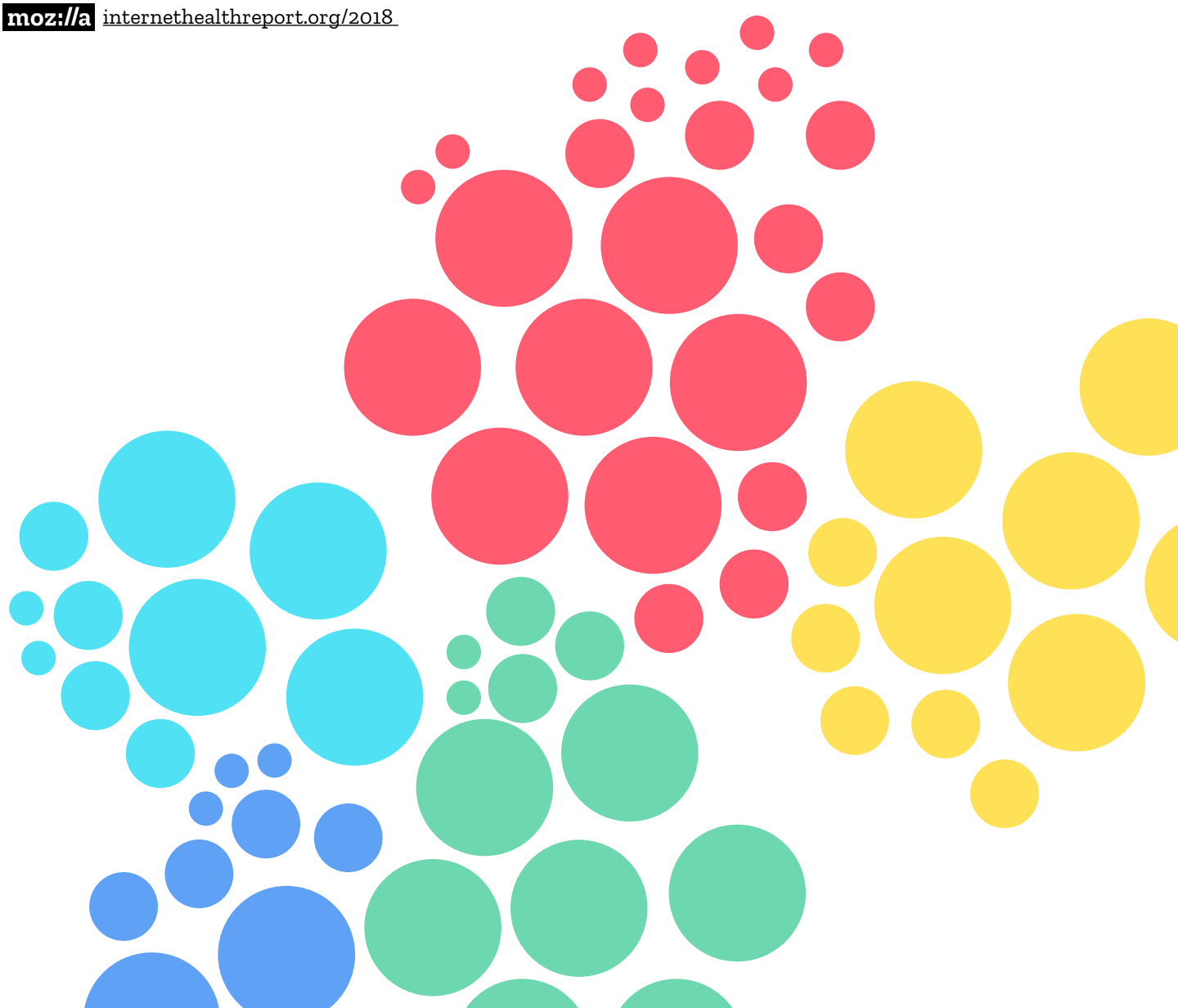
Internet Health Report 2018

Our compilation of research explains what's helping and what's hurting the Internet across five issues, from personal experience to global concerns.

moz://a internethealthreport.org/2018



Index

README

The Internet Health Report is about the human experience of the Internet. It is an independent, open source compilation of data, research and stories that show how the Internet evolves each year across five issues.

You may know other Internet reports that look more squarely at industry trends and new technologies. This is not our goal.

Working with researchers, digital rights activists, Mozilla fellows and our community, we tell a collaborative story of how the Internet is – and isn't – healthy from a human perspective.

The Report draws on a wide body of existing research on issues ranging from privacy to connectivity, to online harassment and the economics of online platforms.

Our aim is to connect the dots and look for patterns between these often siloed issues – to look at the human experience of the Internet as a whole.

By doing this, we want to encourage a broader understanding of how the problems facing the global Internet relate to one another, and to shine a light what people are doing to make the ecosystem healthier.

We, as humans, can change the Internet for the better. This report is a resource and call to action for everyone who is ready, in big ways and small, to take on this challenge.

The "components" of this report can be read in any order. At the end of each, we encourage you to share a reaction and engage with everyone about ideas.

A prototype of this report was published in January 2017 and was followed by an open, public discussion about metrics, several meetings with allies, and the establishment of a smaller "Report Coalition" to support content creation. Read project updates in our blog.

Visit: Internet Health Report v. 0.1

Credits

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

Solana Larsen is the editor of this report.
Kasia Odrozek is the project manager.
Jairus Khan is the outreach coordinator.

Contact us: internethealth@mozillafoundation.org

Our friends at Vizzuality are to thank for all visual and interactive design, coding and user testing. The Internet Health Report (and blog) is available in English, French, Spanish and German. Translations are by Global Voices.

See the full list of contributors online.

How healthy is the Internet?

