cost of a single gigabyte of data by nearly 250% but was repealed just days later, in the face of public protests.

The Zambian government announced a flat daily tax of 30 ngwees (US \$0.03) on IP-based voice calls in August. Despite pushback from civil society and Zambia’s Chamber of Commerce and Industry, government officials went ahead

with the tax, arguing that it would raise public revenues, bolster local telecommunications enterprises, and help cover the cost of investments in infrastructure.

“Jobs such as call centre workers, talk time sellers, conventional call technicians will reduce drastically if more Zambians migrate to internet calls and create jobs in America and elsewhere,” tweeted Dora Siliya, Zambia’s Minister of Information and Broadcasting Services.

Although this reasoning rang hollow for many internet users, Siliya’s argument is consistent with longstanding frustrations on the continent about foreign-owned OTT services that have captured markets for messaging and voice calls, changing the game for national telecom operators.

Countries in Africa are not alone in resenting how the data and advertising-driven business models of big tech bring few immediate benefits to local economies, while enriching technology companies in the United States. Google and Facebook are increasingly now also in the infrastructure game which will affect the power balance with telcos even further. Popular OTT services have helped fuel the uptake of mobile internet, and enabled local businesses to operate more efficiently. Still, they also create dependencies that can negatively affect the local digital economy, especially when technical or commercial priorities change far away.

In a region where governments are known for restricting free speech through censorship, internet shutdowns, surveillance and legal threats, civil society and independent media also view OTT tax schemes as an attack on free speech. In two other cases, this is clearly warranted.

In Tanzania, a so-called “blogger tax” was introduced in April 2018 alongside new restrictions

for online content, in a clear effort to limit online expression. It requires Tanzanian bloggers, YouTube channel operators, and independent website owners to register and pay roughly \$900 USD per year to publish online.

In August, the Mozambican government decreed that individual journalists and media outlets using both traditional and digital platforms now have to register and pay between \$500 to \$3,300 USD for an accreditation license that must be renewed every five years.

Taxes like these propagate the misconception that internet access and social media use are luxuries. But their outcomes — like the drop in internet use in Uganda — offer a compelling case study on the importance of establishing [protections for net neutrality](#). What citizens have emphasized in protests, and what local researchers have also [demonstrated](#), is that access to a truly open internet is a boon for local economies, education, public health and life in general.

### **Further reading**

[Offline and Out of Pocket: The Impact of the Social Media Tax in Uganda on Access, Usage, Income and Productivity](#), Pollicy, 2019

[Taxed, throttled or thrown in jail: Africa's new internet paradigm](#), Global Voices, 2019

[Eastern Africa: New tax and licensing rules for social media threaten freedom of expression](#) ARTICLE 19, 2018

[Challenges and opportunities for advancing internet access in developing countries while upholding net neutrality](#), Nanjira Sambuli, 2016

## Read more online

Internet slowdowns are  
the new shutdowns



Tracking China's censorship  
of news on wechat

Inside Germany's crackdown  
on hate speech



Deepfakes are here,  
now what





Digital Inclusion

Introduction

# Who is welcome online?

It's not just about how many people have access to the internet, but whether that access is safe and meaningful for all of us.



A critical question for internet health remains: how do we create a truly inclusive digital world?

The tech industry itself is grappling with this challenge and its responsibility — increasingly in public settings. Many tech companies have faced high-profile accusations that their services are facilitating harmful discrimination and profiling. The last year saw a wave of protests led by employees of tech giants, many of which called on companies to cancel contracts some staff viewed as unethical. Amazon staff and A.I. experts called on the company to stop selling biased and flawed facial recognition software to law enforcement agencies. A letter signed by over 100 Microsoft employees demanded the company “take an ethical stand” and cancel its contract with U.S. Immigrations and Customs Enforcement. So far, these demands have not been met.

It’s hard to imagine a truly inclusive digital world when the companies building so much of the infrastructure have a bad track record for being inclusive themselves. There’s been some progress: when more than 20,000 Google employees walked out over the company’s mishandling of sexual misconduct cases, some demands were met not only by Google, but also by Facebook, eBay and Airbnb. Still, companies did not make all the changes protesters wanted and there remains much more to do to make the tech industry a safe, welcoming space.

While the mainstream focus tends to center on Silicon Valley, many serious harms are happening elsewhere around the world. Factory workers in China, Malaysia, Brazil and other countries make cell phones, smart watches and hardware in grueling and often dangerous conditions, for meager pay. Major platforms like Facebook and Twitter outsource content moderation to low-wage workers, many of whom experience symptoms of trauma after viewing

thousands of disturbing and violent images every day.

Tech workers organizing and standing up for inclusion within their companies is a positive development for internet health. But it hardly compares to threats to digital inclusion more broadly. Online abusers threaten and intimidate in an effort to silence the voices of especially women, nonbinary people, and people of color. Nearly two-thirds of female journalists say they have been harassed online. Better solutions to solve hate speech are still wanting.

But there’s also good news: codes of conduct, which have long been valued as critical tools for empowerment by underrepresented people in open source, are increasingly being integrated into open source projects. One particular Code of Conduct, called The Contributor Covenant, was adopted by thousands of open source projects in just five years.

Access also remains a fundamental challenge for inclusion. We’re right to celebrate that over half of the world is now online. But the connectivity gap between the richest and poorest countries has not improved in the last decade. The slowest internet in the world is also the most expensive and there are still far fewer women online than men.

It’s clear that equality won’t be achieved by accident. If we want to create a digital world that is welcoming of all people of the Earth, we still have much to do.

# More than half of the world is online, but...

It's cause for celebration that more than half of the world is now using the internet, but the difference in connectivity rates between the richest and poorest countries has remained nearly the same for a decade, and overall growth rates have slowed.

Global averages can hide that only some world regions have connected more than 50% of their population. Europe reached 50% eleven years before the rest of the world, and has now reached nearly 80%. Meanwhile only 24% of people in Africa use the internet.

To really understand the weight of this inequality, consider that more than 80% of the world's population lives in developing countries. If there were only 100 people living in the world, almost 56 of them would be living in the Asia & Pacific region where the world's most populous countries, China and India, are. Only 26 would have internet access.

In Europe, 7 out of 9 people would be using the internet. And in Africa, less than 4 out of 13 would be online.

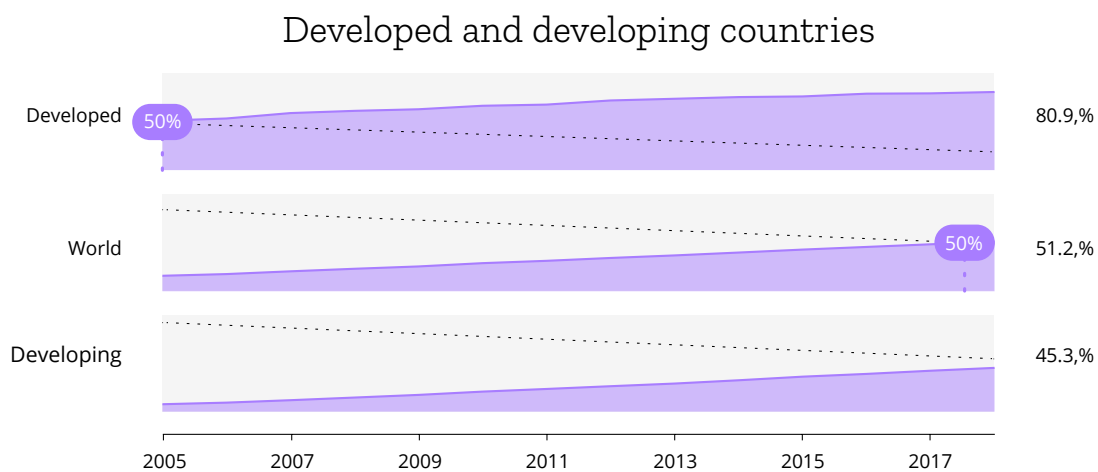
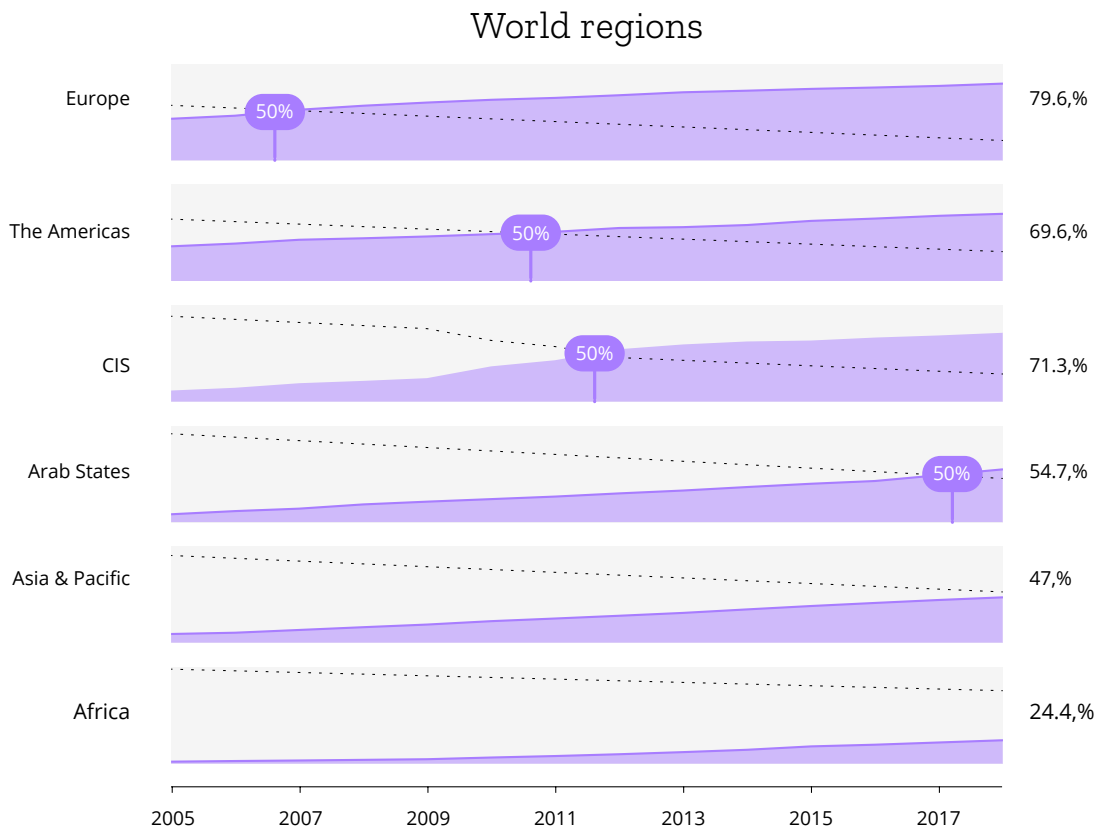
## Further reading:

