Internet Health Report 2019

Mozilla Foundation

INTERNET HEALTH REPORT 2019

[transcript] moz://a

Mozilla Foundation
Internet Health Report 2019

Established in 2003, guided by the Mozilla Manifesto, the **Mozilla Foundation** believes the Internet is a global public resource that must remain open and accessible to all. The Mozilla Foundation is a not-for-profit organization that exists to support and collectively lead the open source Mozilla project. It views its work as part of a global movement for a digital environment that aims at putting people in charge of their own data and that makes the internet a more democratic place by mobilizing a critical mass of conscioуus internet users.

Mozilla Foundation

Internet Health Report 2019

[transcript]

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

The report was edited by Solana Larsen.
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.

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de

First published in 2019 by transcript Verlag, Bielefeld

Cover layout: Maria Arndt, Bielefeld
Typeset by Michael Rauscher, Bielefeld
Printed by Majuskel Medienproduktion GmbH, Wetzlar
Print-ISBN 978-3-8376-4946-8
PDF-ISBN 978-3-8394-4946-2
https://doi.org/10.14361/9783839449462

Content

Introduction | 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.

Read and explore

This report is structured according to five overlapping themes that we consider a helpful framework for assessing internet health: privacy and security, openness, digital inclusion, web literacy, and decentralization, but it's designed so you can read the articles in any order.

In the spirit of engagement with readers, the website of the 2019 Internet Health Report enables you to create and publicly share your own reading list of articles. We also encourage online comments and reflections on individual articles. For instance, how do you make decisions about what to share about your children online? Or would you recommend your country's approach to digital ID? There aren't simple answers to questions like this, but hearing diverse experiences and ideas can expand anyone's perception of the toughest issues. We welcome your input!

Credits

So many researchers, fellows, writers and allies of Mozilla generously contributed data and ideas alongside hundreds of readers who participated with comments and emails.

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.

Rainbow Unicorn in Berlin, Germany developed the visual design (and code for the website). Christian Laesser developed the data visuals that appear online, and Julian Braun produced the 3D artwork.

Website: https://internethealthreport.org/2019
Contact us: internethealth@mozillafoundation.org
Hashtag: #InternetHealth

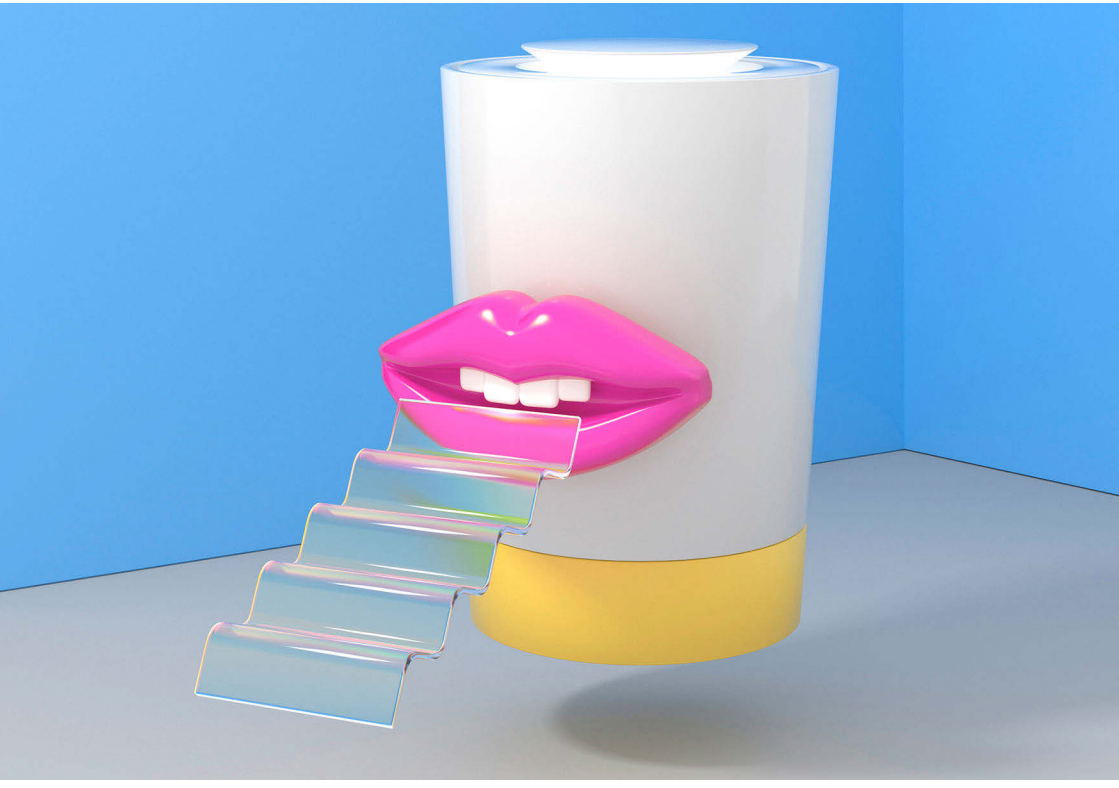
Credits

Katya Abazajian
Coraline Ada Ehmke
Chris Adams
Pablo Aguilera
Esra'a Al-Shafei
Mahsa Alimardani
Christopher Arnold
Miriam Avery
Renata Avila
Juma Baldeh
Juan Barajas
Geraldo Barros
Dan Bateyko
Jochai Ben-Avie
Owen Bennett
Cathleen Berger
Ellery Biddle
Reuben Binns
Julian Braun
Marianna Breytman
Niels Brügger
Jory Burson
Sam Burton
Luis Carlos Díaz
Irvin Chen
Henrik Chulu
Emilio Cobos Álvarez
Norberto Cruz
Chris Dart
Kelly Davis
Christopher De Cairos
Michiel de Jong
Amira Dhalla
Eduardo Diaz
Marianne Diaz Hernandez
Renée DiResta
Stefania Druga
Will Easton
Steven Englehardt
Marshall Erwin
Ayden Ferdeline
Kadija Ferryman
Arturo Filastò
Liz Fong-Jones
Conor Fortune
Ankit Gangwal
Gabriela Garcia Calderon Orbe
Babitha George
Brandi Geurkink
Gaetan Goldberg
Kristina Gorr
Paolo Granata
Sam Gregory
Lisa Gutermuth
Sarah Haghdoosti
Andrew Hatton
Sydette Harry
Mél Hogan
Jen Horonjeff
Gabi Ivens
Joi Ito
Frank Karlitschek
Jofish Kaye
Ephraim Kenyanito
Daniel Kessler
Julia Kloiber
Eireann Leverett
Andrew Losowsky
Elaine Lu
Raegan MacDonald

Rebecca MacKinnon
Nathalie Maréchal
Milena Marin
Zannah Marsh
Don Marti
Meghan McDermott
Uta Meier-Hahn
Alan Mooiman
Alice Munyua
Selina Musuta
Esther Mwema
Mohamed Nanabhay
Shreyas Narayanan Kutty
J. Nathan Matias
Anna Niedhart
Michael J. Oghia
Daniel O'Maley
Jens Ohlig
Juan Ortiz Freuler
Julie Owono
Mong Palatino
Abigail Phillips
Lydia Pintscher
Isabelle Poweleit
Zara Rahman
Pauline Ratzé
Christian Reich
Maya Richman
Martin J. Riedl
Chris Riley
Elizabeth Rivera
Tara Robertson
Jon Rogers
Emily F. Rothman
Chad Sansing
Nathan Schneider
Steve Song
Matthias Spielkamp
Matt Stempeck
Marcel Stirner
Mark Surman
Kasia Szymielewicz
Juan Tapiador
Alek Tarkowski
Berhan Taye
James Teh
Dhanaraj Thakur
Michelle Thorne
Katrin Tiidenberg
Solange Tuyisenge
Claire Ulrich
Amba Uttara Kak
Anne van Kesteren
Kristina Verbo
Edoardo Viola
Andreas Wagner
Maya Wagoner
Sarah Watson
Heather West
Stephanie Ann Whited
Matthew Willse
Yvette Wohn
Natalie Worth
Cori Zarek
Kevin Zawacki

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 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 pub-

lic 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?

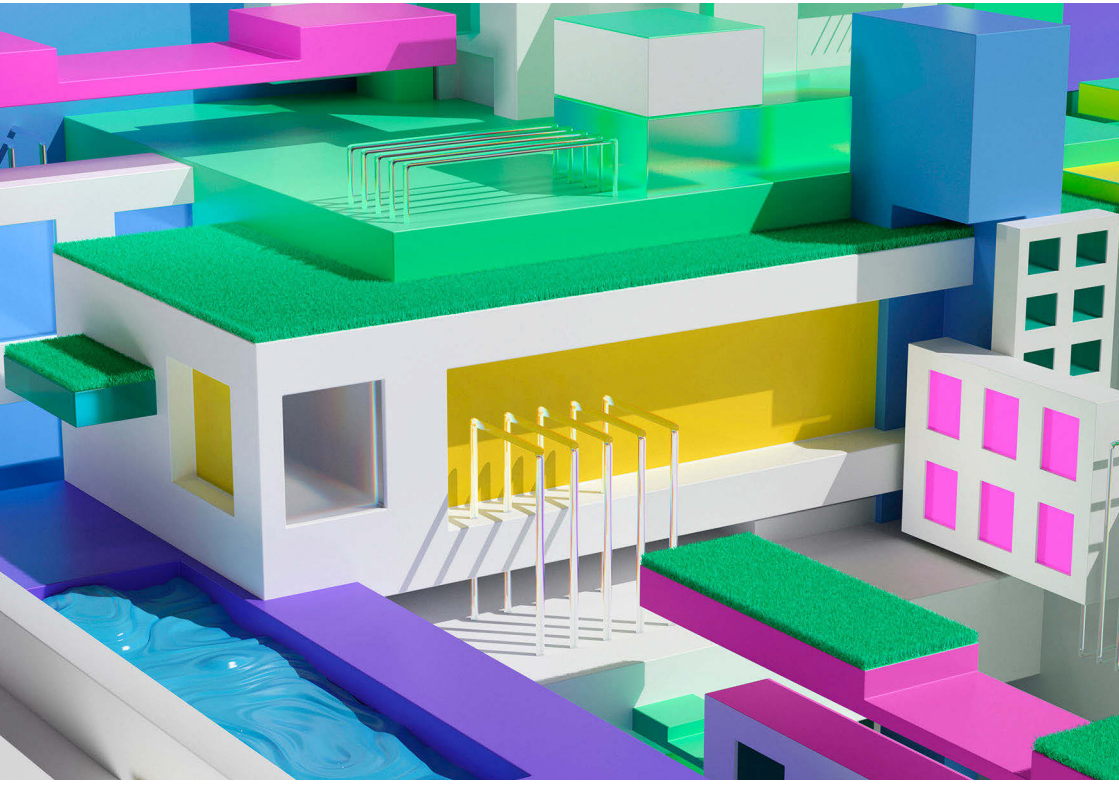
► Further reading

- Situating Methods in the Magic of Big Data and Artificial Intelligence, danah boyd, M.C. Elish, Communication Monographs, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040201
- AI Now 2018 Report, AI Now Institute, December 2018. https://ainowinstitute.org/AI_Now_2018_Report.pdf
- Data Feminism, Catherine D'Ignazio, Lauren Klein, MIT Press Open, January 2019. https://bookbook.pubpub.org/data-feminism
- Anatomy of an AI system, Kate Crawford and Vladan Joler, SHARE Lab and AI Now Institute, 2018. https://anatomyof.ai/

► Further listening

- RecodeDecode podcast: Meredith Whittaker and Kate Crawford: How AI could change your life, April 2019. https://www.recode.net/podcasts/2019/4/8/18299736/artificial-intelligence-ai-meredith-whittaker-kate-crawford-kara-swisher-decode-podcast-interview

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 Sevilia, 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 reframe 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."