It's getting easier to explain what Internet health means. When we launched the prototype for the Internet Health Report in 2016 it it was less so. What changed?

For one, headlines about unhealthy aspects of the Internet have been constant: many have started to argue that technology companies are becoming too dominant; social media has been weaponized as a tool of harassment; our personal information has been stolen; and democratic processes have been undermined by the manipulation of online media and ads.

It's no wonder that 2017 has been called a "terrible year for tech" by some.

Here's what's new: More people are opening their eyes to the real impact the Internet has on our societies, economies, and personal wellbeing. We are beginning to see the health of the Internet as not just a technical issue, but a human one.

That's the approach we take with the Internet Health Report, and why we look across a broad range of factors to consider the ecosystem as a whole.

This report features global insights and perspectives across five issues: Privacy and security, Openness, Digital inclusion, Web literacy and Decentralization.

We also cast a spotlight on three of the biggest Internet health issues of the past year: Securing the Internet of Things, Understanding 'Fake News', and Too Big Tech? These deep dives show how a usually narrow topic can offer a view of the big picture.

In Too big tech? we explore how the dominant companies of the United States and China create unhealthy conditions for struggling innovators and smaller populations trying to break into the market – and for a scientist trying to untangle himself from Google. The consolidation of power in global tech is not only a business story, it raises questions from the geopolitical to the personal. What do we want the Internet to be?

With Understanding 'fake news' we break away from the narrative of Russia and the 2016 U.S. election and explore why misinformation in social media has become a topic of concern to the world. Hint: the online advertising economy is broken and easily bent to fraud and abuse. Beyond propagandists, we consider teens who make easy money on digital ads, and people who share incendiary stories because they don't know better yet.

Finally, cybersecurity is often portrayed as a 'hacker' problem – but it's also deeply intertwined with the health of the Internet ecosystem as a whole. Up to 30 billion devices will come online by 2020, including insecure webcams, baby monitors, and other devices that can be enslaved and collectively wielded as a weapon. Securing the Internet of Things will be a challenge of correcting poor software, hardware and governance practices that make the Internet fragile. Who do we hold accountable? And how do we find

meaningful ways to keep things healthy and safe. There will need to be more than one answer.

Which brings us back to: **How healthy is the Internet?** In most cases it's not a simple question. Certainly, there are some straightforward indicators to watch. Things are getting a bit better in areas like: access, affordability, encryption. And they are getting worse in: censorship, online harassment, and energy use. Simple indicators miss the complexity that comes with global ecosystems like the Internet.

We need to be paying attention to the contractions, like the growing tension between free speech and harassment. We need to be watching for technologies and people who are smaller today but may be huge tomorrow, like open source hardware makers or blockchain innovators. And we need to be thinking creatively about how the people who make technology, the people who use it and the people who regulate it, can work together to create a digital world that is truly enriching for everyone.

More of us around the world are saying things, teaching things, and building things as a way to tackle these challenges. For everyone who is trying to make the digital world better: we hope the Internet Health Report can help along the way, at least a little.

We encourage you to explore the additional components of the Internet Health Report online and engage with the questions and conversations you encounter.

Please contact us and share your ideas. This report is a collaborative, open source initiative and we appreciate and consider all feedback and input.

Securing the 'Internet of Things'

Somewhere in Vietnam, a man is searching for a shoe box in a storage room, a woman is slicing bread in Argentina and a child sits restlessly on his mother's lap in a waiting area of what appears to be a pharmacy in France. A cow is being milked in Germany.

They are being filmed by online security cameras without passwords assigned. They surely don't know they can be watched by anyone who looks for insecure cameras on the Internet. Whoever set up the camera could choose to restrict access with a password. But without that protection, they are just there, broadcasting via the network. They don't have to be hacked.

Now consider that the number of Internet connected devices is expected to double from 2015 to 2020. That's 30 billion devices worldwide. For every device with either no password or a bad one, the Internet becomes a little more fragile and dangerous. But people buy things, connect them to the Internet and never think about securing them as long as they work.

Fitness trackers, kitchen appliances, light bulbs... This year, we will be listened to, watched, recognized and recorded by phones, digital assistants and cameras like never before.

Data will be collected that is vulnerable to hacks and breaches. We could worry about creeps on the lookout for unsuspecting naked people, or financial fraud, or invasive advertising or political manipulation. Do cars share our driving habits with insurance companies? Do vacuum cleaners trade in information about the layout of our homes? To most people, these are hypothetical risks, hardly outweighed by the enjoyment of the Internet of Things (IoT).

The reality is that the "attack surface" of the Internet is growing and that we have already had a taste of the nasty consequences.

In December 2017, three young men pleaded guilty in a US federal court to creating a strain of malware (malicious software) called Mirai in 2016 that enslaved thousands upon thousands of webcams, baby monitors and other devices with factory default usernames and passwords that performed targeted "DDoS attacks" to bring down websites and networks. When the authors publicly shared the code to obscure their own identity, Mirai botnets multiplied, and began competing against each other (and still do) for control over devices around the world, eventually succeeding in temporarily shutting down parts of the Internet in the US and Europe, through a large scale attack on the Internet performance management company Dyn. In Europe, banks and Internet service providers were extorted. In New Jersey, a university was.

Offering "security services" (veiled extortion) was part of the devious original plan of Mirai's authors, as was racking up dollars by creating fake botnet traffic on online ads. At the time, some security experts suspected government actors like China or Russia must be testing the resilience of the Internet. The actual villains

were less ominous, but the risk of all these insecure "things" still exists and the scale grows bigger with every new connected device.

For all the hype around gadgets and home appliances, many of the industries most impacted by IoT will be health care, transportation, energy and utilities. There are great opportunities for improving the efficiency and quality of public services, health and infrastructure.