"New ITU statistics show more than half the world is now using the Internet", International Telecommunications Union, 2018

The Case for the Web, The World Wide Web Foundation, 2018

The Mobile Economy, GSMA, 2019

# Which world regions have more than 50% of people online?



## How to read this chart

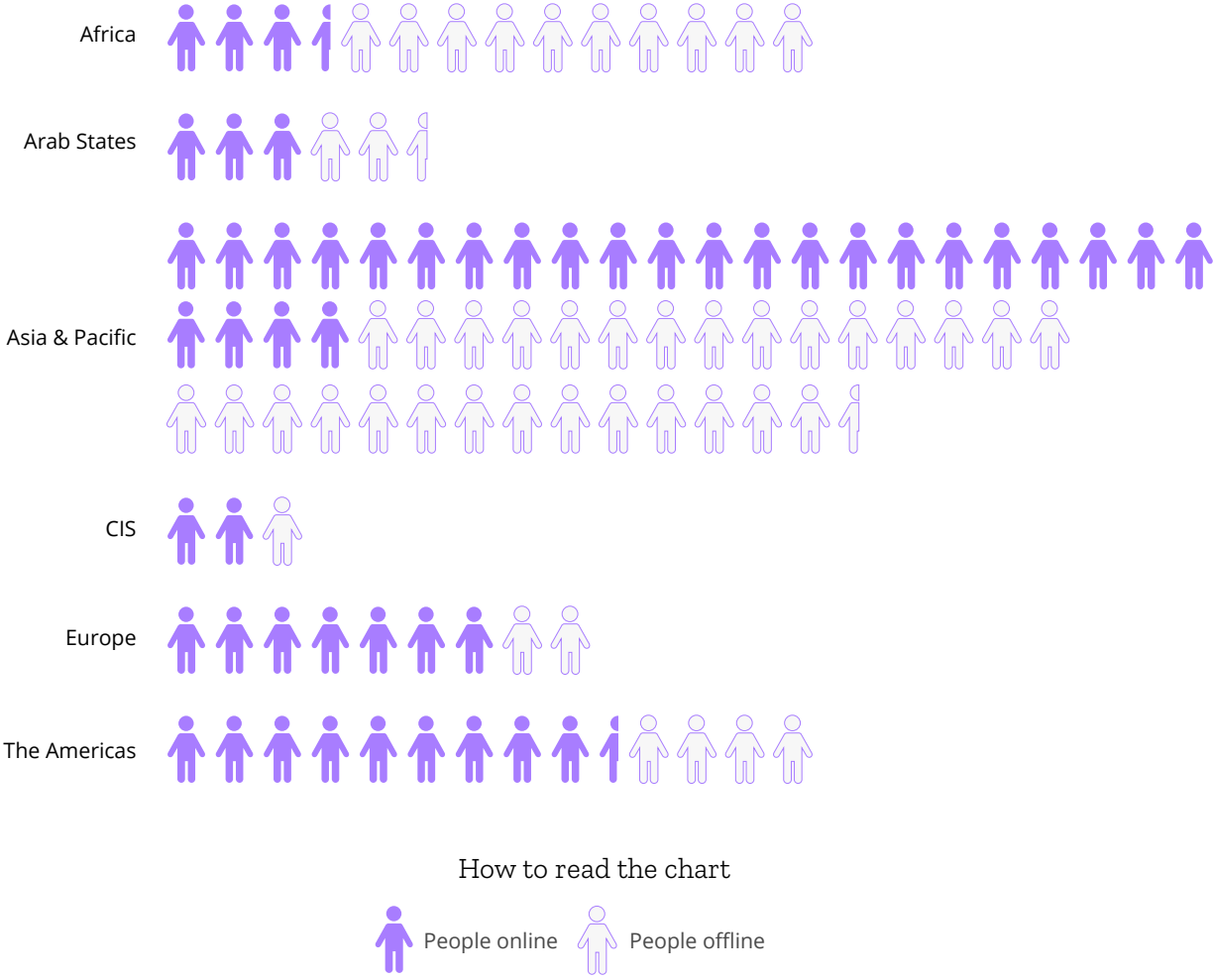
● Percentage of people online    ● Percentage of people offline

Key ICT indicators for developed and developing countries and the world,  
International Telecommunications Union (ITU), 2018

Inequalities don't just stop at access. The least connected regions also contend with the least dependable and slowest internet at the least affordable prices. Moreover, women are disconnected to a higher degree than men, worsening the effects of gender inequality.

Universal and affordable internet for all is one key aspiration of the United Nations Sustainable Development Goals, because unless the internet is accessible, other development factors lag behind, including education, health, and free speech. Overcoming digital divides requires long-term planning and commitments on the part of governments, the private sector and civil society.

# If there were only 100 people in the world, here's who would be online



Combined data from Key ICT indicators for developed and developing countries and the world, International Telecommunications Union (ITU), 2018 and World Population Prospects 2017, United Nations DESA/Population Division, 2017. Icons: "people" by asianson.design on NounProject (CC-BY)

# Codes of Conduct now guide open source communities

Open source software communities have a noble intention: to work together over the internet to create something that benefits everyone. But hostility and bias often flourish in communities where there are no consequences for contributors who display non-inclusive behavior.

Toxic cultures have discouraged many talented developers from contributing necessary improvements to even the most important projects for the Web.

It's a contributing factor to the reality that only 3% of open source contributors are women and that the majority are male and white. For the health of the internet, such lack of diversity is grim. Open source is everywhere now, so it means a very homogeneous group of people is responsible for software the entire world interacts with every day.

In the fight for inclusivity and healthier communities, Codes of Conduct have surfaced as one of the most important (and sometimes controversial) instruments for change. They are valued especially by underrepresented groups in open source, including women, as a tool of empowerment for calling out bad behavior.

Today, Apache, Google, Microsoft, Mozilla and WordPress all have Codes of Conduct for their



Stephanie A. Whited, 2019 (CC-BY-SA 4.0).

open source projects. One established community after another, including those with founders who have controversial communication styles, like [Linus Torvalds of Linux](#), have had to reckon with community members who called for a full stop on rude and aggressive interactions.

“Codes of conduct are vital to open source communities,” explains [Coraline Ada Ehmke](#), a developer and open source-advocate who created the [Contributor Covenant](#), a Code of Conduct text adopted by [thousands of open source projects](#) in just five years.

“A Code of Conduct is a way of expressing community values,” she says.

A core value could be to foster an open and welcoming environment for everyone: “regardless of age, body size, disability, ethnicity, sex characteristics, gender identity and expression, level of experience, education, socioeconomic status, nationality, personal appearance, race, religion, or sexual identity and orientation,” as it says in the Contributor Covenant.

That may not seem controversial. But time and again, some contributors find it unsettling or even infuriating when new rules and processes are introduced to govern language and behaviors they are used to, and may not believe are harmful.

“There are best practices for how to write documentation, or share an idea with a group of potential strangers, in a way not likely to cause offense,” explains [Jory Burson](#), a consultant and educator who helps open source communities build healthy cultures.

Emma Irwin, an open project and communities specialist at Mozilla, says a Code of Conduct is toothless unless it is actually enforced. “Trust comes from enforcement. Stability comes with

enforcement. If you have a Code of Conduct and don’t enforce it, you can actually cause more harm,” she says.

The boundaries of such enforcement are still being tried and tested, as open source communities wrestle with how to create the best conditions for equality and diversity. For instance, should an expulsion from one community [lead to expulsion from another?](#)

Codes of Conduct were initially only introduced at open source conferences and public events to stem disagreements that veered from technical to personal matters.