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 crim-

inal 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.

Nathalie 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. https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/
- It's time for a Bill of Data Rights, Martin Tisne, MIT Technology Review, 2018. https://www.technologyreview.com/s/612588/its-time-for-a-bill-of-data-rights/
- Corporate Accountability Index, Ranking Digital Rights. https://rankingdigitalrights.org/

Is it safe?

Understand the issue: Privacy and security

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 datarich digital age have 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.

23 reasons not to reveal your DNA

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 medtech 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 nonprofit 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. https://gizmodo.com/how-dna-testing-botched-my-families-heritage-and-probab-1820932637
- Ancestry wants your spit, your DNA and your trust. Should you give them all three?, McClatchy, 2018. https://www.mcclatchydc.com/news/nation-world/article210692689.html
- The Forensic Genetics Policy Initiative – Country Wiki. http://dnapolicyinitiative.org/wiki/index.php?title=Main_Page

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 Ann Whited: 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 underappreciated 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?

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?

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?

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?

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. https://metrics.torproject.org/
- "Tor is easier than ever. Time to give it a try", WIRED, January 2019. https://www.wired.com/story/tor-anonymity-easier-than-ever/
- If anonymity isn't the problem, what is?, Internet Health Report, 2018. https://internethealthreport.org/2018/if-anonymity-isnt-the-problem-what-is/

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, "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective" offers a glimpse of how many people fall prey, and suggests a new counting method to better estimate the millions of dollars of payments. For instance, on May 15, 2017 alone the equivalent of $ 24,246.51 USD in ransom payments were transferred to WannaCry ransomware attackers [see animated data visualization on the Internet Health Report 2019 website]. In few days, an estimated 300,000 businesses in 150 countries were hit. There are still new WannaCry victims today.

► Further reading

- The No More Ransom Initiative. https://www.nomoreransom.org/
- On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective; Mauro Conti, Ankit Gangwal and Sushmita Ruj, 2018. https://arxiv.org/abs/1804.01341
- With Ransomware, It's Pay and Embolden Perpetrators, or Lose Precious Data, The New York Times, May 2017. https://www.nytimes.com/2017/05/17/technology/bitcoin-ransomware-pay-lose-data.html

Coordinating complaints for data privacy in Europe

Civil society organisations in Europe are playing a crucial role in enhancing the effectiveness of the European General Data Protection Regulation (GDPR) by using its enforcement provisions to challenge established practices of some of the biggest technology companies in the world.

The GDPR addresses some of the power imbalances between users and tech companies that operate globally. It has strengthened existing rules and given new powers to enforcement authorities. Companies and organizations are forced to be more transparent about how they collect and process personal data.

Even though the GDPR is a European regulation, it is relevant globally. First, because it applies to data collection about European citizens, it is recognized by many internet companies that dominate the global web. Second, countries around the world are watching to understand its strengths and weaknesses as they consider similar regulations.

One year since the law came into effect in May 2018, the efforts of filing complaints across Europe are beginning to bear fruit. By helping users going after companies that collect their data, digital rights organizations in Europe hope to improve how privacy regulations are being enforced to close the gap between legal protections and actual practice.

In January 2019, Google was fined €50 million Euros (about $57 million USD) by the national Data Protection Authority (CNIL) in France following two complaints on "forced consent" by noyb – European Center for Digital Rights in Austria and La Quadrature du Net in France.

Is GDPR working?

A coalition of digital rights organizations in Europe have created the publication GDPR Today to collaboratively collect and publish statistics that help advocacy organizations across Europe understand how the GDPR is being applied and to raise awareness of EU rights.

There are inconsistencies in how different countries collect and provide data but GDPR Today has compiled reports of data breaches and complaints from 10 out of 28 European Union countries in their March 2019 edition.

Between May 2018 and March 2019, there have been at least 71,237 complaints and 28,977 data breach notifications reported in those ten countries

alone – all varying in nature. The Irish data protection authority reports that among the 1,928 GDPR complaints they received between May and December 2018, most fall under the categories of "Access Requests" (30 %), closely followed by "Unfair Processing of Data" (15 %) and "Disclosure" (11 %).

An important right granted by the GDPR is that individuals can request a copy of the data collected about themselves in an unedited and intelligible form. This allows individuals and watchdog organizations to get a better sense of what personal data online services collect. noyb has tested whether and how popular streaming services comply with this requirement by requesting a copy of user data from a variety of companies. According to noyb, none were fully compliant. They filed ten different complaints against eight streaming services in January 2019.

Other contributors to GDPR Today have similarly filed complaints to advocate for a better enforcement of existing protections including Panoptykon, Privacy International and Open Rights Group.

It's clear, the GDPR will only be as effective as its enforcement, and civil society groups are playing a crucial role in ensuring that enforcement happens. That is an important lesson not only for Europe, but for privacy advocates around the world. As data protection authorities across Europe react to these complaints we will see what effect GDPR ultimately has.

► Further reading

- How Is the GDPR Doing?, Slate, 2019. https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html
- GDPR explained, Bits of Freedom, European Digital Rights (EDRi) and Panoptykon Foundation, 2018. https://gdprexplained.eu/

Your mobile apps are tracking you

If you have any apps installed on your mobile phone – be it games, news or fitness apps – it's likely that you are sending some kind of data about your identity, preferences, or physical location to Google, Facebook and other companies without even knowing. This alone shouldn't be news to you, but new research now documents how significant the issue is in scale.

An Oxford University study of nearly 1 million free Android apps in 2018 revealed that the majority of mobile apps contain utilities from companies – including Alphabet, Facebook, Twitter, Verizon, Microsoft and Amazon – that enable them to track and send data about users to these companies. These utilities are incorporated by app developers for a variety of reasons. For instance, the app developer might use them to monitor the use of the app or to display ads.

The researchers make no claims about what data is transferred to companies, but warn that it's common for them to gain access to data that is not directly related to the app in use. Depending on app permissions, this could be as broad as a contact list or location history.

With transparency lacking about what is tracked by whom, the researchers see potential privacy risks that leave people vulnerable. Data combined from multiple apps, along with other online history and behavior, can be used to generate very detailed profiles of individuals. From the apps on a person's phone you could estimate interests, sexual orientation, health status and the identities of their children.

Google disputed the negative implications of the study, telling the Financial Times in October that the researchers mischaracterize "ordinary functions" such as an app merely sending a crash report. Reuben Binns, the computer scientist who led the study, says, "Nobody has disputed that the third parties we identify in the study are capable of tracking user behaviour across multiple apps. This includes when data is used for analytics, crash reporting or – as in 60% of apps with Google's DoubleClick tracker embedded – behaviourally targeted advertising."

On the Web, trackers can log information about what you search, click and type. A variety of browser tools (like Privacy Badger, Ghostery or Lightbeam) exist to see who is tracking you. You can also block access to third party trackers or tracking cookies (see Brave or Firefox, Chrome or Safari) though this usually also means blocking ads because they have the capability to track.

On mobiles, users can turn off or reset advertising identifiers that track them across apps, similar to blocking cookies on the Web. But since many users have no idea this tracking is occurring across apps, they also don't know they can take control.

In the case of Google, they control what apps are available in the Google Play Store for the Android operating system *and* also benefit from the data

generated by those apps. The Oxford University study found that Alphabet is the ultimate owner of several subsidiaries that together were found to have trackers in more than 88 % of the analyzed apps.

New research on smartphones sold by more than 200 different vendors points to an additional risk of invasive data collection with some apps that are pre-installed by manufacturers. "Users are clueless about the various data-sharing relationships and partnerships that exist between companies that have a hand in deciding what comes pre-installed on their phones," says the study, while calling for more transparency and real opportunity for consent about data collection.

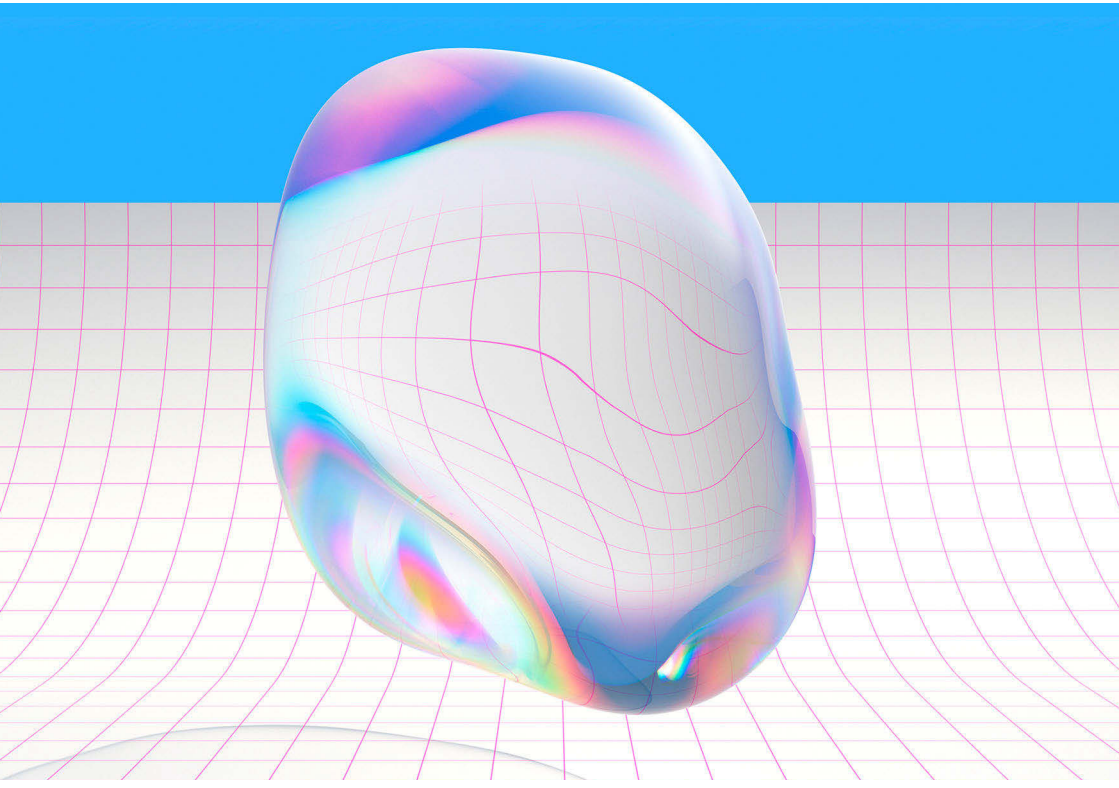
Privacy protections *could* be built into phones from the start, but they are not. With an app ecosystem that is designed for maximum data collection behind the scenes we should not be surprised. As more of us wake up to privacy risks online, we also need to recognize the privacy risks of the smartphones that are now so important to our lives. Knowing is half the battle.