Inexpensive hardware and decentralized innovation is also delivering the Internet to more people, in more shapes and forms than ever. While that is something to celebrate, unfortunately in today's throwaway culture, Internet devices are rarely designed to stay safe and secure over time.

Since all software is vulnerable to attack or malfunction with age, automatic software updates are a must. Small companies selling cheap IoT devices, without the resources and expertise of companies like Google, Apple or Amazon, will find this harder to do on their own.

Who do we hold accountable when the path from manufacturer to consumer is so opaque? Could there be regulations and industry codes of conduct to ensure the use of strong, random and unique passwords on Internet devices? Could there be technical security devices that form a shield around a person's personal IoT network? Could there someday be dependable trustmarks for IoT – like the labels on organic food or energy efficient appliances? What role is there for designers? These and many other ideas need research, exploration and further discussion in 2018.

They key problem is that IoT is growing faster and bigger than we could have imagined. Some of the risks posed are personal (like being embarrassed or perhaps being injured by a hacked car) while other risks are at the system or environmental level (like hospitals or the electric grid being taken down). Either way, it's going to be costly to fix when things go wrong.

One of the great opportunities of the moment for advocacy is in the home – being smarter consumers and especially advocating as parents on behalf of children who ought to be protected from insecure toys that contain hidden microphones, cameras or other personal data recorders. Dolls like 'Hello Barbie' and 'My Friend Cayla' that listen and speak to children have attracted negative headlines for being easily hacked. Germany is one country that bans Cayla as a "concealed transmitting device". Where else could traditional consumer safety regulations be leveraged?

We need to grapple with how we handle these issues as a society today: what we can leave up to industry, what we can leave up to consumer choice and what we need to regulate.

Further reading:

A Trustmark For IoT, Peter Bihr, ThingsCon, 2017

Privacy Not Included, An IoT Buyer's Guide, Mozilla, 2017

Understanding 'fake news'

Speaking truth to power has earned Filip Stojanovski enemies before. As program director of the Metamorphosis Foundation in Macedonia, Stojanovski helped create media watchdog Media Fact-Checking Service along with several other projects that support open knowledge and democracy over the Internet. Still, he found it absurd to see sponsored posts on Facebook linking to false claims about him in 2015.

"It was clear to me, this is a propaganda campaign against people who refuse to be silent about problems in this country," he says. He still doesn't know who paid for them.

What Stojanovski does know, is that it happened in the context of an ongoing campaign to intimidate and malign civil society organizations in Macedonia.

This type of fraud in social media is reaching epidemic proportions worldwide, at least in part because the online advertising economy that underlies much of today's Internet is terribly broken. Local politics aside, the rise of misinformation discussed under today's catch-all banner of 'fake news' needs to be understood in the context of unhealthy market realities that can reward malicious behavior for profit or political gain.

Most people are getting at least some of their news from social media now. In order to maximize dollars from displaying ads, news feeds and timelines show the content that attracts the most attention. This ends up favoring headlines that scream for reactions (expressed as shares, "likes" and comments). Add to this the ability to boost the visibility of any message by buying an "ad" targeting the people most likely to react (based on interests, behaviors and relationships) and anyone can churn out disinformation at unbelievable rates – and track their success. If only reality were as exciting as fiction...

The range of actors who create false information extend from malicious to simply opportunistic, with both local and global targets. And the types of people who forward, share and spread disinformation (when they are in fact real people, and not bots) have no unifying characteristic. Everyone is susceptible, even if extremists are more prone, perhaps because they are already outraged about a lot of things others do not perceive as fact.

In the United States, disinformation scandals (including the one about pedophiles in a pizzeria affiliated with Hillary Clinton) marred the presidential election in 2016, and questions about what role disinformation played in the election of Donald Trump reverberate today. Russian operatives are major protagonists in this line of inquiry, based on clear evidence that a Kremlin-linked organization, Internet Research Agency, spent hundreds of thousands of dollars to fuel toxic political discourse, before and after the election.

In this case, reality is actually so bizarre you'd think it was fiction.

Russians created dozens of 'fake' Facebook

pages, like "BlackMattersUS" and "Heart of Texas" that mimic language at different ends of the political spectrum in the United States. By attracting thousands of followers to the pages, they were able to use them to organize real life protests, and once even a protest and a counter protest at the same time.

Many headlines have been devoted Russia vs. the United States, but such behavior is not specific to Russia. In all too many countries – and that's in democracies as well as in authoritarian states – governments, militaries and political parties are using the Internet to manipulate public opinion at home or abroad under entirely false pretenses. They employ proxies and deploy trolls, bots and other techniques to obscure who they really are.

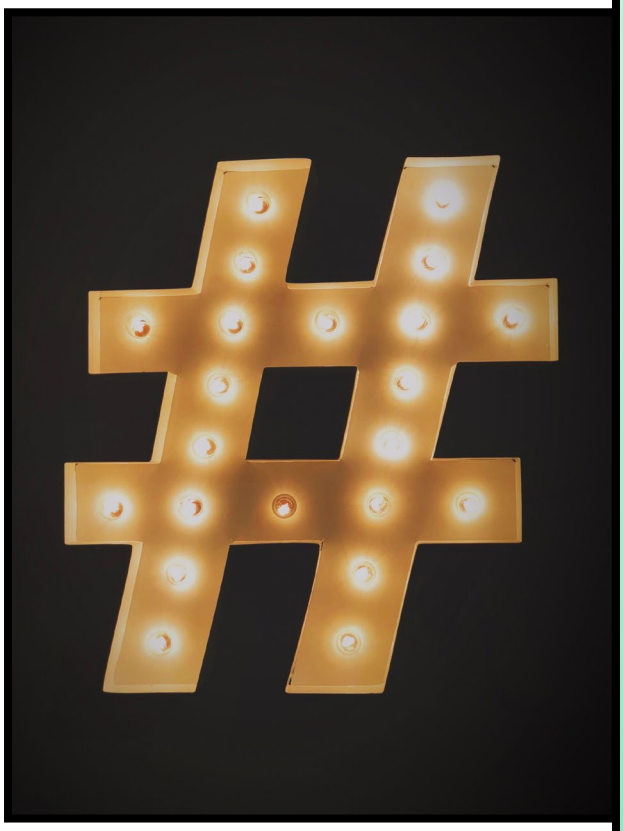
Macedonians are themselves quite familiar with Russian interference. But their own battles with disinformation stretch back long before the Internet.