In 2014, after signing a pledge to only attend conferences with Codes of Conduct, Coraline Ada Ehmke began contemplating a similar approach to online communities.

“I started thinking of ways that we could advance the cause of inclusivity in the wider tech community,” Ehmke recalls. “Since I have a long history of working in open source, it seemed logical to me that these communities of maintainers and contributors also needed a social contract to express and enforce community values of improving diversity and being welcoming to people of all kinds, especially those who are traditionally underrepresented in tech.”

“So the Contributor Covenant was born,” Ehmke says.

“In the last seven to eight years, the practice has shifted from needing the Code of Conduct for events, to needing it for the digital space,” Burson says. “It’s a very good progression.”

**Further reading:**

The Woman Bringing Civility to Open Source Projects, WIRED, 2018

Open source is only ajar without inclusion, Emma Irwin, Internet Citizen (Mozilla), March 2019

Now Intel signs up to open-source code of conduct after Torvalds' Linux hiatus, ZDNet, 2018

Your Code of Conduct, Open Source Guides, Github

# Technology's inhumane underbelly



Amazon supplier factory, Hengyang Foxconn. Photo by China Labor Watch. (CC BY-SA 4.0)

In the U.S.'s Silicon Valley or South Korea's Pangyo Techno Valley, working in tech is often a lucrative job. Writing code and designing new products can yield a sizeable paycheck, stable employment and company perks like free meals.

But not everybody in the technology supply chain is so fortunate. For workers in manufacturing — who build iPhones, smart watches and other hardware, at factories in China, Malaysia, Brazil and other countries — jobs can be grueling and inhumane.

Li Qiang is the executive director of [China Labor Watch](#) (CLW), a New York City-based organization whose goal is to improve working conditions for Chinese workers. The nonprofit carries out undercover factory investigations in China,

documents poor conditions and pressures companies to improve. Over 19 years, CLW has investigated factories that produce hardware for Apple, Dell, Microsoft, Samsung, Huawei and other major companies.

CLW has uncovered child labor, discrimination, mandatory overtime rules, and human rights violations. Recent reports include "[Amazon Profits from Secretly Oppressing its Supplier's Workers](#)" (June 2018) and "[Apple's Failed CSR Audit](#)" (January 2018).



Amazon responded to CLW's findings by telling press they had "immediately requested a corrective action plan from Foxconn," the company running the factory that produces Amazon Echo and Kindle. Apple told reporters it investigated the CLW claims, but "found no standards breached."

"What these companies are looking for are cheaper production costs," Li Qiang explains. "They don't actually put a lot of care into the working conditions."

Factory workers in China frequently do not earn a living wage. They may make the region's legal minimum wage, but Li Qiang says that is still not enough to sustain them. As a result, overtime becomes necessary, and 60-hour weeks — or longer — become the norm.

Further, many workers don't receive proper safety training. "Workers come into contact with toxic chemicals and do not even know about it," Li Qiang says.

Who is to blame for these poor conditions? Li Qiang says there is a lot of finger pointing: "Companies like Apple and Dell push responsibility for these terrible working conditions onto factories," he explains. "And the factories push the responsibility onto the agencies that hire the workers."

Poor working conditions in Chinese factories are hardly a secret. In 2010, a rash of suicides at the Foxconn Technology factories in Shenzhen dominated news headlines. In 2015, WIRED published an exposé that followed a teenager in Dongguan who worked 15-hour days in a factory, used a toxic chemical to clean phone screens, and watched her colleagues grow sick.

Li Qiang acknowledges that working conditions have improved in the last 20 years. Among the achievements is that tech companies now

address some problems: Apple issues progress reports on the labor and human rights law compliance of suppliers. Dell's corporate social responsibility work includes initiatives to improve work standards in the supply chain.

But wages are still far too low, Li Qiang says. And too few organizations monitor companies and advocate for change. Among allies of CLW, are around 100 organizations that belong to the GoodElectronics network. It's a nonprofit coalition in The Netherlands that rallies unions, researchers and academics to defend human rights and environmental sustainability in the global electronics supply chain. Traditional labor organizations also research and advise on best corporate practices, including the International Labor Organization of the United Nations.

The health of the internet includes humane working conditions for the people who build the phones, computers and other devices we depend on for connectivity. Cheap consumer technology can come at a high cost — for someone else. With more transparency and accountability from companies, and stronger protections for worker's rights and safety, we could feel better assured about what degree of respect technology companies hold for humanity. As we invite more tech products into our lives, that's something that ultimately affects us all.

**Further reading:**

[GoodElectronics network](#)

[China Labor Watch](#)

[A fix to our throw-away technology culture](#), Internet Health Report, 2018

[Worker satisfaction starts with talking to factory employees](#), Fairphone blog, March 2019

**Further listening:**

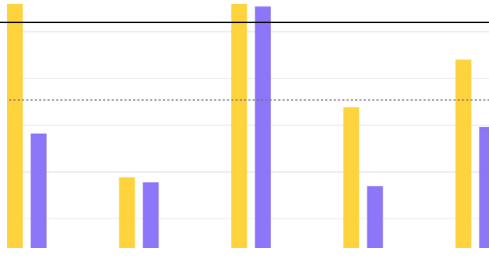
[Restart Podcast Ep. 24: Goodbye iSlave \(Pt 1\)](#), The Restart Project, September 2017

## Read more online

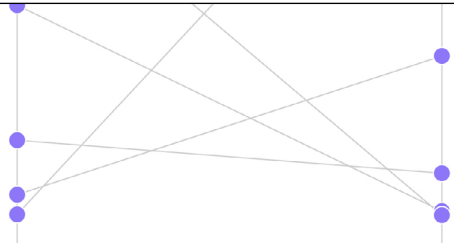
Recognizing the bias of artificial intelligence



Women journalist feel the brunt of online harassment



The world's slowest internet is the least affordable



Tech employees power up



A global push to identify everyone, digitally



Web Literacy

Introduction

# Who succeeds online?

Getting online isn't enough on its own. Everyone needs skills to read, write and participate in the digital world.

In 2018, the world passed an important milestone: more than 50% of people are now online. At this juncture, Web literacy is more critical than ever before.

We make hundreds of choices online every day. For many, it's now routine to use our phones to pay for coffee or bus tickets, or ask a voice assistant to play our favorite song. But for most of us, the technology we use every day is a black box. We don't fully understand the implications of the decisions we're making — or the decisions others are making for us.

The basic Web literacy skills are important. But they don't necessarily prepare us to identify and address the big questions and serious challenges like bias, harassment and concentration of power in our connected world. From the personal to the political, the role of technology in our lives is evolving rapidly. It's vital for our understanding of the digital world to evolve too.

Parents share baby photos on social media without a thought. But as children age, some see intimate information shared about them online as a violation of their privacy. Even small decisions have lasting effects. We need strong Web literacy skills to make informed choices.

The internet makes it easy to keep in touch with friends and connect with like-minded people. But how is our well-being impacted by the time we spend clicking and scrolling? Knowing what the research says (and doesn't say) can help us build healthier relationships with technology.

It's critical that we understand how the internet is impacting our societies — and are ready to demand change when necessary. In most countries, the internet is both helping and hurting democratic processes. There is greater access to information about candidates, more transparent public data and new avenues for

grassroots organizing. But it also facilitates election interference and the spread of harmful disinformation.

In the past year, we have gained a better understanding of how fringe groups, individual actors and governments and political parties exploit digital platforms to influence people. When governments propose solutions, there are risks of new harms. "Fake news laws" in different parts of the world (most recently Singapore) can seriously threaten free speech.

With deeper and more nuanced understanding of the digital world we can join global communities to help human rights defenders seek justice. We can create safer online spaces for young people to understand their sexuality. We can better understand the power dynamics of the online world, from the ad economy to the scale of mass surveillance.

We can imagine different worlds. We can demand change.

Investing in universal Web literacy is more urgent now than ever. This means supporting educators and activists, and learning with diverse communities. It also means creating products that are intentionally designed to be easy to understand and modify or repair.

The more of us who understand the evolving technologies, norms and business models of the online world, the closer we'll be to unlocking the full potential of a healthy internet.

# Sex education in the digital age

The internet didn't invent pornography, but it's no secret that adult content is more accessible today than ever before – including to younger audiences. How parents and teachers approach what for many is a taboo subject will be key to adapting sexual education to the digital age.

Concerns about the effects of pornography on adolescents have become part of mainstream conversation now that 80% of the worldwide youth population are online.

Because so much freely accessible adult content features hypermasculinity and prioritizes male pleasure, a major worry is that young people who watch porn could develop harmful attitudes about sex or abusive behaviors towards women.

Most research stops short of suggesting causal links between pornography and specific sexual attitudes and behaviors. But young people themselves say that it can affect them – whether they stumble on pornographic images accidentally or search for it themselves.

Emily Rothman is a Professor of Community Health Sciences at Boston University School of Public Health. She has been researching the connections between pornography and sexual violence for nearly a decade. In 2016, she led a study of 72 teens aged 15-17 and found that pornography was their number one source of information about sex.



Emily Rothman, 2019. Photo by Flynn Larsen. Courtesy of the Robert Wood Johnson Foundation, used with permission.

Rothman wanted to understand how and why pornography played such an important role in their lives, but also felt the insights could be used to help address the risks.