► Further reading

- AppCensus. https://www.appcensus.io/
- Third Party Tracking in the Mobile Ecosystem by Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt, Proceedings of the 10th ACM Conference on Web Science, 2018. https://arxiv.org/abs/1804.03603
- Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, The New York Times, December, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html
- An Analysis of Pre-installed Android Software, Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador and Narseo Vallina-Rodriguez, 2019. https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf

How open is it?

Understand the issue: Openness



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

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.

First layer: 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.

Second layer: 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.

Third layer: 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.

See interactive visualization on the Internet Health Report 2019 website.

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?

Katarzyna Szymielewicz: 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?

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?

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. https://crackedlabs.org/en/networksofcontrol
- Data Ethics – the new competitive advantage, Gry Hasselbalch and Pernille Tranberg, 2016. https://dataethics.eu/wp-content/uploads/DataEthics-UK-original.pdf
- The Age of Surveillance Capitalism by Shoshana Zuboff review – we are the pawns, The Guardian, 2019. https://www.theguardian.com/books/2019/feb/02/age-of-surveillance-capitalism-shoshana-zuboff-review
- Your digital identity has three layers and you can protect only one of them, Quartz, 2019. https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/

► Further listening

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

Internet slowdowns are the new shutdowns

"Imagine you're on a flight. You don't know when you will arrive. You're perpetually stuck in the air until the pilot decides to land." That's how Berhan Taye from Ethiopia describes the strange limbo of an internet shutdown. She leads the #KeepItOn campaign of Access Now, which brings together a coalition of organizations to keep the internet open and accessible.

Around the world, internet shutdowns are on the rise. In 2018, Access Now documented 188 shutdowns around the world. That's more than double what they counted in 2016. Most shutdowns occurred in Africa and Asia, with India being the worst offender.

Official justifications range from cracking down on terrorism, social unrest or false political rumors, to the curbing of cheating during school exams. Other times, authorities simply deny a shutdown or offer no expla-

nation at all. Each case is different, but every time the internet is shut down, peoples' rights are denied. In Cameroon, the government completely blocked Anglophone regions from accessing social media for 230 days. In Chad, citizens have not been able to freely access Whatsapp, Facebook and Twitter for nearly a year. Blocking like this is another way that many governments have been trying to subtly censor access to information without attracting the attention of a full network shutdown.

Recently, Taye says, governments, police and local authorities have become more tactical about how they block people from getting online, moving from internet shutdowns to slowdowns to further obscure who is responsible.

Q: What is it like to experience an internet shutdown?

Berhan Taye: With #KeepItOn we've begun collecting and sharing more personal stories of shutdown experiences because people have a hard time understanding the human impact. Internet shutdowns don't just happen on a random Tuesday. They tend to happen in the context of election violence, protests, or emergencies. That's one reason it can be such a traumatic experience. We've heard from people in the Democratic Republic of Congo, who were unable to verify if family members were alive. We also know of cases in Cameroon where doctors working with the World Health Organization were providing emergency medical advice to patients over WhatsApp. With no internet, there was suddenly no way for them to administer care.

In shutdowns, people's lives are more than just inconvenienced at work, in school, and at home. Their lives can be endangered. In Pakistan, a woman was struck down in traffic by a hit-and-run driver. She tried to call emergency services but the whole mobile network was down. She passed out and almost bled to death. Can you imagine what that must feel like?

Q: How are authorities getting smarter about shutting down the internet?

If we take the example of Ethiopia, where I am from – the first time they shut down the internet, it was like they didn't know what they were doing. They took us off the grid completely. That was extreme, and the economic cost was huge. So the next time they said, 'OK, we're just going to shut down mobile data' since shutting down broadband affects businesses more.

Governments also realize that they can limit a shutdown to a specific city or region now. This is very common in Pakistan and India. It's rare to see a national outage anywhere in the world. And when it's just a neighborhood or small city that is affected, it's harder to document.

Making shutdowns harder to document seems to be the main reason many governments are now opting to simply slow down the internet. It can be slow to the point where it can take a whole day to upload one photo to Twitter, but still be really hard to figure out whether someone is tampering with the internet. For instance in Togo or Cameroon, in countries that don't have the best infrastructure, it might just be that your bandwidth is having a bad day.

For the global community of technologists working to figure out how to spot, measure and analyze shutdowns, slowdowns are an especially big challenge. We can often use data from the Open Observatory of Network Interference (OONI) to confirm if a website is blocked or a shutdown took place, but it's much harder to verify if a deliberate slowdown is happening.

Q: What needs to happen to address these problems?

What keeps me up at night, are the shutdowns we are *not* able to document or understand why happen. Internet shutdowns and human rights violations go hand in hand. In some contexts when we're unable to document shutdowns, egregious human rights violations have happened. That's why we also need more tech companies to come on board with detection and documentation efforts. Google and Facebook are the first ones to know when the internet goes down because practically everyone uses their services. I feel they could be more open about sharing data about internet interruptions with us, and with people around the world.

► Further reading

- Open Observatory of Network Interference (OONI). https://ooni.torproject.org/
- Measurement Lab. https://www.measurementlab.net/
- Netblocks. https://netblocks.org/
- Oracle Internet Intelligence Map. https://map.internetintel.oracle.com/

Taxing social media in Africa

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. Meanwhile, it's a fact that popular OTT services have helped fuel the uptake of mobile internet, and enabled local businesses to operate more efficiently. They have been critical to creating a virtuous cycle of record growth in internet use, network investments, and also telco profits.

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. http://pollicy.org/wp-content/uploads/2019/01/Offline-and-Out-of-Pocket.pdf
- Taxed, throttled or thrown in jail: Africa's new internet paradigm, Global Voices, 2019. https://globalvoices.org/specialcoverage/taxed-throttled-or-thrown-in-jail-africas-new-internet-paradigm/
- Eastern Africa: New tax and licensing rules for social media threaten freedom of expression ARTICLE 19, 2018. https://www.article19.org/resources/eastern-africa-new-tax-and-licensing-rules-for-social-media-threaten-freedom-of-expression/
- Challenges and opportunities for advancing internet access in developing countries while upholding net neutrality, Nanjira Sambuli, 2016. https://www.researchgate.net/publication/302555638_Challenges_and_opportunities_for_advancing_Internet_access_in_developing_countries_while_upholding_net_neutrality

Tracking China's censorship of news on WeChat

In China today, it is nearly impossible to live life without WeChat. What began as a chat app, similar to WhatsApp or Facebook Messenger, has become an essential tool for everything from reading the news to paying for your morning beverage of choice.

After Facebook, WeChat is the most popular social media service in the world. The company now boasts more than 1,0825 billion individual users, along with more than 20 million registered public accounts. These public accounts are where many people in China get their everyday news and information. While many news outlets still maintain their own websites, virtually all media in the country also use WeChat as a publishing platform. Some publish their stories only to their WeChat pages, where followers can comment or discuss the stories of the day.

But of course, not all comments – or even media stories – are permitted to stay online. With its massive user base and powerful social influence, WeChat has become a major implementer of China's rigorous censorship regime. What is published on WeChat – and what the company censors at the state's behest – is a powerful indicator of government concerns about sensitive political issues.

With no transparency about what is censored or why, citizens and researchers are left to speculate and guess where the red lines are drawn.

A group of researchers at the University of Hong Kong have been working to track technical censorship on WeChat, using an innovative Web "scraping" system that captures millions of posts from the platform's most popular public accounts and makes them available to others in formats that can be visualized, mapped and understood in the context of time.

Summarizing the WeChatscope project in a story for Global Voices, Marcus Wang and Stella Fan explained their approach:

"Our team tracked more than 4,000 public accounts covering daily news through our computer program which visits (and periodically revisits) published articles and records the contents. When the system sees that a post has disappeared, it is detected as censored. A copy of the post is then restored in the database and made available for public access."

By the end of 2018, the group had identified roughly 11,000 posts that had been censored. These posts reflected some of the hottest and most controversial media stories and scandals of the year, ranging from the China-US

trade war, to tax fraud allegations against X-Men actress Fan Bingbing, to the #metoo movement at universities across China.

Explaining the context and possible reasons for censorship to a global audience is the subject of an article series on Global Voices, written in English and translated into multiple languages by volunteers. The stories describe in vivid detail how online speech in Chinese platforms can often initially be as vibrant, argumentative or controversial as elsewhere – despite censorship.

The WeChatscope project sheds light on what often feels like a black box of censorship policies and practices that are crafted and carried out by the Chinese government – and the companies required to comply with state demands. It also offers new possibilities for tech experts inside and outside the country to seek new ways to circumvent censorship in China.

► Further reading

- WeChatscope. http://wechatscope.jmsc.hku.hk/
- WeChatscope articles on Global Voices. https://globalvoices.org/author/wechatscope/
- What do Xi Jinping and Winnie the Pooh have in common? They're both flagged by Chinese censors, Shan Wang, Nieman Lab, 2018. https://www.niemanlab.org/2018/03/what-do-xi-jinping-and-winnie-the-pooh-have-in-common-theyre-both-flagged-by-chinese-censors/

Inside Germany's crackdown on hate speech

At the heart of the dilemma about what to do about the plague of hateful and harassing comments online, are questions of free speech, local laws and who should decide what can be said by whom.

Historically, internet companies have benefited from well established safe harbors from liability for the speech of their users, an approach that has helped enable the Web to become the creative and impactful environment it is today. However, hate speech and harassment have flourished online, and efforts by global platforms like Facebook, YouTube and Twitter to respond have been inconsistent and largely ineffective.

Germany (with a population of nearly 83 million people) recently thrust itself into the global spotlight on this question, implementing a law in 2018

intended to reduce hate speech and defamation online. The law introduces steep fines for popular social media companies if they do not take down manifestly unlawful content within 24 hours of a notification, and other unlawful content within up to seven days.

The Network Enforcement Act (NetzDG) was praised by some politicians as an important measure to curb hate speech and vehemently opposed by others. It was widely criticized by digital rights groups concerned about threats to free speech and overbroad takedowns. From abroad, it was observed with glee by governments who limit free speech. Russia, Venezuela and Kenya are among countries who quickly designed their own versions of the law.

In Germany, one year after implementation, the new law seems to be neither particularly effective at solving what it set out to do, nor as restrictive as many feared. However, without more insight into the kinds of notices that are being sent and the methods and guidelines platforms have adopted to handle them, it's difficult to assess the real impact.

NetzDG was designed to put the onus on companies to moderate content and remove it quickly. Germany's Federal Office of Justice can fine companies up to 50 million Euros ($56.3 million USD) if platforms fail to comply with valid removal requests by users or authorities. After the law was passed, Facebook and Twitter said they hired additional moderators in Germany to review content flagged as problematic by users or algorithms.

To comply with the law, Facebook, Google+, YouTube and Twitter each published reports in July 2018 and December 2018 detailing how they enabled users to file complaints and how they dealt with those complaints. So far, the number of content takedowns reported by platforms appears low compared to the number of complaints received.

Twitter, for example, said they received 256,462 complaints between July and December 2018 and took action on just 9%. Facebook said they saw 1,048 complaints and took down just 35.2% of reported content. What these complaints were about, or why so many were rejected, is unknown. Independent researchers have no access to raw data, and there is no standardized reporting process between platforms. The numbers are open to interpretation from every angle.