Filip Stojanovski believes that decades of government propaganda through various stages of conflict and political transition from socialism to democracy in Macedonia has resulted in jaded citizens. Disinformation is a regular feature of how public opinion is shaped, he says, because mainstream media perform directly in the service of populist parties.

This particular ecosystem for truth, lies and politics, has proved fertile ground for a cottage industry for 'fake news' that also made a cameo appearance in the U.S. election.

Investigative journalists in different countries (starting from as early as six months before the U.S. election day) traced the origins of thousands of 'fake news' stories to a small town in Macedonia called Veles that used to be known for its porcelain. Young people here have created hundreds of websites with headlines in English designed to rake in digital ad dollars. They produce websites on anything from health and sports to finance and more.

But what they found most lucrative? Stories about Donald Trump. Exploiting the same social media mechanics as described above, Macedonian teenagers were able to make the "attention economy" work for them. Realistically speaking, these are the same dynamics that make Trump the biggest story in mainstream U.S. digital news media. People click, ads pay, more articles are written.



Online misinformation is a major threat to the health of the Internet and all of the societies it touches because of the potential for political disorder, undermining of the truth, hatred and rumors that spread in conflict or disasters, but also because attempted quick fixes by politicians (with or without ulterior motives) may threaten the openness of the Internet.

For example, Germany's reaction to misinformation and hate speech online was to make social media platforms responsible for taking down unlawful content. Other countries, including Russia and Kenya, have

passed laws that follow suit. We should be wary of any solutions that make Facebook, Twitter or any other corporations (or their algorithms) gatekeepers of the Internet.

Instead of quick fixes, we need to take the time to better understand the problem and the kaleidoscope of actors and symptoms. We're facing a mix of: junk news, computational propaganda, information pollution and low digital literacy.

Numerous people are already working on ways to tackle parts of the problem. Developers and publishers are trying to build more thoughtful and balanced communities around their news. The Credibility Coalition is working on a Web standard to support the detection of less trustworthy or reliable content. Teachers are developing curricula to help their students grapple with misinformation. And social platforms are trying to make political ads more transparent, although with limited effect. These are still early days for many ideas.

Even if efforts like these succeed, many argue that we'll still have to tackle a bigger Internet health problem: the underlying online advertising and engagement model that rewards abuse, fraud and misinformation. It's hard to imagine fixing this problem without regulation, radical changes in Internet business models or both.

We also can't fall into the trap of blaming technology for the global social and economic conditions that lead to polarized political debate, hyper partisan media or any of the other very human factors that contribute to these problems.

That the very tools designed for civic discourse and community building are being abused and undermined, plays precisely into the hands of those who prefer closed societies, fewer facts and a less healthy Internet.

While these problems are big and complex, coming up with solutions is critical to the health of the Internet – and our societies. If we can tackle these problems while still leaving the open, free-speech-friendly nature of the Internet intact, we have the potential to reinvigorate the public sphere. If not, we will be stuck in a very big mess.

That's the truth.

Further reading:

The Promises, Challenges, and Futures of Media Literacy, Data & Society, 2018

Why education is the only antidote to fake news, Huw Davies, New Statesman, 2018

Real News About Fake News, Nieman Lab

Fake News and Cyber Propaganda: The Use and Abuse of Social Media, TrendMicro, 2017

Too big tech?

You know an Internet company is big when your friends think you're weird for opting out of their services. In 2014, Chris Hartgerink was fed up with what he calls "corporate surveillance" and wanted to be more mindful of his privacy. He began an arduous process of disentangling his life from Gmail and Google, which took more than a year. When Hartgerink informed everyone that he would soon only be reachable on an encrypted ProtonMail email, his friends were disbelieving. They kept asking him, "Why are you moving email?"

"This social aspect just made opting-out of these services even more difficult," says Hartgerink who is a Mozilla Fellow and a PhD candidate in statistics at Tilburg University in The Netherlands. "I'm sure it would have prevented others from making the same decision."

The network control of major Internet services is only part of the grip they hold on our lives. Through sheer size and diverse holdings, a few companies including Google, Facebook and Amazon – or if you live in China, Baidu, Tencent and Alibaba – have become intertwined not only with our daily lives, but with all aspects of the global economy, civic discourse and democracy itself.

These are companies born of the dreams of Internet pioneers. They have supported billions of people from all walks of life to realize the benefits of the Internet. They have helped human communication, creativity and commerce flourish. Without them, we would have less information, less speed, less efficiency – less laughter!

Where contradictions lurk is in the consolidation of power. The problem isn't that these companies have billion dollar valuations, hundreds of millions of users or large acquisition portfolios. It's that they are too big. Through monopolistic business practices that are specific to the digital age, they undermine privacy, openness and competition on the Web.

Corporations are gaining unfettered access to our personal lives (just try hiding a pregnancy from online marketers). They box out competitors, restricting innovation in the process. As their capacity to make sense of massive amounts of data grows through advances in artificial intelligence and quantum computing, their powers are also likely to advance into adjacent businesses through vertical integrations in hardware, software, infrastructure, automobiles, media, insurance and more – unless we find a way to disrupt them or break them up.