She teamed up with the Boston Public Health Commission's Start Strong peer leadership program to design an elective "porn literacy" course for high school students in Boston, Massachusetts in the United States.

The complete title of the course is "The Truth About Pornography: A Pornography-Literacy Curriculum for High School Students Designed to Reduce Sexual and Dating Violence" and it provides space for critical discussion about how gender, sexuality, consent, race, relationships and body image are portrayed (or not) in pornography.

Lessons range from defining terms used in online porn to helping students avoid clicking on things they don't want to see. Students are also guided through sensitive discussions about whether porn contributes to violence against women.

"We actually want to talk to kids about dating and sexual violence," Rothman says. "We discovered that kids find it fun and funny to talk about pornography. So we use it as a vehicle to talk about things we think are really critical, like negotiating consent and establishing healthy boundaries in a relationship."

Rothman believes that the best way to defend young people against negative impacts of pornography is to equip them with comprehensive, factual and sex-positive education. "In the absence of any other kind of education or information, of course it's more likely that kids will get their information from things made for profit or entertainment," she says.

"If they were flush with knowledge when they first encounter pornography, they would be

inoculated against some of the worst potential influences," says Rothman.

The internet can also play a positive role in providing safe spaces for young people to learn. For example, 70% of LGBTQ American college students said they researched their sexual orientation online. And many studies show that the internet helps LGBTQ youth connect with supportive peers, which in turn can increase their knowledge and self-confidence.

Positive outcomes like these is part of what free speech advocates say must be defended against censorship and why the right to anonymity matters so much. At least 16 countries censor online pornography though it's still possible to seek content from abroad. Proposals to enforce age limits on pornographic content have been opposed by digital rights groups including the Electronic Frontier Foundation who say it would infringe on the privacy of internet users.

In 2018, microblogging platform Tumblr banned adult content on their platform, sparking controversy about the loss of a "safe space" online for LGBTQ+ communities and sex workers. Bans on nudity and sexually explicit content are common on most platforms, including Facebook and YouTube, which now leaves thousands with no alternative place to go.

In this complex and changing digital landscape, what remains constant is the important role that supportive parents and educators can play in equipping young people with the knowledge and awareness to have positive understandings of sexuality and of healthy relationships. For young people on their own discovery journeys, the internet offers a wealth of resources – publications and communities of support – that can be a better starting point than porn for understanding sexuality and health, including websites like Amaze.org, Scarleteen.com and Ahwaa.org.

**Further reading:**

10 years on: why we still need better sex education for the digital world,  
Jessica Ringrose, Amelia Jenkinson,  
Sophie Whitehead, IOE London Blog,  
UCL Institute of Education, 2019

What Teenagers Are Learning From Online Porn,  
New York Times, 2018

Porn and sex education, porn as sex education,  
Kath Albury, UNSW  
Sydney, 2014

Adolescent Pornography Use and Dating Violence among a Sample of Primarily Black and Hispanic, Urban-Residing, Underage Youth,  
Emily Rothman and Avanti Adhia,  
Behavioral Sciences, 2016



# The challenge of democracy in the digital era

Is the internet helping or hurting democratic processes around the globe? In most countries, it is doing both.

In its golden era, the internet was celebrated for giving voters newfound access to information about candidates and unprecedented levels of transparency for public data. It laid the groundwork for a new generation of campaigns and social movements, enabling citizens to challenge existing power structures and information gatekeepers.

Today, this optimism has been tempered by the steady drip of news about election interference over the internet in the United States and countless other countries. It has awoken democratic institutions to new levels of concern. What happened in the 2016 presidential election in the [United States](#) may have surprised many Americans, but it was hardly unique on the world stage.

Take Brazil. Just ten days before right-wing Jair Bolsonaro was elected president, leading newspaper [Folha de São Paulo](#) uncovered a \$3 million USD scheme, paid for Bolsonaro affiliates, that promoted [viral, divisive messages](#) and false reports in Bolsonaro's favor, despite efforts by [fact-checking groups](#) and Facebook to stem the tide of disinformation.

Soon after, the reporter who wrote about the scheme began [receiving threats](#) and had her personal WhatsApp account hacked and inundated with pro-Bolsonaro messages.

Efforts to promote candidates with underhanded methods and stifle independent reporting are also widespread in India. [Civil society groups](#) have long observed [trolling and disinformation campaigns](#) on Facebook and WhatsApp that appear designed to undermine dissenting voices and promote Prime Minister Narendra Modi's ruling Bharatiya Janata Party (BJP).

In the lead up to an April 2019 election, social media platforms like [Facebook](#) and [Twitter](#) announced they took down hundreds of pages (with millions of followers combined) for ["coordinated inauthentic behavior"](#) and ["promoting spam"](#). Some favored the BJP, and others the opposing Indian National Congress party.

Facebook's role in particular, in these and other elections, has generated significant public scrutiny. In 2018, a globally reported [hearing of Mark Zuckerberg](#) by the United States Congress in light of a public scandal involving the consulting group, Cambridge Analytica, played a big role in putting [data harvesting for political purposes](#) into view.

Zuckerberg apologized then for not doing more to prevent the platform from being used for harm, including, "fake news, foreign interference in elections and hate speech."

Facebook has since pledged to improve transparency in political advertising. Twitter has added “elections integrity” to its public values. But such solutions may be mere band-aids. Platforms are designed in ways that incentivize and reward extreme and sensationalist content that generates clicks and shares through outrageous claims and attacks. Newsfeed algorithms are easily gamed by bots and professional trolls. Google search results can be manipulated.

In 2017 and 2018 Cambridge Analytica was also found to have collected data from users in India, Brazil, Indonesia and Mexico for campaign work. The consulting firm also put down roots in Kenya. In a case study from current President Uhuru Kenyatta’s 2013 election campaign, Cambridge Analytica described having built a strategy for the candidate “based on the electorate’s needs (jobs) and fears (tribal violence).” This struck a chord for Kenyans, who have grown accustomed to social media sparking violence between different ethnic groups.

In 2017, Kenyan parties engaged in targeted advertising and even personal SMS messaging to citizens, leveraging the Kenyan government’s ample collection of personal data, for which there are currently no legal protections for data privacy. President Uhuru Kenyatta won this election in a re-vote, after his initial win was nullified by the Supreme Court on the grounds of irregularities.

These cases represent just a handful of those that have dominated headlines and news feeds around the world in recent years. What they tell us, in sum, is that on the open internet anyone can reach and change the minds of millions of people -- especially if they have money to spend and are willing to weaponize information and data. Powerful and wealthy people and institutions, local and foreign governments, are wielding the internet in this way for political gain.

Ideas to mitigate the risks have begun to emerge. Support for independent fact checking initiatives is rising worldwide, and voters are becoming wiser to the digital machinations of political leaders and interest groups. Ahead of European elections in 2019, four leading tech companies (Facebook, Google, Twitter and Mozilla) signed the European Commission’s Code of Practice on Disinformation pledging to take specific steps to prevent disinformation from manipulating citizens of the European Union. Worldwide, social media platforms including Facebook, Instagram, Google, Youtube and Twitter are urged to be more transparent about how internet users are tracked and targeted, and give people more control over their own data.

Everywhere, there is consternation about what is to come. In Africa, elections are scheduled in 19 countries in 2019. In Asia, in upwards of 10 countries. In Latin America, there will be as many as nine elections, six presidential. Responsible reporting and factual information is crucial for people to make informed choices about who should govern. That is why fighting misinformation with care for free speech and open access to information is key. When power is up for grabs, no expense is spared to sway public opinion or to silence critics.

### **Further reading**

Our Data, Ourselves: Politics and Data, Tactical Tech, 2019

Digital Deceit: The Technologies Behind Precision Propaganda on the Internet, Dipayan Ghosh, Ben Scott, New America, 2018

A multi-dimensional approach to disinformation, Independent high level group on fake news and online disinformation, European Commission, 2018

Elections – Global Voices

# Who babysits your children's data?



Photo by Kelly Sikkema on Unsplash.

We teach children not to trust strangers in public. But far too often, parents themselves give strangers access to their children's lives over the internet.

Kids born today will have the largest digital footprint in history. In fact, some are "datafied" even before birth, as parents upload sonogram scans to the internet and marketers relentlessly track pregnant women. It's hard to say exactly what effect this will have on individuals in the future, but when parents and caregivers log milestones in apps, track their children's movements, and broadcast their lives in social media, their digital identity becomes a goldmine of information.

A 2018 report by the Children's Commissioner for England, "Who knows what about me?",

found that the average person in the United Kingdom will have 70,000 posts shared about them online by the time they turn 18. Highlighting the risk of this, Barclays Bank forecasts that "sharenting" (meaning parents who share info about their children) will be the cause of two-thirds of identity fraud and financial scams facing young people by the end of 2030.

Children themselves are growing up to discover information about themselves online they wish could be erased. From the Austrian teen who sued her parents for posting hundreds of photos

of her with their 700 social media contacts (including of her using the bathroom) to the fourth grader who asked her columnist mother to stop sharing private stories and photos.