"If we want to better understand how companies make decisions about acceptable and unacceptable speech online, we need a more granular understanding of case-by-case determinations," wrote researchers from Germany's Alexander von Humboldt Institut für Internet und Gesellschaft in reac-

tion to the reports. They call for greater transparency and insight in order to understand what the effect of the law has been: "Who are the requesters for takedowns, and how strategic are their uses of reporting systems? How do flagging mechanisms affect user behavior?"

While most platform content rules are understood to be based on terms of service, community guidelines and other user policies, relatively little is communicated directly by platforms about how they enforce their own rules on prohibited content.

In Germany, an opportunity to come out of a contentious and politicized debate about harmful content with greater knowledge and better solutions has so far not materialized. Greater transparency around the sources of hateful and violent speech online, who reports it and how takedowns are approached by intermediaries would be an important step toward understanding how to foster a healthier internet for all.

▶ Further reading

- Removals of online hate speech in numbers; Kirsten Gollatz, Martin J. Riedl and Jens Pohlmann, Digital Society Blog, 2018. https://www.hiig.de/en/removals-of-online-hate-speech-numbers/
- Germany's NetzDG: A key test for combatting online hate, Olivia Knodt of the Counter-Extremism Project (CEP) and William Echikson of the Centre for European Policy Studies (CEPS), 2018. https://www.ceps.eu/system/files/RR%20No2018-09_Germany%27s%20NetzDG.pdf

Wikidata gives wings to open knowledge

How do voice assistants like Alexa and Siri know so much? How can search engines tell you the height of Mount Kilimanjaro (5,895 meters) so quickly and so accurately? Now more than ever, it is because they have access to more than 60 million open data records via Wikidata.

Wikidata is a project of Wikimedia, the non-profit organization that also runs the online encyclopedia Wikipedia. For six years, volunteer contributors to Wikidata have been structuring data so that it can be read and edited by both humans and machines.

This ensures that information can fly freely between the Web and other technology platforms. As more people interact with the internet, not just through the Web and websites like Wikipedia, but through speaking and listening to devices, this is becoming increasingly important.

Machines can understand Wikidata because it parses information you would normally read in a Wikipedia article into separate blocks. For example: "Paris is the capital city of France." "Paris has a population of 2,206,488." "Paris' coordinates are 48°51'23.68"N, 2°21'6.58"E."

By structuring this information and giving every entry a unique ID, Wikidata gives more than 5,000 websites, archives, libraries and databases a shared backbone: if you update one entry, other entries where the information is referenced will automatically be updated too, in every language.

Wikidata isn't the only initiative to organize, or try to organize, the Web's data. Similar projects have struggled due to its vastness. So what makes Wikidata successful? "Community is the biggest asset for Wikimedia," says Lydia Pintscher, Wikidata's Product Manager. "Without our partners and contributors, and the people who use the data, it wouldn't be there."

Indeed, Wikidata's community of tens of thousands of volunteer contributors have provided more than 850 million collective edits over the years.

Wikidata is also unique in that it is a completely open public domain resource: Their application of the Creative Commons CC0 Public Domain Dedication to all of Wikidata's data enables people and companies to use Wikidata freely and without copyright restrictions for whatever they like, from voice assistants to search engines.

For Wikidata, this open-access, no-citation approach means people benefiting from its information usually won't know where it comes from – or, that Wikidata depends on volunteers and donations to conduct its work, including updates and quality controls.

For big tech companies offering services on top of Wikidata and other Wikimedia properties, it ups the duty for them to help sustain the resource for everyone. "As companies draw on Wikipedia for knowledge – and as a bulwark against bad information – we believe they too have an opportunity to be generous," wrote Wikimedia's executive director, Katherine Maher, in an op-ed in WIRED in 2018 calling for companies to pay back to the community.

Companies including Google, Amazon and others have met this call to varying degrees (Amazon naming Wikipedia as part of the reason for Ama-

zon Alexa's success) but the vast majority of Wikimedia's resources come from donations by more than six million individuals who on average give $10 USD. In 2018, only 4 % of funding came from corporations.

For the health of the internet, open access to knowledge and information is essential. For institutions, companies, organisations and individuals with small and large data sets to share with the world, Wikidata is where it can really grow wings.

► Further reading

- A Brief Introduction to Wikidata, Björn Hartmann, Towards Data Science, April 2018. https://towardsdatascience.com/a-brief-introduction-to-wikidata-bb4e66395eb1?gi=d6b5aad15e2a
- Wikidata Tours. https://www.wikidata.org/wiki/Wikidata:Tours
- Amazon Owes Wikipedia Big Time, Slate, 2018. https://slate.com/technology/2018/10/amazon-echo-wikipedia-wikimedia-donation.html

"Deepfakes" are here, now what?

In a 2018 video, Barack Obama looked into the camera and warned: "We're entering an era in which our enemies can make it look like anyone is saying anything, at any point in time. Even if they would never say those things."

The video looks and sounds like Obama. But Obama never said those words.

The video is actually a *deepfake*: a photo, video or audio clip manipulated using AI to depict a person saying something that they have never said, or doing something they have never done.

The Obama deepfake was a project by filmmaker Jordan Peele and BuzzFeed CEO Jonah Peretti, intended to warn the public about misinformation online. Using free tools (and the help of editing experts) they superimposed Peele's voice and mouth over an existing video of Obama.

This kind of technology has long been available to Hollywood filmmakers. But in the last two years, it has taken a giant leap forward in accessibility and sophistication.

Deepfakes gained mass notoriety in 2018, with a wave of manipulated videos that used AI to put celebrities' faces onto porn actors' bodies. The term

deepfake itself comes from the handle of a Reddit user – Deepfakes – who made these kinds of videos and started the /r/deepfakes subreddit to share them.

The rise of deepfake porn prompted decisive responses from some platforms, several of which classified it as non-consensual pornography. The /r/deepfakes subreddit was banned in February 2018 for this reason.

But the name *deepfake* stuck. Possibly because it seems to make sense: 'deep' referring to 'deep learning' techniques used to create the media, and 'fake' referring to its artificial nature.

The technology is not only getting more accessible, but its applications are also expanding in multiple directions including producing full body deepfakes, creating real-time impersonations and seamlessly removing elements from videos. Concern is growing worldwide about the negative impacts that deepfakes could have on individuals, communities, and democracies.

The potential for harm is real. But Sam Gregory, Programme Director at the human rights organization WITNESS, says that instead of letting fear paralyze us, we need to focus on finding solutions. He published an extensive survey of solutions to malicious usage of deepfakes and synthetic media, based on conversations with experts in the field.

In the category of technical solutions, many platforms, researchers and startups are exploring using AI to detect and eliminate deepfakes. There are also new innovations in video forensics that aim to improve our ability to track the authenticity and provenance of images and videos, such as ProofMode and TruePic, which aim to help journalists and individuals validate and self-authenticate media.

While Gregory believes technical solutions are important, he says that they can't solve the problem alone. "It is vital to ask what communities might be excluded from technical solutions, and who has control over the data," he says. "If tools for tracking provenance become obligatory, they could be weaponized against individuals who can't access them or choose to remain anonymous."

Digital literacy is a critical solution that Gregory says is underexplored: "How do you get people to ask questions when an image looks flawless?" He says it's especially pressing to upskill people working with vulnerable groups and whose work could be negatively affected by deepfake technology, people like journalists and human rights advocates.

Many governments are grappling with how best to deal with online misinformation. But some activists and scholars caution against an outright ban of deepfake technology. They worry that if a law gives government officials the power to decide what is true or false, there is a risk that it might be used to censor unpopular or dissenting views.

Gregory also says civil society should develop a position on what role commercial platforms should play. "In many ways, platforms have the largest opportunity to detect deepfakes because they will have the largest body of training data. We should be clear now as civil society about what we want them to detect, and how we want them to inform the public, governments and key watchdog institutions."

Overall, Gregory cautions us to acknowledge the risks but resist the hype.

"It's good to not be apocalyptic about it, but to use this moment to have a rational discussion," he says, "The greatest harm of deepfakes may be to make people question everything."

► Further reading

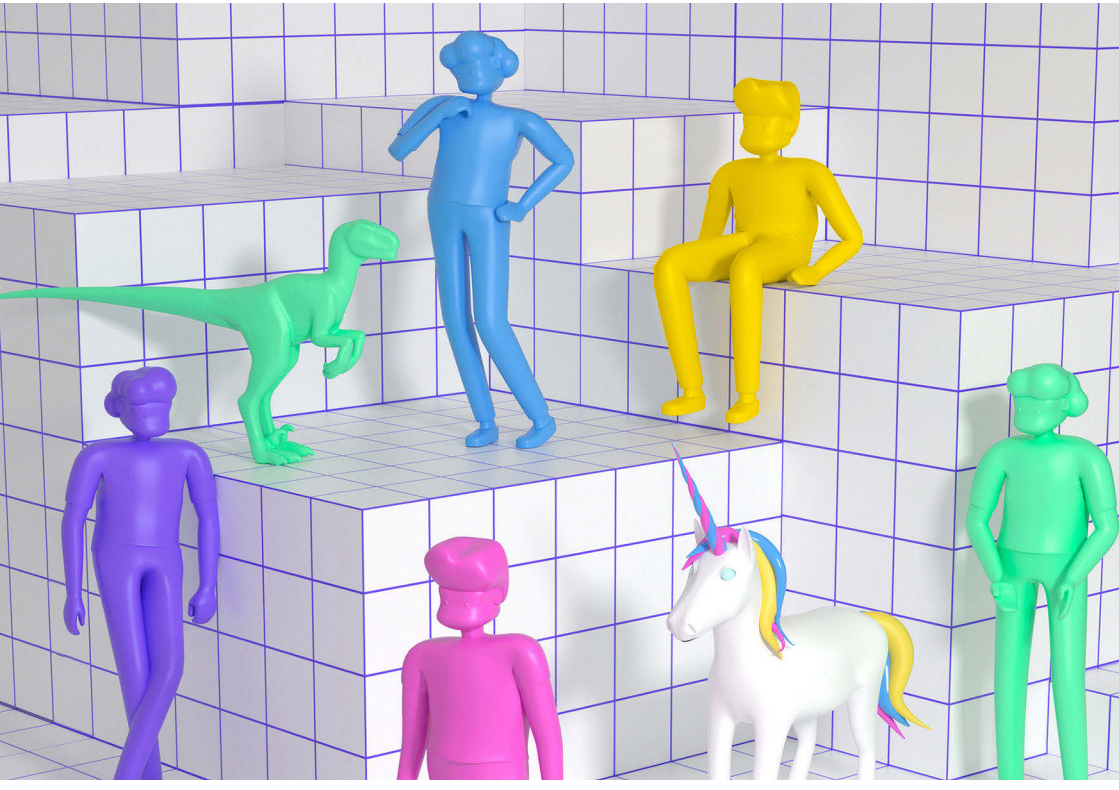
- Deepfakes and Synthetic Media: Survey of Solutions against Malicious Usages, Sam Gregory, WITNESS, July 2018. https://blog.witness.org/2018/07/deepfakes-and-solutions/
- Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, Robert Chesney and Danielle Keats Citron, California Law Review, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954
- Prepare, don't panic: dealing with deepfakes and other synthetic media, Sam Gregory, 2019. https://www.journalismfestival.com/programme/2019/prepare-dont-panic-dealing-with-deep-fakes-and-other-synthetic-media

► Further listening

- Breaking News, Simon Adler, RadioLab podcast, July 2017

Who is welcome?