How? If you delete your Facebook account tomorrow, your mom will probably mind the most. But the future of a company born only 14 years ago is not predetermined. Teenagers are growing noticeably tired of Facebook, and its founder Mark Zuckerberg now acknowledges – in a year of exceptionally bad publicity – that they need us to feel "our time is well spent."

Companies and technologies can change, and so can the regulatory environment around them. Merger enforcement and competition law are being called on to fight for a healthier Internet in many countries. This year, India's antitrust regulator fined Google $21 million USD for anti-competitive behavior (the process began seven years ago).

Last year, an even bigger $2.8 billion USD fine was levied against Google by the European Commission (this process also started seven years ago, and is being appealed). And Facebook, Apple and Amazon have all been probed regarding unfair competition.

These actions show that governments can play a role in rebalancing power. They also show how slow and outdated our antitrust models are. We need to rethink them so they can be more effective in the fast moving era of digital markets and network effects.

Real technical interoperability could also be an effective way to rebalance power and open up competition: Imagine if you could open WhatsApp and chat with someone using Signal. It could boost competition between existing services and innovation in new ones. Interoperability could ultimately be an imposed standard condition of future mergers.

If users had control over their own data and could move it freely to other services, it would decrease "lock in" and empower them to move between services of their choosing, including ones that don't have hundreds of millions of users. This principle of "data portability" is a requirement of Europe's General Data Protection Regulation (GDPR) which comes into force in May, but it's not yet clear exactly how it will be enforced.

We have grown used to enjoying free Internet services in exchange for giving companies access to our personal data, which they repackage and resell to digital advertisers who wish to target a specific audience or behaviors.

Google and Facebook control 84% of global digital ad revenue, outside China. It has not gone unnoticed by them that 36% of desktop Internet users now use ad-blockers to avoid annoying ads, excessive tracking, malware, misinformation and slower Web browsing. They are engaging in campaigns for "better ads", but more equitable models for advertising are not likely to be born from this.

Similar levels of consolidation have emerged in the world's foremost 'independent' Internet

market: China. For example, WeChat, a mobile app of Tencent, is a service so ubiquitous that it is used for practically all online interactions. "It is like Facebook, Whatsapp, Instagram, Yelp, Square and Snapchat rolled into one, with a hundred other apps thrown in," writes Aman Agarwal in a Hackernoon post with app screenshots. You can even browse the Web from within. This year, WeChat accounts will be tested in several locations in China for suitability as electronic national ID.

Plenty of nations (authoritarian and otherwise) glance enviously at China as one of the few countries that has effectively limited the rise of Silicon Valley companies within its borders. It has enabled local alternatives to thrive in the country that is home to the biggest number of Internet users. Yet, China only serves as an another example of what extreme consolidation of power looks like, and what a distant future of even bigger Internet giants could bring.

Throughout the rest of the world, Facebook, Google and Amazon dominate the Internet experience. Developing countries have the smallest share of the global app economy, and it's here that complaints of "digital colonialism" are gaining traction.

If no search engine can ever challenge Google, and no local apps can ever gain a sustainable market share, the opportunity promised by a free and open Internet erode. Open source challengers to social media giants, such as Diaspora and Mastodon, are few and far between, and they may at best deliver a proof of concept for an alternative future unless people can move their data freely.

Laws like Europe's GDPR are promising on issues like data portability but they will not deliver meaningful results unless consumers make specific demands of companies and regulators. Even when the law is on our side, we need to say: "Hey companies, this is how I want to move my photos around between Facebook, Instagram and my iPhone."

The only way to keep the Internet in the hands of all of us is to ask for it, build it and demand it. Consumers, governments and technologists need to push for fair competition, open innovation, interoperability and standards so the Internet can evolve in more healthy and humane ways.

Further reading:

OK Google: Delete My Account (No Wait. No Really.), Chris Hartgerink, 2018

Can Washington Stop Big Tech Companies? Don't Bet on It, Farhad Manjoo, New York Times, 2018

Competition through interoperability, Chris Riley, 2017

My Experiment Opting Out of Big Data Made Me Look Like a Criminal, Janet Vertesi, Time Magazine, 2014

Is it safe?

The Internet is where we could live, love, learn and communicate freely. To be ourselves, we need trust and confidence that there are systems in place to protect us.

Whether we know it or not, we are sharing more personal information than ever before.

The core business models of the Internet depend on knowing as much as possible about everyone, and analyzing, repackaging and selling that information. These data troves enable many new services, including machine learning and voice recognition. But the data collection is also accompanied by a constant risk of our social, financial, romantic, or political information being leaked in ways that expose us to harm.

In 2017, the disclosures of breach after breach – Equifax, Yahoo, Uber, the list goes on – show that many of the companies we trust with our data are not doing enough. The prying eyes of governments are watching too.

Security is only becoming harder to deliver at scale. Every technology, be it software or hardware, presents new risks. In 2017, WannaCry ransomware crippled high-profile targets, including Britain's National Health Service. A flaw in Intel chips put millions of devices at risk. Electrical grids in the Ukraine and the United States were hacked.

But people are not passively accepting these risks. They are creating technology to protect key infrastructure from attacks. Volunteer cybersecurity teams respond to emergencies. Cyberpeace efforts continue, in the face of worldwide information warfare.

As the Internet expands with more connected devices, the challenges will only grow. We have reached a point where you can't opt out. When homes have listening machines, shopping centers have facial recognition cameras, and satellite images can identify our cars, can we really control our digital footprints?

Despite these huge challenges, there have been steps forward.