“Teens get a lot of warnings that we aren’t mature enough to understand that everything we post online is permanent, but parents should also reflect about their use of social media and how it could potentially impact their children’s lives as we become young adults,” wrote one 14-year old girl in the United States who said she would quit social media, after feeling embarrassed and betrayed by what her mother and sister had posted online about her since she was born.

The United Nations has called for “strong guidelines” to protect children’s privacy. In France and Italy courts have sided with the child over the parent when intimate details are made public without a child’s consent. What else can be done?

Governments can set limits for what kind of data collection and marketing to children is acceptable. In Europe, for instance, the General Data Protection Regulation (GDPR) now imposes stricter rules on how children’s data can be collected and processed.

Schools can help teach students and their families how to navigate a digital world with privacy intact. App developers and internet platforms can create understandable privacy guidelines so parents (and children themselves) can assess the tradeoffs of using online services and games.

Caregivers can be mindful of what internet-enabled devices and toys they bring into children’s lives. Some of them listen in on conversations and capture data in pernicious ways.

Perhaps the simplest of all? Think hard before you post anything about children online. Is this

something their future friends or employers might see? A healthy internet is one where we feel comfortable with the information shared about ourselves and our families, whether we are children or adults.

#### **Further reading:**

Who Knows What About Me?  
Children’s Commissioner for England, 2018

I’m 14, and I quit social media after discovering what was posted about me, Fast Company, 2019

Sharenting: Children’s Privacy in the Age of Social Media, Stacey B. Steinberg, University of Florida Levin College of Law, 2017

YouTube Is Improperly Collecting Children’s Data, Consumer Groups Say, New York Times, 2018

## Read more online


Decoding images of war in Syria

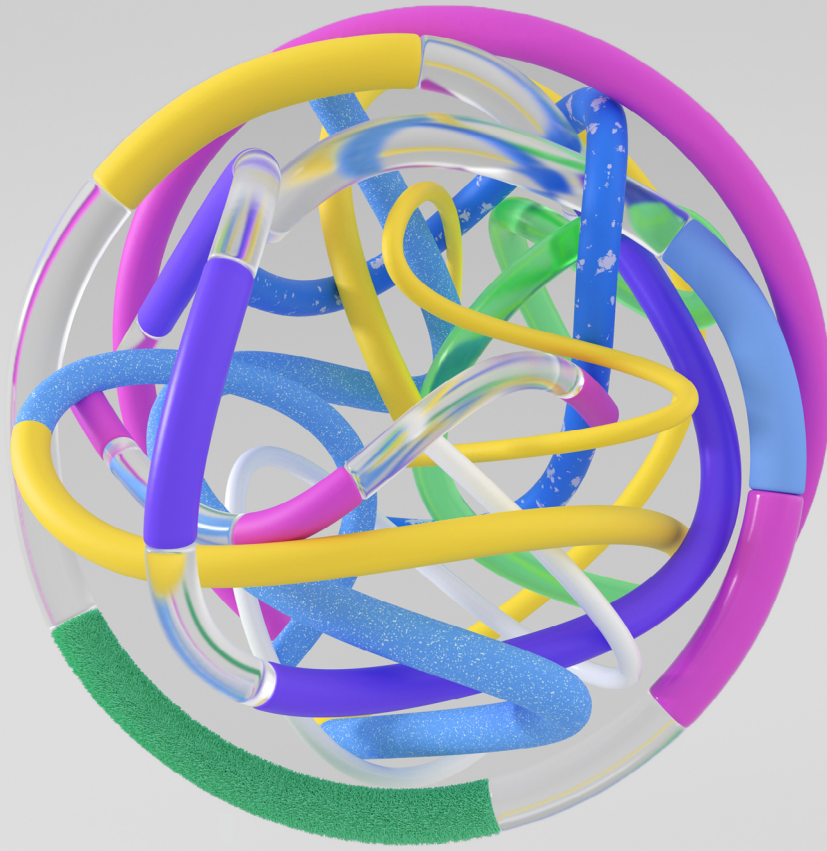


Spot the surveillance with VR



Breaking free of the addiction machine





Decentralization

Introduction

# Who controls the internet?

A few large players dominate much of the online world,  
but the internet is healthier when it is controlled by many.

Decentralization

Introduction

Many of the challenges facing the health of the internet today, can be traced back to the fact that the most ubiquitous digital products and services are controlled by a handful of players.

In the last year, the debate about this consolidation of power has continued, sharpened and, in some cases, started to grow teeth.

The digital world is dominated by eight American and Chinese companies: Alphabet (Google's parent company), Alibaba, Amazon, Apple, Baidu, Facebook, Microsoft and Tencent.

These companies and their subsidiaries have outsized control over the internet. They dominate all layers of the digital world, from the search engines, browsers and social media services many of us use daily, to core infrastructure like undersea cables and cloud computing that few of us see. They built their empires by selling our attention to advertisers, disrupting business models and creating new online marketplaces, and designing hardware and software that is now deeply integrated into many of our lives. Their influence is ever-increasing in our private lives and public spaces. Where they misstep, we can experience real harm.

A healthy balance of power in our global internet ecosystem depends on a delicate interplay between governments, companies and civil society. We need effective competition standards and technical interoperability — between the products of *different* companies — to ensure that the internet grows and evolves in ways that accommodate the diverse needs of people around the world.

Fines for breaking antitrust laws like the \$5 billion fine that European Union regulators hit Google with in 2018 have not had the effect needed to ensure a balanced and open future.

Many are exploring alternatives to an internet driven by the interests of corporate goliaths on their own. New business models are emerging that seek to distribute control among users, including platform cooperativism and collaborative ownership.

Vibrant communities of innovators are working to create alternatives to centralized systems by upscaling local connectivity, spinning up decentralized products, protocols and products and even creating independent alternatives to publishing on the big tech platforms.

From the start, the internet has enabled people to challenge authority, upend traditional business models and create greater transparency, openness and accountability. But the disruptive-for-good vision of the internet isn't something we can take for granted.

Everyone who uses the internet has a stake in its future. From city officials to technical professionals, to tomorrow's generation of internet users.

For an internet where there is true choice, we need to support products that diversify the market, and laws and policies that protect users and foster healthy competition. We need to join forces and drive citizen action, research and innovation to build a healthier internet.



# How the biggest internet companies make money

Eight companies wield enormous power over the entire internet: Google, Facebook, Microsoft, Amazon, Apple, Baidu, Alibaba and Tencent. Most internet users today are in daily contact with at least one.

They each have so many different products, services and investments that it's not always clear what their main source of revenue is, or how a company profits from services offered for "free," such as search, email, games, social media or instant messaging.

Just how do these giants of the internet make money? We've sorted them into four overlapping categories according to their primary source of revenue.

## **Further reading:**

[Spotlight: Too big tech?](#), Internet Health Report 2018

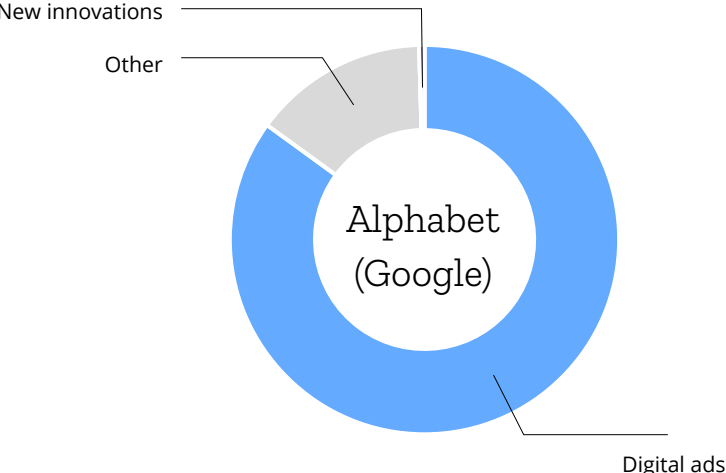
['Big Tech' isn't one big monopoly – it's 5 companies all in different businesses](#), The Conversation, 2018

[Tencent, the \\$500bn Chinese tech firm you may never have heard of](#), The Guardian, 2018

[Breaking Down How Amazon Makes Money](#), Visual Capitalist, 2017

# The Attention Merchants: Google, Facebook and Baidu

There’s money to be made from selling your attention to advertisers. The main business of Google, Facebook and Baidu is to collect data about what you do online, and enable publishers and marketers to target you with personalized ads. In 2018, Google and Facebook together controlled an estimated 84% of the global digital ad market outside of China.

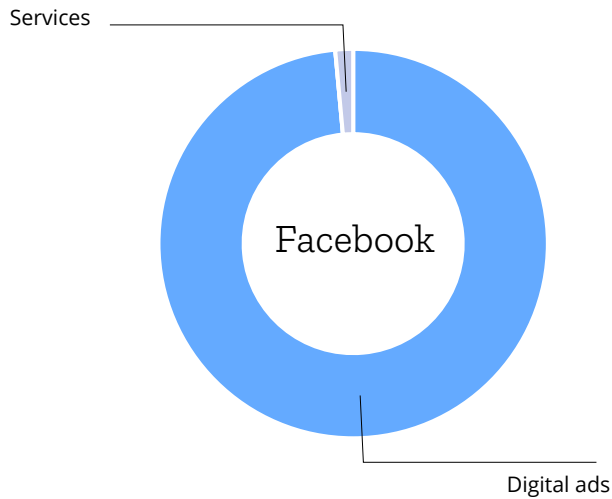


**Alphabet (Google)**  
Google’s parent company Alphabet earns 85% of their revenue from digital ads. Around 70% comes from ads on Google’s own products, e.g. Google Search or YouTube. Alphabet also owns Google’s AdSense and AdMob — services for placing ads on other websites — that together account for 14.6% of revenue. Sales of devices, like phones, home assistants, and apps in the Google Play store make up 14.5% of Alphabet’s total revenue.