Understand the issue: Digital inclusion



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 par-

ticular 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.

Recognizing the bias of artificial intelligence

"We have entered the age of automation – overconfident yet underprepared," says Joy Buolamwini, in a video describing how commercial facial recognition systems fail to recognize the gender of one in three women of color. The darker the skin, the worse the results.

It's the kind of bias that is worrying now that artificial intelligence (AI) is used to determine things like who gets a loan, who is likely to get a job and who is shown what on the internet, she says.

Commercial facial recognition systems are sold as accurate and neutral. But few efforts are made to ensure they are ethical, inclusive or respectful of human rights and gender equity, before they land in the hands of law enforcement agencies or corporations who may impact your life.

Joy Buolamwini is the founder of the Algorithmic Justice League, an initiative to foster discussion about biases of race and gender, and to develop new practices for technological accountability. Blending research, art and activism, Buolamwini calls attention to the harmful bias of commercial AI products – what she calls the "coded gaze". To inform the public and advocate for change, she has testified before the Federal Trade Commission in the United States, served on the European Union's Global Tech Panel, written op-eds for major news publications and appeared as a keynote speaker at numerous academic, industry and media events.

On websites and in videos [see "Ain't I a Woman?"] she shares her lived experience and spoken word poetry, about a topic that is more commonly dealt with in dry, technical terms (or not at all).

The "coded gaze" refers to how commercial AI systems can see people in ways that mirror and amplify injustice in society. At the MIT Media Lab's Center for Civic Media, Buolamwini has researched commercial facial analysis systems, illustrating how gender and racial bias and inaccuracies occur. Flawed and incomplete training data, false assumptions and lack of technical audits are among the numerous problems that lead to heightened risks.

To fight back, the Algorithmic Justice League and the Center on Privacy & Technology at Georgetown Law launched a Safe Face Pledge in December 2018. It's a series of actionable steps companies can take to ensure facial analysis technology does not harm people. A handful of companies have signed the pledge and many leading AI researchers have indicated support.

It's one of many initiatives Buolamwini and colleagues are experimenting with to elicit change from big tech companies. So far, she has found that drawing public attention to facial recognition biases has led to measurable reductions in inaccuracies. After Amazon attempted to discredit the findings of her research, leading AI experts fired back in April calling on the company to stop selling its facial recognition technology to law enforcement agencies.

More can be done, she says. "Both accurate and inaccurate use of facial analysis technology to identify a specific individual (facial recognition) or assess an attribute about a person (gender classification or ethnic classification) can lead to violations of civil liberties," writes Buolamwini on the MIT Media Lab blog on Medium.

She says safeguards to mitigate abuse are needed. "There is still time to shift towards building ethical AI systems that respect our human dignity and rights," says Buolamwini. "We have agency in shaping the future of AI, but we must act now to bend it towards justice and inclusion."

▶ Further reading

- Biased Algorithms Are Everywhere, and No One Seems to Care, Will Knight, MIT Technology Review, 2017. https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/
- Response: Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces, Joy Buolamwini, Medium, 2019. https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bi

as-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced
- Lawmakers say Amazon's facial recognition software may be racially biased and harm free expression, Techcrunch, 2018. https://techcrunch.com/2018/11/30/lawmakers-amazon-recognition-racially-biased-harm-free-expression/

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 [see data visual on the 2019 Internet Health Report website].

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.

► Further reading

- "New ITU statistics show more than half the world is now using the Internet", International Telecommunications Union, 2018. https://news.itu.int/itu-statistics-leaving-no-one-offline/
- The Case for the Web, The World Wide Web Foundation, 2018. http://webfoundation.org/docs/2018/11/The-Case-For-The-Web-Report.pdf
- The Mobile Economy, GSMA, 2019. https://www.gsma.com/r/mobileeconomy/

Technology's inhumane underbelly

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 bet-

ter 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. https://goodelectronics.org/
- China Labor Watch. http://chinalaborwatch.org/home.aspx
- A fix to our throw-away technology culture, Internet Health Report, 2018. https://internethealthreport.org/2018/a-fix-to-our-throw-away-technology-culture/
- Worker satisfaction starts with talking to factory employees, Fairphone blog, March 2019. https://www.fairphone.com/en/2019/03/21/worker-satisfaction-starts-with-talking-to-factory-employees/

► Further listening

- Restart Podcast Ep. 24: Goodbye iSlave (Pt 1), The Restart Project, September 2017. https://therestartproject.org/podcast/islave/

A global push to identify everyone, digitally

Governments around the world have different systems for identifying their residents. Many countries are surging ahead to institute digital identity systems for both on and offline purposes. How such systems are designed, and what measures exist to protect citizens from harm, are influenced by not only the government, but the biggest technology companies and global governance institutions like the World Bank.

Digital identity systems aim to combat a big issue for government: an estimated 1.1 billion people in the world lack any form of legal ID. These unidentified people risk exclusion from government services while causing issues regarding accurate population statistics.

The UN acknowledges this problem in its Sustainable Development Goals that has called for "providing legal identity for all" by 2030. This general need for legal identification for all is interpreted by many as a call for all-purpose biometric, digital ID systems, as opposed to physical IDs.

For example, the World Bank's Identification for Development Initiative encourages developing countries to "leapfrog" to biometric and digital IDs to curtail fraud and increase efficiencies. This leap, however, brings with it new risks and concerns and should not be uncritically embraced.

Digital ID systems typically tie together multiple pieces of data about a person, which could include home address, citizenship status, marital status, financial information, and often their "biometrics" (a photo, fingerprints, iris scans or even DNA). This information may be used for everything from collecting tax payments, to allocating food subsidies, to voter identity authentication. These systems may use chip-based smart cards containing biometric data or unique number IDs for those who use mobile-based identification and authentication. Potential linking opportunities within these systems create a powerful tool for mass surveillance.

In practice, many of these systems have not lived up to stated aspirations. They are often built and administered by private companies under opaque government contracts that offer people little, if any, option to identify problems or complain about errors. The consequences of a system like this can be dire, especially for marginalized or vulnerable populations.

India uses an ID system called Aadhaar which has become a mandatory prerequisite for accessing essential public services and benefits like education, healthcare and food subsidies. Yet technical errors and glitches in the system have actually prevented some Indians from accessing vital resources like food subsidies. And in multiple incidents, millions of Aadhaar card holders' private data has been leaked on the internet, leaving personal identification information open for misuse and harm.

In 2017, civil society advocates challenged the Aadhaar scheme on privacy grounds in India's Supreme Court. Although the court ruled unanimously to uphold privacy protections as a fundamental right, the Aadhaar scheme has proceeded apace. Technology and policy experts have worked to expose the security and privacy problems in the Aadhaar system, but their efforts have not been well-received by officials.

India is not the only country that has seen robust civil society resistance to a national ID system. In Kenya, human rights groups took the government to court over its soon-to-be-mandatory National Integrated Identity Management System (NIIMS), which was intended to capture people's DNA information, the GPS location of their home, and more. Kenya's High Court

suspended key components of the plan in April, thanks to these petitions from civil society.

On the other hand, Estonia's digital citizenship program has been lauded for its accessibility, strong (though not flawless) security protections and robust integration with state agencies. It is designed to put control in the hands of users, rather than the ID authority or the requesting entity.

Implemented correctly, ID systems can empower vulnerable and underrepresented populations but it's far from clear that digital (and especially biometric) systems are necessarily the best way to go about this. Without adequate protections, state agencies may use these systems to conduct surveillance, profile voters, or exclude communities. Private companies will have the opportunity to take advantage of the ability to link discrete databases, affecting people's privacy, safety, and online lives in ways that we are only beginning to understand.

For the many national governments still contemplating adoption of a national ID system, these examples should be instructive. Emerging research initiatives seeking to evaluate these systems and their positive and negative effects on people's lives will be instrumental in charting the path forward. For digital ID systems to empower communities adherence to constitutional and international human rights standards, must be baked into their design and implementation from the start.

► Further reading

- Understanding identity systems Part 1: Why ID?, Privacy International. https://www.privacyinternational.org/explainer/2669/understanding-identity-systems-part-1-why-id
- National identity programmes: what's next?, Access Now, March 2018. https://www.accessnow.org/national-digital-identity-programmes-whats-next/

Tech employees power up

In April 2019, Google dismantled its brand-new ethics board for development of artificial intelligence (AI) after just one week. The announcement followed an employee protest staged by thousands of Google staffers who were out-

raged that the board included members accused of discrimination against transgender people, climate change skepticism and the use of artificial intelligence in warfare.

Since early 2017, internal protests like these at Google, Amazon, Microsoft, and other tech companies have spilled into public view. Software engineers, researchers and others with ties to these companies have emerged as a force to help hold them ethically accountable.

#TechWontBuildIt has been a rallying hashtag on Twitter.

As tech companies race to build artificial intelligence for facial recognition and other software and services that may be used by military, immigration and law enforcement authorities, many engineers are keen to ensure that privacy, equality, and safety are part of the equation. As a result, tech companies are beginning to see the loyalty of their employees tested.

At Microsoft and Salesforce, hundreds of employees campaigned in June for a stop on sales of AI to immigration authorities after the children of immigrants were forcibly removed from their parents. Thousands of Amazon employees have called on the company to adopt a more aggressive plan to confront climate change, following another internal protest demanding the company stop selling its racially biased facial recognition software to the US government's immigration department.

For anyone hoping to push the tech giants into alignment on human rights, labor rights, and other common good agreements, tech employees protesting is an exciting development.

But it's a precarious approach for those involved. There's discord among employees, the threat of reprisals from superiors, and the risk of public exposure and harassment.

Even if a majority of employees were to agree on an issue, companies don't operate like democracies. Still, a growing number of people are feeling the urgency to raise their voices and have also seen clear results from their organizing.

One of those (now former) employees is Liz Fong-Jones, who left Google in early 2019. She'd joined the company at the beginning of 2008, inspired by their mission to organize the world's information and make it universally useful and accessible. Over the years, she helped employees hone in on a playbook for how to turn outrage over ethically questionable practices into an organized counterposition, for instance in 2010 on the "real name" policy for Google Plus.

Using the company's own flagship communication tools, employee-organizers inside Google have repeatedly managed to rally their colleagues to stand up for the company's ideals when management has failed to. "You have to be 120% good at your day job to defend yourself against blowback, or to generate the room in your schedule to work on it," Fong-Jones says.

Their largest action yet came in October 2018, when employees of Google led a 20,000-employee-strong "Walkout for Real Change" to protest the company's misconducts on sexual harassment. The action generated awareness and a wave of headlines. Employees won a partial victory within a week of the walkout, which resonated further when Facebook, eBay and Airbnb immediately followed Google's lead in ending the contractual practice of "forced arbitration" and opening up for the possibility of lawsuits from employees for discrimination or wrongful termination.

And yet, in Fong-Jones's view, Google didn't seriously consider the walkout's core demands. The arbitration victory only applies to current full-time employees, not temps, vendors, and contractors. Most critically, in Fong-Jones's view, management sidestepped their demand for an employee board seat. She left the company after fighting for 9 years, but still advocates that tech employees will find more leverage in broad collective action, like a strike, than via a smaller number of resignations.