In Europe this year, a new General Data Protection Regulation (GDPR) will require companies to adhere to stringent terms of privacy and consent, raising the bar for what we demand of data holders worldwide. More people are using security techniques like two-factor authentication, though they're still the minority. And we've seen an uptake in encryption for messaging and Web traffic.

In the coming years, we will explore opportunities to expand privacy and data protection frameworks worldwide —and push companies to take security seriously.

And yes, we should pick better passwords too.

Privacy and security // Data

Encrypted websites have become the norm

The number of encrypted websites is rising fast. Nearly 70% of Web traffic in Firefox is now on HTTPS encrypted Web pages, compared with just 50% at the beginning of 2017.

That's a healthy development for the Internet.

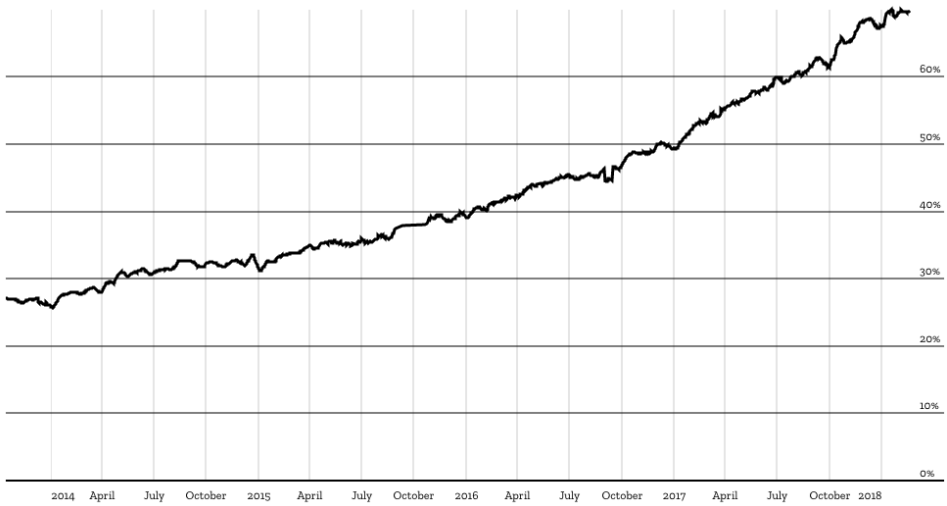
With HTTPS, the information you enter into any website, like your email login or banking information, is kept more secure from attackers. It also means that anyone tracking your browsing activity can only see which website you are viewing but not which pages.

Earlier, far fewer websites used encryption and uptake was slow. Adding HTTPS was difficult and required payment to a certificate authority of up to hundreds of dollars a year.

The non-profit project Let's Encrypt upended the status quo by developing open tools that make it easy and free for any website to encrypt. They launched in December 2015 and by June 2017, they had issued 100 million certificates through their automated system.

Percentage of page loads in Firefox using HTTPS

% of websites encrypted via https



Data source: Firefox Telemetry, Mozilla 2018

81 of the top 100 sites on the Web now use HTTPS by default. But depending on where you live, you may still be viewing far fewer encrypted sites than people elsewhere.

In some countries, governments may actively block or degrade HTTPS traffic to be able to monitor activity. In other cases, companies or organizations may lack the technical resources or know-how to implement HTTPS, or simply don't consider it a priority.

HTTPS is gradually expanding into more geographies, but the Web still needs to become a lot more secure for everyone.

Percentage of HTTPS page loads in Firefox per country

Data source: Telemetry data for Firefox from January 20 to February 20, 2018. For privacy reasons the data does not include countries with fewer than 5,000 page loads.

Privacy and security // Data

What Internet and telecom companies aren't telling us

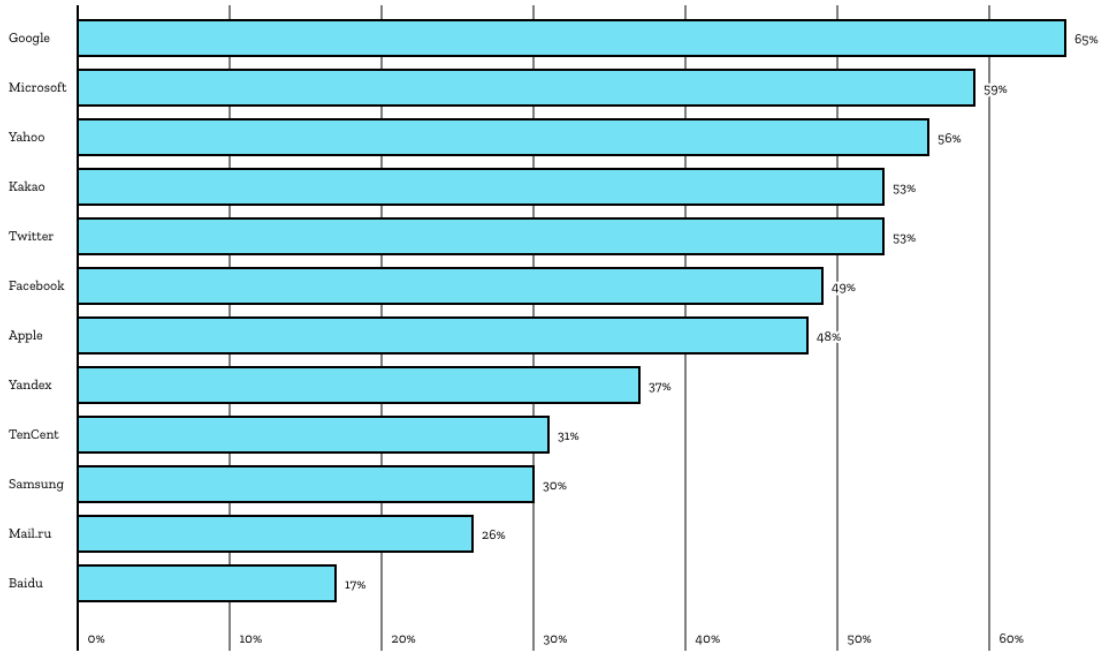
We place enormous trust in Internet and telecommunications companies with insufficient information in exchange about their privacy policies and practices.