**Revenue (2018)**  
\$136.8 billion USD

**Market capitalization**  
\$795.3 billion USD

**Alphabet (Google) Source:**  
Annual Report 2018, Alphabet, 2019. Market capitalization estimate from [Yahoo Finance](#) on March 4, 2019



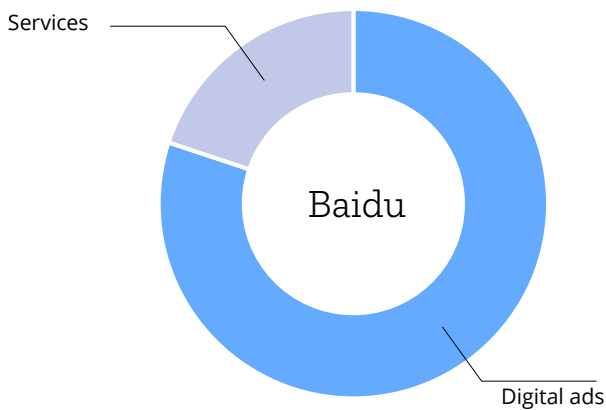
**Facebook**

We think of Facebook as a “social network,” but they are in fact an ad company. With around 2.32 billion monthly active users, Facebook makes more than 98.5% of its revenue — over \$55 billion USD — from selling ads that appear in our news feeds, mostly through the Facebook app. A fraction of their overall revenue (1.5%) is from games and other apps and products sold on Facebook.

**Revenue (2018)**  
\$55.8 billion USD

**Market capitalization**  
\$463.1 billion USD

**Facebook Source:**  
Annual Report 2018, Facebook, 2019.  
Market capitalization estimate from [Yahoo Finance](#) on March 4, 2019



**Baidu**

Baidu owns the top search engine in China with over 70% of the market share. It has a smaller revenue and footprint than Google, but a similar business model. Baidu makes about 80% of its income from selling ads. A smaller revenue stream (about 20%) is from membership services of iQIYI (a video streaming service similar to Netflix) and payment services. Like Alphabet, Baidu also invests in artificial intelligence and other innovations, like self-driving cars.

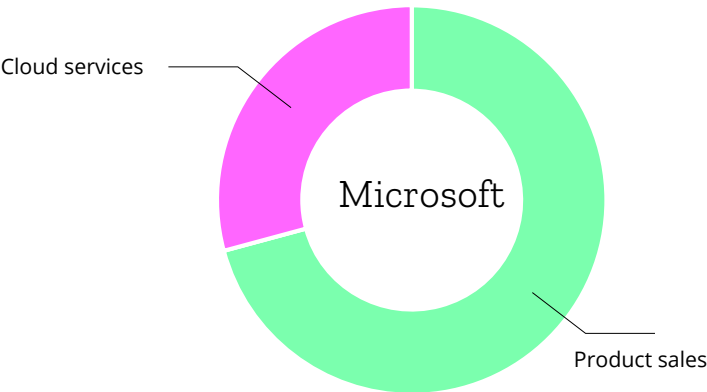
**Revenue (2018)**  
\$14.9 billion USD

**Market capitalization**  
\$56.6 billion USD

**Baidu Source:**  
Annual Report 2018, Baidu, 2019. Market capitalization estimate from [Yahoo Finance](#) on March 4, 2019.

# The Machinists: Apple and Microsoft

Microsoft and Apple earn most of their revenue from creating and selling the devices and software that allow us to access the online world. Mobile phones, computers, gaming consoles — as well as software like word processors and cloud storage — are all products that bring in revenue.

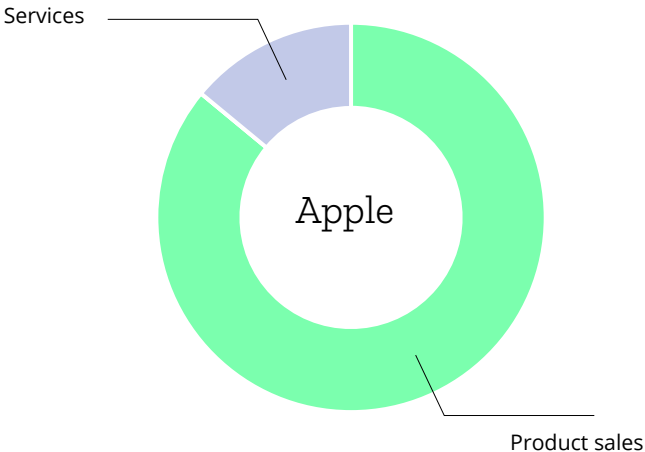


**Microsoft**  
70.8% of Microsoft's revenue is from product sales, but these products span many categories, including "productivity" products like Microsoft Office software and the online recruitment platform LinkedIn. Also in the category of product sales is software (including Windows), hardware (including Xbox and Surface tablets) and search ads. Microsoft's cloud-based services generated 29.2% of their total revenue in 2018.

**Revenue (2018)**  
\$110.4 billion USD

**Market capitalization**  
\$863.4 billion USD

**Microsoft Source:**  
Annual Report 2018, Microsoft, 2018.  
Market capitalization estimate from [Yahoo Finance](#) on March 4, 2019



**Apple**  
Apple earns 86% of its revenue from sales of digital devices and computers. The iPhone reigns supreme by a large margin: over half of Apple's total revenue in 2018 — nearly \$167 billion USD — was thanks to the pricey mobile phone. Sales of Mac computers accounted for 9.6% of product sales and iPads 7%. Apple's services including iCloud, Apple Care or Apple Pay make up 14% of their overall company revenue.

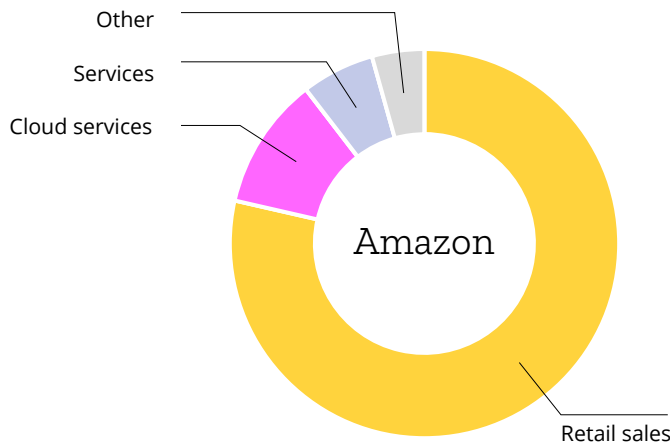
**Revenue (2018)**  
\$265.6 billion USD

**Market capitalization**  
\$825.0 billion USD

**Apple Source:**  
Annual Report 2018, Apple, 2018. Market capitalization estimate from [Yahoo Finance](#) on March 4, 2019

# The Retail Middlemen: Alibaba and Amazon

Amazon and Alibaba primarily make their money by selling us things online. Both Amazon and Alibaba have also begun to open physical retail stores that meld with online experiences. There's much more. They each also sell digital ads and services including online video streaming, logistics and cloud computing, money transfers — even food delivery services!



## Amazon

It used to be a book business, now it's an everything business. Amazon makes most of its revenue (78.5%) through retail sales. Subscription fees for Amazon Prime (including video streaming) brings in 6% of their revenue. Amazon Web Services brought in 11% of Amazon's total revenue in 2018, an on-demand cloud computing service offering computing power, database storage web hosting and other functionality.

### Revenue (2018)

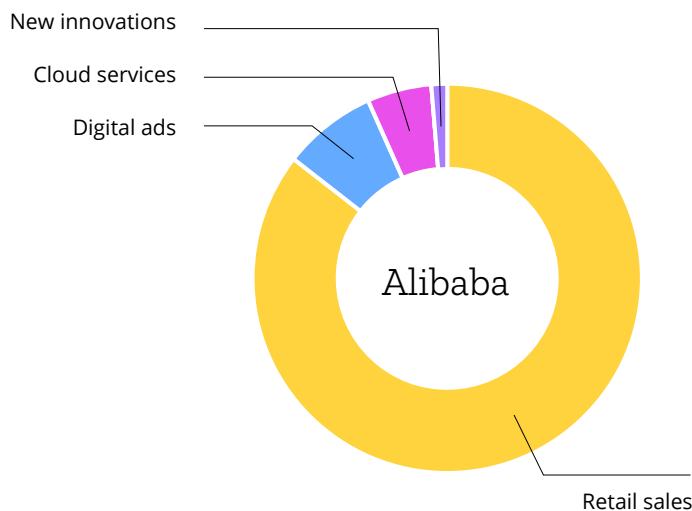
\$232.9 billion USD

### Market capitalization

\$821.2 billion USD

### Amazon Source:

Annual Report 2018, Amazon, 2019. Market capitalization estimate from Yahoo Finance on March 4, 2019



## Alibaba

Alibaba earns most of its revenue (85.6%) by selling goods to 552 million customers in China, but also from digital ads, subscription fees for Youku Tudou (a popular video streaming service) and with cloud-based services. Alibaba offers cloud services and invests into integrating and further digitizing its different businesses. Moreover, Alibaba is innovating on software products like AutoNavi, a mapping service with approximately 60 million daily active users.