For her part, Fong-Jones is continuing to build power for tech employees. When news leaked that Google is building a censored search engine in China, she launched (and matched donations to) a strike fund that has raised over $200,000. The fund intends to support economically vulnerable Google staff (like those on work visas) who join a strike, or resign, in an organized response to perceived concerns with the company's conduct.

Software and algorithms reflect the biases of their creators, which is one reason why diversity and equality among the people who work for the biggest internet companies matters to internet health. With new technologies, including AI, having an even greater impact on our lives and carrying even bigger risks for vulnerable populations, it's important for companies to hear from a diverse employee base – and *listen* when they sound the alarm. As advocates for a healthier internet grapple with how to push for change, it appears many tech employees are ready allies.

► Further reading

- Code Red, Organizing the tech sector. https://nplusonemag.com/issue-31/politics/code-red/
- Video and podcast: Moira Weigel discusses the new tech worker movement at the Berkman Klein Center for Internet & Society. https://cyber.harvard.edu/events/2019-02-26/goodbye-california

Women journalists feel the brunt of online harassment

It's a fact proven by numerous studies worldwide: women and nonbinary people are more affected by online harassment than men, especially if they are also people of color. When it happens in the context of journalism, it sends an especially damning message that women and minorities have no right to a public voice. Threats of sexual violence and other intimidation tactics threaten the diversity of voices in the media and healthy online dialogue.

Women have long been outnumbered in journalism worldwide. Now, in addition to discriminatory hiring practices and other barriers, personal attacks in online comments, social media posts, emails and more, represent a serious threat to diversity. Because of online harassment, several studies show that women journalists experience depression and anxiety, avoid engaging with readers, reporting on certain topics, or say they consider leaving journalism altogether.

Nearly two-thirds of female journalists surveyed by TrollBusters and the International Women's Media Foundation in 2018 said they had experienced online harassment. Though media contexts differ, there are many similarities to how harassment is experienced worldwide. True everywhere, is that attackers are rarely held accountable – whether they are individuals acting alone or as part of orchestrated attacks by governments or groups who weaponize social media. What is worse, people in positions of authority often encourage an escalation of attacks.

A 2018 report by Reporters without Borders on the online harassment of journalists worldwide, documents many such cases, including that of Maria Ressa, the founder and executive editor of the news website Rappler in the Philippines. In the context of government attacks on Rappler's reporting, Ressa says she regularly receives online threats of rape, murder and arrest in

social media. She has made a point of publicly exposing attackers and refusing to be silenced.

Even in countries that are relatively safe for journalists or where free speech is protected, receiving hateful comments is the norm for many female journalists, whether they cover sports, fashion or politics. An analysis of 70 million reader comments on The Guardian newspaper from 2006–2016 shows that articles written by female journalists saw a higher proportion of comments rejected by moderators, especially in news sections with a high concentration of male writers, like "Sport" or "Technology" [see data visual on the Internet Health Report 2019 website].

As the methods of online harassment differ, so must the responses. News organizations can help set standards for meaningful and positive dialogue on their own websites and social media channels, and display zero tolerance to discrimination and harassment in comments. They should also offer support to journalists and freelancers before and after harassment happens.

Social media amplifies the volume and intensity of attacks on journalists, not least when platforms become vehicles for state-sponsored attacks. Large platforms have a responsibility to help curb harassment globally, but companies and governments who aim to get to grips with online hate speech can also overreach and undermine free speech. Solutions to online harassment should be developed with care, in dialogue with organizations who represent affected people, as well as with researchers who understand the nuances of the problems.

► Further reading

- "It's a terrible way to go to work:" what 70 million readers' comments on the Guardian revealed about hostility to women and minorities online, Becky Gardiner, Feminist Media Studies, 2018. https://doi.org/10.1080/14680777.2018.1447334
- Attacks and Harassment: The Impact on Female Journalists and Their Reporting, Michelle Ferrier, International Women's Media Foundation and Trollbusters, 2018. https://www.iwmf.org/attacks-and-harassment/
- Online harassment of journalists: the trolls attack, Reporters without Borders, 2018. https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf

- Trolls and threats: Online harassment of female journalists, Al Jazeera, 2018. https://www.aljazeera.com/programmes/listeningpost/2018/10/trolls-threats-online-harassment-female-journalists-181006101141463.html

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 homogenous 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 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, socio-eco-

nomic 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."

The world's slowest internet is the least affordable

More than half of the world's population is now online, but access alone says nothing about the quality and affordability of that internet experience. The speed of internet access is as important to overcoming digital divides as providing affordable access in the first place.

For entire countries, rural regions or individual house blocks, whether the internet is fast can determine who can stream movies and music, take online courses, manage finances or conduct work online – and who is excluded from those opportunities.

It's a sad fact that the slowest mobile broadband internet in the world also happens to be the least affordable. A 2018 report by the Alliance for Affordable Internet (A4AI) found that world regions where people on average pay the most for mobile broadband internet relative to their average monthly income also contend with the slowest download speeds (in Mbps).

A4AI call this a "double barrier to meaningful internet access".

Internet access is considered affordable by the A4AI when 1GB of mobile broadband data is priced at 2% or less of the average monthly income.

Using data from M-Lab, an open source platform to test internet speeds, the A4AI report shows how Africa, for instance, has both the least affordable *and* slowest internet in the world. The median download speed in Africa was found to be less than a seventh of that in Europe [see data visual on the 2019 Internet Health Report website].

Loading a video on YouTube is practically instantaneous in most of Europe – for internet users in some regions of Africa, Latin America or Asia where the internet is slow, the same simple act could be an act of patience, lasting up to several hours.

Both geography and policies can contribute to less affordability and slower internet speeds. For example, smaller countries or regions that are less populated can face higher costs because they have less opportunity to realize economies of scale.

Island nations can face additional challenges because they may need to deploy undersea internet cables for both domestic and international connectivity. In a country comprised of multiple islands, like the Philippines, providing mobile broadband access requires multiple undersea cables and multiple cable landing points, which increases the complexity and cost.

A4AI suggests that to bring down prices for consumers, regulators must incentivize healthy market competition, establish clear and enforceable rules, promote transparency standards, conduct public consultations and develop region-specific strategies. In Colombia, for example, Quality of Service (QoS) regulations to ensure better internet speeds have been conducted in a participatory manner involving the government, operators, civic groups and consumers.

Guaranteeing global minimum standards of internet speed and reliability, as well as affordability, requires long-term planning and engagement among policymakers, regulators and operators to meet the unique challenges of individual countries.

► Further reading

- New mobile broadband pricing data reveals stalling progress on affordability, Alliance for Affordable Internet, 2019. https://a4ai.org/new-mobile-broadband-pricing-data-reveals-stalling-progress-on-affordability/
- Improving Mobile Broadband Quality of Service in Low- and Middle-Income Countries, Alliance for Affordable Internet, 2018. https://a4ai.org/research/improving-mobile-broadband-quality-of-service-in-low-and-middle-income-countries/
- 2018 Affordability Report, Alliance for Affordable Internet, 2018. https://a4ai.org/affordability-report/report/2018/

Who can succeed?

Understand the issue: Web literacy

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.

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 pornogaphy, 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. https://ioelondonblog.wordpress.com/2019/03/17/10-years-on-why-we-still-need-better-sex-education-for-the-digital-world/
- What Teenagers Are Learning From Online Porn, New York Times, 2018. https://www.nytimes.com/2018/02/07/magazine/teenagers-learning-online-porn-literacy-sex-education.html
- Porn and sex education, porn as sex education, Kath Albury, UNSW Sydney, 2014. https://www.researchgate.net/publication/264558246_Porn_and_sex_education_porn_as_sex_education
- 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. https://www.mdpi.com/2076-328X/6/1/1

Who babysits your children's data?

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. https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/
- I'm 14, and I quit social media after discovering what was posted about me, Fast Company, 2019. https://www.fastcompany.com/90315706/kids-parents-social-media-sharing
- Sharenting: Children's Privacy in the Age of Social Media, Stacey B. Steinberg, University of Florida Levin College of Law, 2017. https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub
- YouTube Is Improperly Collecting Children's Data, Consumer Groups Say, New York Times, 2018. https://www.nytimes.com/2018/04/09/business/media/youtube-kids-ftc-complaint.html

Decoding images of war in Syria

In the hands of human rights defenders working to protect and seek justice for vulnerable people worldwide, the internet is a powerful tool. Amnesty International harnessed this potential by creating the Decoders: a community of over 50,000 online volunteers from more than 150 countries, who donate their time and skills to support human rights research.

Decoders projects break research into microtasks that anyone with an internet connection can complete, making massive jobs more manageable by distributing them among a very large group.

The Decoders played a crucial role in Amnesty International's recent investigation into civilian deaths in Raqqa, Syria. The global network of digi-

tal volunteers was activated to help prove beyond any doubt the extent of the destruction in the city.

Raqqa was once the sixth largest city in Syria and home to over 200,000 people. Over the course of four months in 2017, large parts of it were turned to dust. Air strikes and artillery bombardments rained on the city from June to October in a military operation by a US-led coalition to oust the terrorist organization Islamic State (IS) from Raqqa in the context of civil war in Syria.

From the start, human rights organizations including Amnesty International and Airwars, warned that civilians were dying. By the time the coalition declared victory, nearly 80 % of Raqqa was destroyed. Hundreds of civilians were killed and thousands were injured.

But in the initial aftermath of the battle, the coalition acknowledged only 23 civilian deaths. Human rights organizations were outraged. "We can't have a situation … where they wash their hands of it," said Conor Fortune, Senior Communications Adviser on the Crisis Response team at Amnesty International, "We want justice for these people."

In an effort to document civilian casualties, Amnesty International investigators surveyed the destruction on the ground, interviewed hundreds of survivors, gathered evidence from social media, and conducted expert military and geospatial analysis.

The Decoders would tackle a very specific problem for the investigation: Amnesty International wanted to know precisely when each building in the city had been destroyed.

Destroying a building, even one with civilians inside, is not a violation of the laws of war. But a timeline of the city's destruction could be combined with the other evidence Amnesty and partner organizations were gathering to more accurately depict the number of civilian casualties.

For the crowdsourced research, Amnesty created Strike Tracker: an online application where anyone could look at a timeline of satellite images on a mobile phone or laptop, to help pinpoint the dates before and after each individual building's destruction in Raqqa.

Over 3,000 volunteer Decoders logged on to help. Together, they spent over 4,000 hours combing through 2 million photos, and identified the dates of when over 11,200 buildings were destroyed. With creativity, rigor and technical expertise, Amnesty's Decoders demonstrates how online activism can go beyond 'liking' posts or signing petitions, to offering more people opportunities for safe, meaningful participation in real human rights investigations.

Conducting research of this scale, particularly within Amnesty International's time frame and resource limitations, would have been next to impossible without the internet, digital volunteers, open source crowdsourcing software Hive, and high-quality satellite imagery.

The result of the 18-month long investigation into Raqqa is an online multimedia platform that combines the Decoders' work with research and evidence collected by Amnesty, Airwars and other partners. These combined efforts help demonstrate the scale of destruction, and have caused the coalition to revise the number of civilian deaths it acknowledges.