Ranking Digital Rights works to raise standards for company disclosures on policies regarding governance, freedom of expression and privacy through a Corporate Accountability Index.

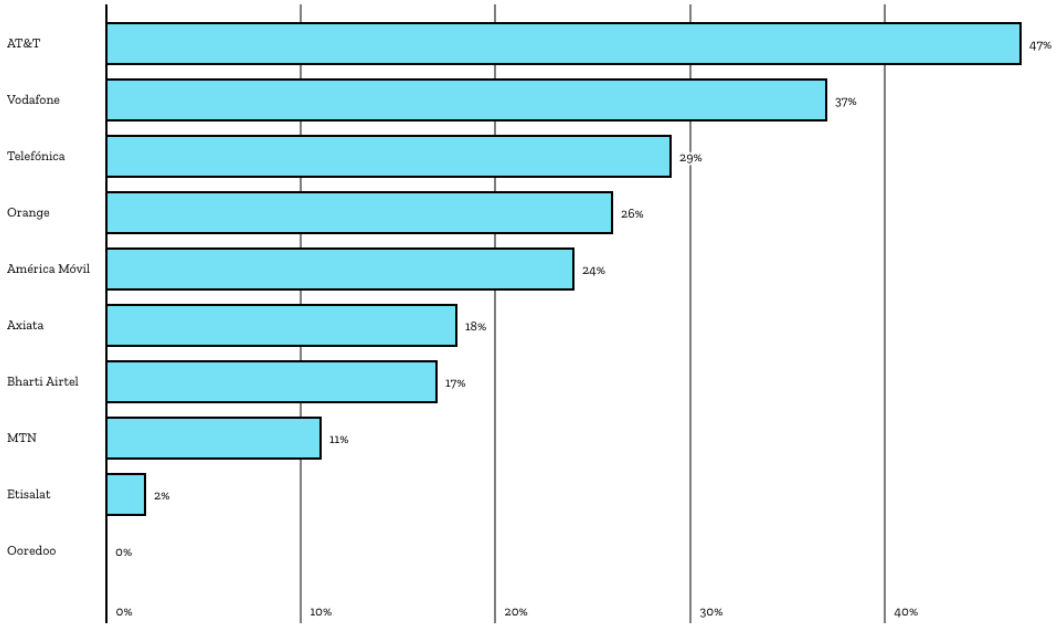
Their 2017 conclusions were damning: Most of the world's internet users lack the information they need to make informed choices. None of us know enough about how our information is collected, shared, retained, and perhaps reused – and commitments to governance and free speech are likewise inadequate.

Being able to hold the companies we depend on for Internet access and services accountable, requires us to define, compare and demand their respect for our digital rights. None of the 22 companies listed in the 2017 Index scored above 65% on measures of disclosure about customer rights to privacy.

How companies compare on disclosures of privacy policies and practices (Internet and mobile companies)



How companies compare on disclosures of privacy policies and practices (Telecomunications companies)



Data source: Corporate Accountability Index, Ranking Digital Rights, 2017

Privacy and security // Data

The top 50 passwords could easily be better

The top 50 passwords among 10 million leaked logins reveal a lot about what we can do to improve security on the Web. Is your password "123456"? Even if it's not, keep reading.

A report by WP Engine from 2015 analyzes passwords gathered from the Web and shared openly for security research purposes. Based on frequency, WP Engine estimates that 16 out of 1,000 passwords could be guessed simply by using the top 10.

"Unmasked: What 10 million passwords reveal about the people who choose them" describes the average length of passwords (8 characters), average strength (weak), and demonstrates how most people use passwords that are easy to crack because the words, numbers, or keyboard typing patterns they use are predictable.

Someone could access your email or other accounts simply by guessing your password. Or hackers may get hold of breached data from a service you use, and figure out how to reveal your password and try it across multiple other services. If you use the same password as thousands of others, you become an easier target for attackers.

Here's the good news: Using a password manager, automatically generated passwords, and two factor authentication can really help keep your data safe. With unique, strong passwords, we easily improve our individual security and can even protect Internet-connected devices from global scale attacks that endanger Internet health.

The top 50 most commonly used passwords

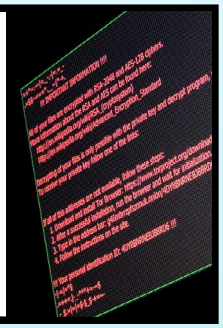
1. 123456	**11.** 123123	**21.** mustang	**31.** 7777777	**41.** harley
2. password	**12.** baseball	**22.** 666666	**32.** f*cky*u	**42.** zxcvbnm
3. 12345678	**13.** abc123	**23.** qwertyuiop	**33.** qazwsx	**43.** asdfgh
4. qwerty	**14.** football	**24.** 123321	**34.** jordan	**44.** buster
5. 123456789	**15.** monkey	**25.** 1234...890	**35.** jennifer	**45.** andrew
6. 12345	**16.** letmein	**26.** p*s*y	**36.** 123qwe	**46.** batman
7. 1234	**17.** shadow	**27.** superman	**37.** 121212	**47.** soccer
8. 111111	**18.** master	**28.** 270	**38.** 121212	**48.** tigger
9. 1234567	**19.** 696969	**29.** 654321	**39.** trustno1	**49.** charlie
10. dragon	**20.** michael	**30.** 1qaz2wsx	**40.** hunter	**50.** robert