### Revenue (2018)

\$39.9 billion USD

### Market capitalization

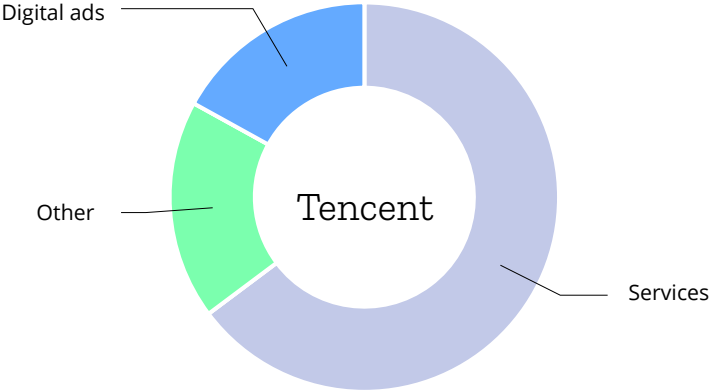
\$476.7 billion USD

### Alibaba Source:

Annual Report 2018, Alibaba, 2018. Market capitalization estimate from Yahoo Finance on March 4, 2019

# The Multi-Faceted One: Tencent

The Chinese company Tencent is especially known for its messaging platform WeChat, but the company does not disclose how much money it makes from it directly. Unlike WhatsApp or Telegram, WeChat is much more than a messenger app — it is deeply integrated into everyday life in China and allows you to do things like pay bills and schedule a doctor’s appointment.



**Tencent**

The majority of Tencent's revenue comes from in-app purchases of virtual goods (mostly extras in games), and subscription fees on Tencent Video (lumped together in 'Services' with 56.6% of the total 2018 revenue). An increasingly important section for Tencent are payment services (included in 'Other' with 24.9%), which mostly refers to fees for online transactions through WeChat Pay. Other than that, Tencent makes money with digital ads on its media platforms and messengers (18.5%).

**Revenue (2018)**  
\$45.5 billion USD

**Market capitalization**  
\$397.2 billion USD

**Tencent Source:**  
Annual Report 2018, Tencent, 2019. Market capitalization estimate from [Yahoo Finance](#) on March 4, 2019

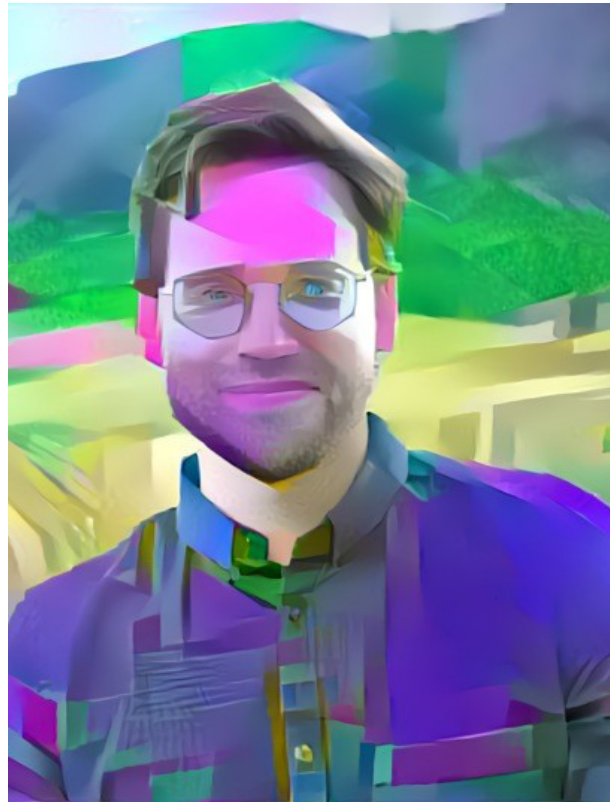
# What if Facebook were owned by its users?

For decades, startup founders have looked with dollar signs in their eyes at anything you could possibly do with the internet. In a corporate culture fostered by large venture capital funds, startups compete to become the next big billion-dollar disrupter, like Uber or WhatsApp.

Too often, the business models of the biggest internet companies have led them to squander the trust of users and workers by putting profits ahead of people's best interests.

At the height of public scandals, consumers have launched campaigns like #DeleteUber or #DeleteFacebook to voice their objections. But with few good alternatives to major internet companies like Amazon, Google or Facebook, the social or economic cost of abandoning them can be too high. Could there be a truly democratic way for users to steer companies?

A new generation of internet entrepreneurship is emerging to respond. There is Zebras Unite, a women-led movement to push for more ethical and inclusive alternatives to the "unicorn" culture of Silicon Valley. There is the Purpose Foundation that promotes "steward-ownership" as a legal structure to prioritize a mission over profit. And there are hundreds of cooperatively owned and managed companies around the world exploring how to share power and profits directly with users, in order to break the cycle of maximizing gain at any cost.



Emily Rotham, 2019. Photo by Flynn Larsen, Courtesy of the Robert Wood Johnson Foundation.

Mapping such alternative forms of internet entrepreneurship – or "platform cooperativism" – is a passion of Nathan Schneider at the

University of Colorado Boulder in the United States. Together with [Trebor Scholz](#) who initiated the [Platform Cooperative Consortium](#) at the New School in New York, he co-organized some early gatherings of the platform coop community. Schneider is the author of [Everything for Everyone: The Radical Tradition That Is Shaping the Next Economy](#) and a co-founder of [Start.coop](#), a business accelerator for new cooperatives.

Mozilla: What is the problem platform cooperatives could solve?

Nathan Schneider: We are in a major accountability crisis with the online economy. Companies are taking on utility roles, but we don't have a choice of whether to use their services because there are no meaningful alternatives. We see people agonizing about giving away their data, but not really doing anything because they have no other choice. Community ownership is an opportunity to build accountability into platforms. It is a vehicle for users to gain a voice and build democracy into companies. Maybe it can even lead to a rejuvenation of the democratic sphere.

In most places, people don't even stop to consider that they have the choice to create an alternative to existing companies that are giving people a bad deal.

When Uber backed out of Austin, Texas following a dispute with local authorities in 2016, it led to the creation of a new ride-sharing nonprofit, [Ride Austin](#). It's [better for drivers](#) and supports local nonprofits. It's better for drivers and supports other local nonprofits. It's a totally different vision for how things can work in an economy.

Mozilla: Do you think big tech could evolve in the direction of cooperative models?

Nathan Schneider: Wouldn't it be great if these big companies would share ownership with

the people who are really generating value for them? Instead we have an online economy that is structured to generate massive profits for a small number of shareholders. Involving users in ownership means making sure they are not getting cut out of the value they are creating, and ensuring that they benefit alongside investors in the wealth that they are creating together.

In 2017, I was involved in a campaign to bring a shareholder resolution to a Twitter annual meeting to encourage the company to consider options for expanding user ownership and governance in the platform as a way to address systemic problems. We weren't successful, but we do need more strategies to bringing democracy to companies. Especially when we recognize they're so big that they basically become utilities. For instance, it could be a legal structure and tax treatments that would lead somebody like Facebook's Mark Zuckerberg to see it as a reasonable option to transfer large amounts of stock and control [to users](#).

Mozilla: The allure of venture capital funding is strong. What motivates founders to go for a cooperative business model instead?

Nathan Schneider: Often people are trying to solve deep problems and realize that handing something over to investors just isn't going to cut it. One example is [Jen Horonjeff](#), the founder of [Savvy](#). It's a health insights platform for patients and their families. She has a chronic illness and she was obsessed with patients having more control over their illness. She knew that whenever you hand medical processes over to investors, patients get exploited. So she turned to a coop model as a last resort to protect people, and at the same time run a business.

The economy needs variety. There may always be a need for the classic high risk and high return model of venture capitalism, but at the same time we can create more options.



**Further reading:**

Ours to Hack and to Own: The rise of platform cooperativism, a new vision for the future of work and a fairer Internet, edited by Nathan Schneider and Trebor Scholz, 2017

Platform Cooperative Consortium

The Internet of Ownership Website and Directory

Why the cooperative models need to be at the heart of our new economy, Fast Company, 2018

# When a hurricane zaps the internet



Loiza Puerto Rico six months after Hurricane Maria. Photo by Preston Keres (public domain).

The internet is designed to be resilient. But after Hurricane Maria in 2017, as Puerto Ricans rushed to contact friends and family, many found they couldn't get online.

The storm broke power lines and toppled telecom towers, taking out 95.6% of cell sites and leaving Puerto Ricans scrambling for a signal. It zapped the internet.

Half a million homes were damaged, thousands of people died. By some estimates, the territory experienced the worst power failure in U.S. history.

Extreme weather caused by climate change increases the likelihood that disaster will strike

again soon – in Puerto Rico and around the world – and that once again, loss of internet will make a humanitarian crisis even harder to overcome.