The actions of online volunteers around the world exist alongside countless examples of online activism, blogging, storytelling and photography pioneered by Syrians themselves throughout the conflict. In so many ways, from inside and outside the country, the internet can be a lifeline to communicate unimaginable human loss, devastation and cries not to be forgotten.

► Further reading

- Amnesty International, Decoders Strike Tracker. https://decoders.amnesty.org/projects/strike-tracker
- Nowhere to Run: Trapped in Raqqa, Syria, Amnesty International Report, 2017. https://raqqa-syria.amnesty.org/
- Syrian Archive. https://syrianarchive.org

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. https://ourdataourselves.tacticaltech.org/projects/data-and-politics/
- Digital Deceit: The Technologies Behind Precision Propaganda on the Internet, Dipayan Ghosh, Ben Scott, New America, 2018. https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/
- A multi-dimensional approach to disinformation, Independent high level group on fake news and online disinformation, European Commision, 2018. https://publications.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en
- Elections – Global Voices. https://globalvoices.org/-/topics/elections/

Spot the surveillance with virtual reality

Virtual reality (VR) is often associated with entertainment: With a VR headset, or even just a smartphone and folded cardboard glasses, you can enter the surroundings of your favorite video game world, or watch a movie as though sitting directly alongside the characters.

But the emerging technology has applications beyond just fun. It's used in classrooms for virtual field trips. It's used to train surgeons and astronauts. And it's used for therapy and rehabilitation.

VR can be used for activism too. One example is the Electronic Frontier Foundation's Spot the Surveillance project, which was created in 2018 to help people learn to detect mass surveillance technology in their neighborhoods and spark conversations about privacy.

In Spot the Surveillance, individuals use a VR headset to immerse themselves on a sunny San Francisco street corner. They can turn 360 degrees to fully examine the scene, and are prompted to spot surveillance technology that is embedded in the neighborhood.

Very quickly, users can uncover a range of surveillance devices. There is a PTZ camera mounted on a street light, which livestreams car and pedestrian traffic. There is an automated license plate reader that uploads all the information it captures to a searchable database.

There's a mobile biometric device, which allows police to collect identifying data like fingerprints and iris scans. And up in the clouds, there's a drone that at first glance looks like a bird.

In total, there are seven mass surveillance technologies on just one street corner. It only takes a few minutes to spot them all.

EFF Senior Investigative Researcher Dave Maass explains why EFF created the project: "We made our Spot the Surveillance VR tool to help people recognize these spying technologies around them and understand what their capabilities are."

Of course, mass surveillance isn't an unknown issue. For years, civil society and activists in the United States have sounded off on the dangers of law enforcement overreach, especially in communities of color.

VR provides an immersive window for those who feel far from the issue.

"One of our goals at EFF is to experiment with how emerging online technologies can help bring about awareness and change," says EFF Web Developer Laura Schatzkin, who coded the project. "The issue of ubiquitous police surveillance was a perfect match for virtual reality. We hope that after being immersed in this digital experience users will acquire a new perspective on privacy that will stay with them when they remove the headset and go out into the real world."

► Further reading

- Street-Level Surveillance: A Guide to Law Enforcement Spying Technology, EFF. https://www.eff.org/sls
- How to Stop 'Smart Cities' From Becoming 'Surveillance Cities', ACLU, 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/how-stop-smart-cities-becoming-surveillance-cities
- Teaching encryption in Harlem, Internet Health Report, 2017. https://internethealthreport.org/v01/stories/teaching-encryption-in-harlem/

Breaking free of the addiction machine

Tracking how long we spend online, how many times we pick up our phones, and how many hours we devote to certain apps has become a bit of a global obsession in the news media and within families. If it is true that the aver-

age American adult spends nearly 6 hours per day on digital media should we automatically call this "addiction"? We might question what is "too much" and what is healthy, but we should also resist scaremongering and moral panic about technology and carefully assess claims to scientific certainty when high quality research is lacking.

It's no accident that the time we spend online has increased dramatically over the last decade. And it isn't only because mobile phones and internet connections are becoming faster and more affordable in most parts of the world. Our phones have become our alarm clocks, navigation aids, memory enhancers and constant companions. Smartphone apps and social media are often also explicitly designed to optimize engagement, like comments and shares, and to increase the amount of time we spend, watching, reading, scrolling or playing.

Natasha Dow Schüll calls this "addiction by design". Schüll is an associate professor at New York University, and spent 15 years studying how casinos and slot machines pull people into an addictive "machine zone" that is hard to escape. She and many others see the same design principles being applied in smartphone apps, social media platforms and recommendation engines. Such *intents* on the side of companies have been documented, but there is still inconclusive evidence of how much control they actually wield over users.

To illustrate this point, scientists Amy Orben and Andrew Przybylski at Oxford University examined existing data sets about the relationship between technology use and well-being in young people. The results published in Nature Human Behavior in 2019 show that there is no overwhelmingly consistent correlation – good or bad. Other factors had greater impact.

"In one dataset, for example, the negative effect of wearing glasses on adolescent well-being is significantly higher than that of social media use. Yet policymakers are currently not contemplating pumping billions into interventions that aim to decrease the use of glasses," writes Orben in a behind-the-scenes analysis for the Nature Research Community.

Anecdotally, countless people report feeling anxious, sad or depressed about the way technology has meshed with their lives, or dissatisfied with the terms on which they are offered free services that vacuum personal data. Many actively seek to change their relationships with their devices: Digital detoxes, social media hiatuses, or buying phones that can't go online are

but a few of the tactics that those privileged enough to choose to go offline employ.

One of the most visible organizations working to stop the design of addictive technologies is the Center for Humane Technology, whose co-founder Tristan Harris himself was a design ethicist at Google. Advised by former and current technology executives, the launch of the organization in 2016 (originally named Time Well Spent) helped spark a public debate about the vast potential for harm from technology that is *not* designed with humanity's best interests in mind.

Tech industry leaders responded to a deluge of bad publicity by designing new tools to assist people in managing the time they spend with devices and in apps. In an apparent nod to the organization in 2018, Facebook CEO Mark Zuckerberg announced, "One of our big focus areas for 2018 is making sure the time we all spend on Facebook is time well spent …"

Later that year, Facebook introduced new tools to support "safety" and "well-being", including options to mute notifications for Facebook and Instagram and create time limits. Meanwhile, Apple introduced a new iPhone feature called ScreenTime to help users "understand and take control of the time" they spend with their device. And as part of a digital well-being initiative, Google announced similar controls for Android and YouTube, including an app timer.

But such tools constitute nothing in the way of a change in design practices. Business models that incentivize engagement still reign. As awareness about the questions and potential risks of the current systems grow, so do the ways to help us understand how we're using technology – and make choices about how and whether to do things differently. For instance, one whimsical browser extension, Facebook News Feed Eradicator (for Firefox or Chrome), aims to counteract the lure of social media by replacing your news feed with "an inspiring quote".

But the responsibility for change shouldn't lie with individuals alone.

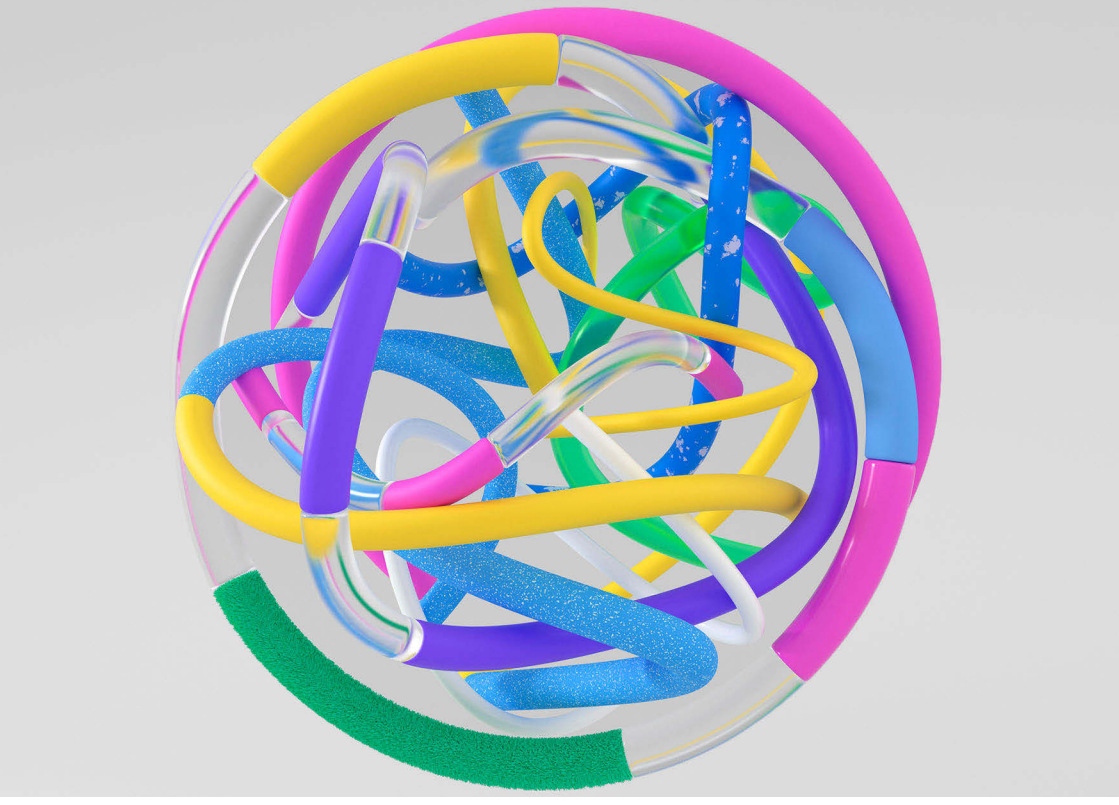
We also need collective action to design different incentives and business models. There is an opportunity for people within the tech sector – developers, designers, content creators, marketers and others – to be leaders in creating apps and services that do not encourage addictive behaviours and instead incentivize positive, healthy online experiences.

► Further reading

- Data Detox Kit, Tactical Tech. https://tacticaltech.org/news/data-detox-kit/
- Three problems with the debate around screen time, Amy Orben, Pete Etchells and Andy Przybylski, 2018. https://www.theguardian.com/science/head-quarters/2018/aug/09/three-problems-with-the-debate-around-screen-time
- Logged off: meet the teens who refuse to use social media, Sirin Kale, The Guardian, 2018. https://www.theguardian.com/society/2018/aug/29/teens-desert-social-media
- Surviving a day without smartphones, Marcello Russo, Massimo Bergami, and Gabriele Morandin, MIT Sloan Management Review, 2018. https://sloanreview.mit.edu/article/surviving-a-day-without-smartphones/

Who controls it?

Understand the issue: Decentralization



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

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, open-

ness 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.

When a hurricane zaps the internet

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. https://www.internetsociety.org/resources/doc/2018/post-hurricane-connectivity-in-the-caribbean/
- After Hurricane Maria, Puerto Rico's Internet Problems Go from Bad to Worse, NOVA Next, October 2018. https://www.pbs.org/wgbh/nova/article/puerto-rico-hurricane-maria-internet/
- Lights Out: Climate Change Risk to Internet Infrastructure, University of Wisconsin – Madison, 2018. https://ix.cs.uoregon.edu/~ram/papers/ANRW-2018.pdf
- Puerto Rico's Slow Internet Recovery, Oracle Internet Intelligence, 2017. https://blogs.oracle.com/internetintelligence/puerto-ricos-slow-internet-recovery

The new investors in underwater sea cables

"The cloud" exists deep under the sea. Although you might first think of satellites and cell towers, before the data reaches your phone or router, it often travels beneath oceans: through a massive, global network of undersea fibre optic cables.