“We’re talking about humans of flesh and bone [who died] because of telecommunications, because you couldn’t pick up the phone or message someone,” said Puerto Rican journalist Sandra Rodriguez in an interview with NOVA Next about the internet outages.

Following Hurricane Maria, Puerto Rico's internet problems soon spread. Several countries in South America that rely on submarine cables that land on the Caribbean island, including Argentina and Brazil, experienced network disruptions in September 2017 due to power failures.

A variety of small and big scale initiatives to restore the internet blossomed. The non-profit NetHope sent and installed WiFi equipment. Telecom companies deployed mobile hotspots. Google's Project Loon delivered internet via balloons. Still, it took nearly a year to restore power to the whole island, and average internet speeds did not reach pre-storm levels until August 2018, according to NOVA Next.

With hurricane season looming every year, Puerto Rican internet advocates are pushing for measures to fortify the internet for the next big storm. In February 2018, The Internet Society (ISOC), a nonprofit that champions internet access for all, issued a report informed by their Caribbean chapters of what could be done to prevent another connectivity disaster.

Electricity is a must-have. But the island's natural geography and historic planning makes energy supply tricky. For instance, while most of Puerto Rico's 3.3 million people live in northern metropolitan areas, 70% of power generation happens in the south. That awkward centralization means the grid system has to cut across the island, exposing wires to the elements.

Distributing power up Puerto Rico's mountains is also difficult and costly. After the power outage, cell towers relied on backup generators. Once the generator fuel ran out, "You couldn't get to the towers because the roads were blocked, so antennas started to drop off because they didn't have power. It was messy," said Eduardo Diaz, a director of the ISOC Puerto Rico board who is also assembling an

advisory committee to help develop the chapter's strategic plan.

Diaz says local loss of confidence in the grid is driving new, sustainable, decentralized energy solutions that fit the climate better. "This is a tropical island, you get sun most times of the year... You won't believe how many people want to get into solar, or be offgrid in case something like this happens again. There's a huge market," Diaz says.

But Puerto Rico also needs to raise climate awareness among internet stakeholders. Despite working in a storm-prone area, the internet industry doesn't always build sustainably.

Shernon Osepa, Regional Affairs Manager for Latin America & The Caribbean Bureau at ISOC, sees a need to address this problem. "These operators know that we live in a very vulnerable environment, but some of them are deploying networks as if we're living in a region where these things don't happen," Osepa cautioned, noting that some Caribbean infrastructure is only rated to withstand category 3 hurricanes, despite facing category 4-5 hurricanes.

Opening data to the public is also key for the recovery. "We don't have a picture of how bad the telecommunication is," Diaz says. He argues that the Puerto Rico Broadband Taskforce should prioritize creating a map of what parts of the island are without broadband service..

Puerto Rico suffered from broken infrastructure and budget cuts long before the storm. The U.S. Federal Emergency Management Agency has contributed large sums to emergency repairs, but politicians are reluctant to supply the funds necessary for a complete infrastructure redesign. Instead they opt for quick-fixes, or even plans that are not in Puerto Rico's best interests.

In response to tight budgets, Diaz encourages creative thinking and more sustainable solutions. For instance, he says, existing internet access grants for public schools could be used to create “anchor institutions” that help supply internet to people in surrounding communities.

Climate change is rapidly creating new hurdles for internet advocates in the Caribbean and around the world. We can expect more hurricanes and natural disasters for sure. This urgently calls for alternative and regionally appropriate infrastructure to be deployed already today.

### **Further reading**

Report from the Field: Post-Hurricane Connectivity in the Caribbean, Internet Society, February 2018

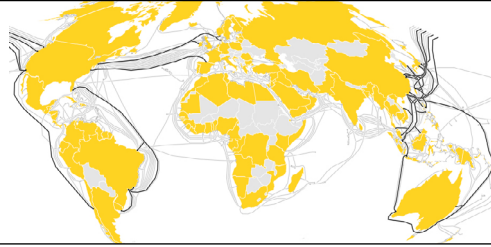
After Hurricane Maria, Puerto Rico’s Internet Problems Go from Bad to Worse, NOVA Next, October 2018

Lights Out: Climate Change Risk to Internet Infrastructure, University of Wisconsin – Madison, 2018

Puerto Rico’s Slow Internet Recovery, Oracle Internet Intelligence, 2017

## Read more online

The new investors  
in undersea cables



An open source alternative  
for the cloud



# 10 minutes to a healthier internet

What you can do right now to improve your internet health:

## 1. Check the privacy of your apps.

Apps can be great for games, getting around town and staying in touch with friends. But they also know a lot about you, and they might be sharing your data. But they also know a lot about you, and they might be sharing your data. You can check the privacy setup of your favorite Android apps on [AppCensus AppSearch](#) to learn more about what data they access and share with other parties over the internet.

## 2. Protect your accounts.

Your private information is only as safe as your passwords.

[Check to see if your account has been compromised](#). If it was, stop using the exposed password and change it everywhere, even for old accounts. If your financial information was involved, alert your bank and monitor your statements.

Protect yourself by using a different password for every account. A password manager like [1Password](#), [LastPass](#), [Dashlane](#), and [Bitwarden](#) can help you by generating super-strong passwords and remembering them all for you.

Install two-factor authentication [wherever possible](#). To stay on top of data breaches that affect your account, sign up for the [Firefox Monitor alert](#).

## 3. Think twice before getting a DNA test.

Your DNA sample has [privacy implications](#) not just for you, but also for your family members. Where possible, have a conversation with those affected about the implications for everyone's privacy, and about whether or not the test is likely to give you accurate results, and make a plan for how to navigate potential surprises.

# Join the movement

There are many organizations and groups worldwide — and likely also in your country or city — that work directly to make the internet healthier. Getting involved with an organization is often the best way to learn more and contribute to creating a healthier internet.

**The organizations we mention in this year's report are great places to start.** We suggest ways you can connect with some of them below. The question is: what do you want to do?

**You're also invited to get involved with Mozilla, the organization that publishes the Internet Health Report.** You can find opportunities to participate [online](#).

## I want to help

### I want to help support an open internet

- **Support and contribute to [Wikimedia](#):** a global movement whose mission is to bring free educational content to the world. They're probably best known for [Wikipedia](#), a free online encyclopedia. But they also have other projects, like [Wikidata](#). There are [many ways to get involved](#), including finding the [local affiliate nearest to you](#).
- **[Help Access Now](#) fight internet shutdowns by joining their [#KeepItOn](#) campaign.** Internet shutdowns are on the rise: Access Now documented 188 shutdowns worldwide in 2018. That's more than double than the number of shutdowns in 2016. Through [#KeepItOn](#), Access Now is collecting and sharing stories about how internet shutdowns impact people's lives, and gathering supporters to demand that world leaders pledge to keep the internet on.

## I want to help make the internet more private and secure.

- **Run a relay for the Tor Project**, a free browser that enables people to publish and share information online with a high degree of privacy and security. By supporting Tor, you'll help defend anonymity online for millions of people worldwide.
- **Join the The Internet Society**, an organization that helps build and support communities that make the internet work, as part of their mission to create a globally-connected, secure and trustworthy internet. See if there's an Internet Society chapter where you live. If not, consider forming a chapter.

## I want to help create an inclusive internet.

- **Get involved with the Algorithmic Justice League to help fight bias and increase accountability in automated systems.** Founded by Joy Buolamwini, the Algorithmic Justice League conducts research into topics like how commercial facial analysis systems encode gender and racial biases, and proposes solutions like the Safe Face Pledge: a guide to help companies build facial analysis technology that does not harm people.
- **Become a TrollBuster.** When you spot online threats, cyberharassment or other troll behavior against women writers, report them to TrollBusters. The organization will send you, or whoever is under attack positive messages, virtual hugs or reputation repair services. Nearly two-thirds of female journalists surveyed by TrollBusters and the International Women's Media Foundation in 2018 said they had experienced online harassment.



## I want to help improve web literacy.

- **Help improve the readability of Terms of Service with the “Terms of Service; Didn’t Read” (ToS;DR) project.** “I have read and agree to the Terms” is one of the biggest lies on the web. ToS;DR aims to fix that. Project contributors read and rate Terms of Service, with the goal of pushing companies to make it easier for their users to understand what they’re agreeing to.
- **Learn how to support Amnesty International’s Decoders to support human rights research.** It’s a community of over 50,000 online volunteers from more than 150 countries who donate their time and skills online. In the hands of human rights defenders working to protect and seek justice for vulnerable people worldwide, the internet is a powerful tool for documentation. Decoders projects are broken into micro-tasks that anyone can help with.

## I want to help keep internet decentralized.

- **Donate your voice to the Common Voice project.** Common Voice was founded to spark more decentralized innovation, by helping to make the data needed to create voice recognition systems open and accessible to everyone. It’s is now the largest dataset of human voices available for use.
- **Consider alternative business models for the internet.** Explore communities like the Platform Cooperativism Consortium; projects like The Internet of Ownership; or Zebras Unite, a women-led movement to push for more ethical and inclusive alternatives to the “unicorn” culture of Silicon Valley.



**moz://a** [internethealthreport.org/2019](https://internethealthreport.org/2019)