This global submarine cable network is growing, bringing the opportunity of high speed internet to more people, including in remote island nations. But who is building this network?

This network of submarine cables transports petabytes of information around the world on a daily basis, in a manner that is invisible to most users – a huge technical feat. Historically, these submarine cables have been built by telecom carriers, who form consortia to finance the construction of a cable. In the 1990s, undersea cables began to attract investment from private companies, who saw the potential to make a profit by selling capacity to telecom companies and private companies alike [see interactive map and timeline of undersea cables on the Internet Health Report 2019 website].

Today, the investment landscape in undersea cables is shifting yet again. Because they now make up the greater part of undersea cable traffic, internet companies are beginning to finance and construct their own undersea cables. In fact, Google, Facebook, Amazon and Microsoft owned or leased more than half of the undersea bandwidth in 2018. Currently, Google alone owns six active submarine cables, and plans to have eight more ready within two years.

An equally significant driver of investment in undersea cables today are concerns regarding cybersecurity. The Snowden revelations in 2014 exposed the extent of government surveillance of internet infrastructure, including fibre optic cables. Given that 95 percent of the internet's data and voice traffic travels between continents underwater, the corporate and political powers that influence and control the infrastructure can have significant global social and security implications. In this context, physical ownership of undersea infrastructure to mitigate the risk of surveillance is emerging as an investment motivation.

Still, the rapid expansion of the submarine cable network in the last decade was largely fueled by the meteoric increase in demand for internet services. The rapid uptake of cloud computing, connected devices, streaming and countless other services many of us now take for granted – combined

with users' expectation that it all works quickly and smoothly – put major pressure on service providers.

For videos to play and links to open milliseconds after a click, with minimal latency, content needs to be cached as close as possible to users. So companies like Facebook and Google began to build global networks of data centers. To connect those data centers, they not only invest in existing cables, but also increasingly build their own cables to ensure that their services are quickly and readily available anywhere in the world.

It's a new development for online platforms to also be the owners (or co-owners) of the delivery infrastructure. At a time when there is already significant concern about the consolidation of power by the biggest technology companies in multiple realms, and telcos are merging with traditional media companies, it raises questions about who (literally) controls the internet, and how we wish to see it develop in the future. When the same companies own the online platforms and the infrastructure to access them, we have to consider whether the incentives and agreements for sharing access to cables thus far will still make sense.

With so many aspects of our societies and economies relying on the internet – and the undersea cables that power it – we can and should demand that the public has a say in the regulation of this critical infrastructure.

► Further reading

- The Submarine Cable Map, TeleGeography, 2019. https://www.submarinecablemap.com/
- Internet Economics is a Thing and we Need to Take Note, Geoff Huston, 2018. https://labs.ripe.net/Members/gih/internet-economics-is-a-thing-and-we-need-to-take-note
- Internet Drift: How the Internet is Likely to Splinter and Fracture, Steve Song, 2018. https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/
- 'People think that data is in the cloud, but it's not. It's in the ocean', New York Times, 2019. https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html

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.

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.

Q: 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 other local nonprofits. It's a totally different vision for how things can work in an economy.

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

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.

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

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. https://www.orbooks.com/catalog/ours-to-hack-and-to-own/
- Platform Cooperative Consortium. https://platform.coop/
- The Internet of Ownership Website and Directory. https://ioo.coop/
- Why the cooperative models need to be at the heart of our new economy, Fast Company, 2018. https://www.fastcompany.com/90249347/why-the-cooperative-model-needs-to-be-at-the-heart-of-our-new-economy

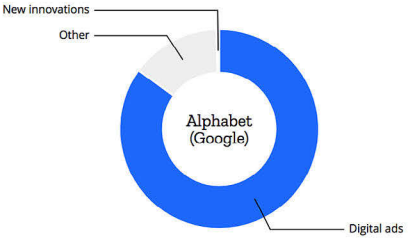
How do the biggest internet companies make money?

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.

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.

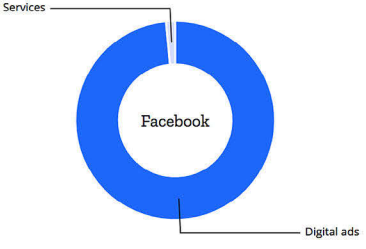


Alphabet (Google)
Google's parent company Alphabet earns 85% of their revenue from digital ads. Around 70% comes from ads on Google's own products, e.g. Google Search or YouTube. Alphabet also owns Google's AdSense and AdMob –– services for placing ads on other websites –– that together account for 14.6% 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

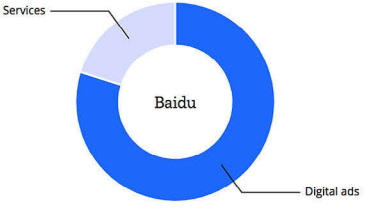


Facebook
We think of Facebook as a "social network," but they are in fact an ad company. With around 2.32 billion monthly active users, Facebook makes more than 98.5% of its revenue — over $55 billion USD — from selling ads that appear in our news feeds, mostly through the Facebook app. A fraction of 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.

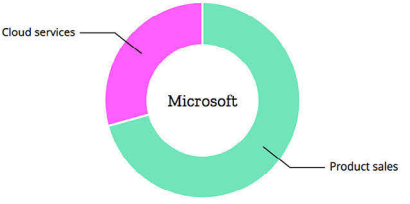
Revenue (2018)
$14.9 billion USD

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.

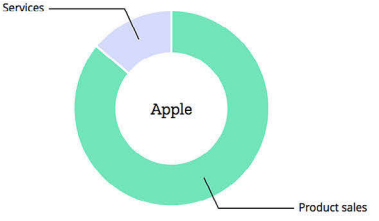


Microsoft
70.8% of Microsoft's revenue is from product sales, but these products span many categories, including "productivity" products like Microsoft Office software and the online recruitment platform LinkedIn. Also in the category of product sales is software (including Windows), hardware (including 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.

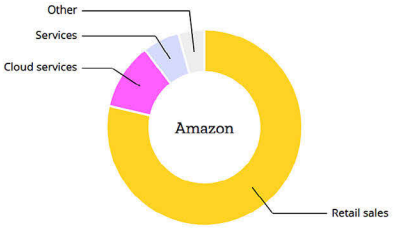
Revenue (2018)
$265.6 billion USD

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!

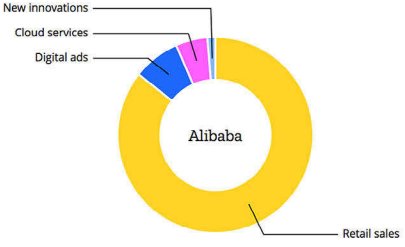


Amazon
It used to be a book business, now it's an everything business. Amazon makes most of its revenue (78.5%) through retail sales. Subscription fees for Amazon Prime (including video streaming) brings in 6% of their revenue. Amazon Web Services brought in 11% of Amazon's total revenue in 2018, an 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 Todou (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.

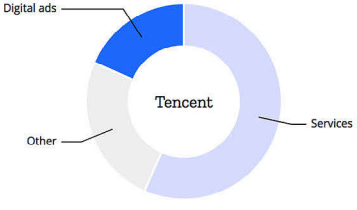
Revenue (2018)
$39.9 billion USD

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

An open source alternative for "the cloud"

Cloud services have become the default tools many people use to get their work done. But this can mean giving up privacy and control. Some open source alternatives are now offering tools to put people back in charge.

Frank Karlitschek is a German open source developer and founder of Nextcloud, a platform for storage, collaboration and everything else you expect to work together online.

"We have this huge centralization of everything. The cloud infrastructure that drives a lot of the services on the internet, is controlled by very few entities, like Amazon, Google and Microsoft. They are the backbone of everything and this is not healthy," he says.

Nextcloud was originally founded as an alternative to Dropbox, but where the user could get the benefits of cloud services on infrastructure they control. It has since evolved into a fully modular productivity suite, meaning you can choose which applications you run on the platform

"The idea was that you can run your own server on your own infrastructure, so it's decentralized and federated," says Karlitschek. He compares the current version of Nextcloud to G Suite from Google or Microsoft Office 365.

"There's a lot of sharing, collaboration and communication features, document editing, calendars, contacts, all kinds of things. It's a full modern collaboration suite but it's a hundred percent open source and on your own infrastructure."

Nextcloud has about 1,800 individual contributors of code, from single fixes to multi-year engagements. "But it's more than code," says Karlitschek. "For examples there's translations. It's available in 95 different languages and they are all done by volunteers all over the world."

It is not purely volunteer-driven, however. 45 people are employed to maintain the codebase full-time. Their business model is to sell support subscriptions to organizations that use Nextcloud for free, a time-tested way of generating revenue from free and open source software.

Free and open source software emerged at a time when people ran software on their own computers, whether a PC on their desk, or a server in a hosting center. By running non-proprietary code, you had more control of what your computer was doing.

But as cloud services are becoming the default mode of working together, that kind of control is slipping away. "In a way it's even more closed than

proprietary software running on your own laptop, because at least there you know where it is," says Karlitschek.

In order to create a product that compares and competes with the global internet monopolies, you need to get a lot of things right.

"You need to have an alternative software that is as good. You need to have all the features that the user expects. If you have less features they will use the other software," says Karlitschek.

But even if you make the user interface and workflows interesting and useful, there are still obstacles to adopting decentralized cloud services.

With Google or Microsoft, you just create an account and get started. To use Nextcloud, you first need to install it on a server. No matter how easy this process is made, it is still one step more than the experience of the proprietary cloud. Hosting your own cloud also costs money.

"In the old days, with open source and free software, we always had the cost benefit on our side. We could say, if you use Linux it's as good as Microsoft and it costs nothing, where Microsoft costs money. With cloud services it is unfortunately the other way around. Nextcloud is free, but you still need to host it somewhere. Hosting now comes for free with the other services," says Karlitschek.

► Further reading

- Nextcloud. https://nextcloud.com/
- Orkney Cloud. http://orkneycloud.org/
- Decentralized Web Summit. https://www.decentralizedweb.net/
- IndieWeb: Getting Started. https://indieweb.org/Getting_Started

Participate

The internet is for all of us to shape and make healthier. You've read the stories in this report, and now you're probably asking "What can I do?"

10 minutes to a healthier internet

What you can do right now to improve your own 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. 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. 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 here.

I want to help

1. 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.

2. 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 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.

3. 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.

4. 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.

5. I want to help keep the 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 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.

Feedback

The Internet Health Report is an open source publication, and we value constructive feedback. We warmly encourage suggestions for research or data to include in the next version. We'd also like to know: What do you think of this initiative? Has it changed your perception of the Internet, sparked ideas for research, or motivated you in any way?

Contact us with your feedback by sending us an email: internethealth@mozillafoundation.org.

Our project blog at https://internethealthreport.org is the best way to keep up to speed with our latest activities.