Data source: Unmasked: What 10 million passwords reveal about the people who choose them, WP Engine, 2015

Read more online

Privacy and Security // People

Story of a ransomware victim



Privacy and security // Analysis

India's digital ID dilemma could be yours too

Privacy and security // People

Meet the Internet's FIRST responders to security emergencies

Privacy and security // People

Dispatches from the fight against unwarranted surveillance

Privacy and security // Analysis

Sweeping attacks on encryption worldwide

Privacy and security // People

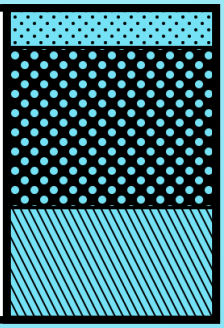
Design for a more secure Internet

Privacy and security // Analysis

The good, the bad and the ugly sides of data tracking

Privacy and security // Data

Ultra nerds are more optimistic about our connected future



Is it open?

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

You don't need permission to build new technologies for the Web. The openness of the Internet enables constant innovation and collaboration across borders. It extends from the architecture of the network and the underlying software, to how we publish content online. That openness is a radical concept, and it is constantly at risk.

Governments block mobile apps or shut down the Internet at will, media trade groups lobby for expanded copyright worldwide and corporations seek to enclose and control whatever they can: email, messaging, social media, voice technology, virtual reality, machine learning and more – stifling competition and hampering innovation.

Still, the openness of the Internet has proved resilient. It drives positive changes in governance and civic accountability.

In 2017, the debate about the open Internet sharpened, as we confronted hate speech, online harassment and misinformation worldwide, and divisive politics in numerous countries played out on social media.

People are asking: Can we have an Internet that is both open and inclusive?

In the United States, this dilemma made its way into headlines in August when companies including Google, GoDaddy and Cloudflare terminated their services to neo-Nazi website The Daily Stormer, following a white nationalist rally in Charlottesville, Virginia. Their actions briefly pushed the site offline.

Germany made waves with a controversial "hate speech law" that introduced steep fines for social media companies if they do not take down illegal content quickly. Countries, including Russia, Kenya, Venezuela and The Philippines, have modeled legislation based on Germany's.

Incidents like this point to a growing tension between the need to stymie hate online, and the risks of making Internet companies the arbiters of free speech.

The urgent question ahead of us as technologists, policy makers and citizens is: how can we preserve the open nature of the Internet, while at the same time building a digital world that is inclusive and welcoming to all?

Openness // Data

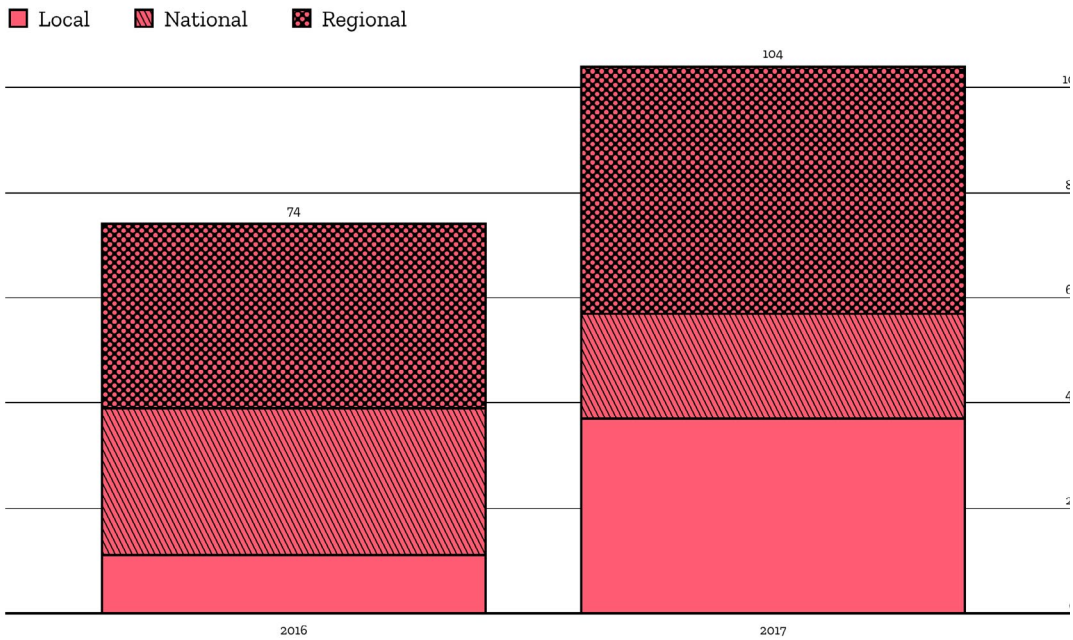
Internet shutdowns are rising

There were at least 104 Internet shutdowns in 20 countries in 2017 ranging from a few hours to months, says the #KeepItOn team at Access Now who track worldwide reports of shutdowns. Justifications for shutdowns vary, but there is mounting evidence that access to the Internet is used as a tool of control and oppression by the authorities of different countries, for instance to silence opposition voices during protests or elections.

Shutdown instances counted in 2017 more often target local or regional populations instead of national ones, which makes them harder for civil society groups fighting to keep the Internet open to track and document. Access Now says it could be a trend, but that it's hard to say for sure. We hear less about these shutdowns in the news – even within the countries affected. India alone has authorized dozens of shutdowns concentrated in the north of the country, far away from the urban centers of Bangalore or Mumbai where outages would never go unnoticed.

Shutdowns that are ongoing since the previous year only count as one "instance" and do not register in the numbers shared below. Among these, Pakistan has kept millions of people in a semi-autonomous tribal region offline since 2016, and populations of northwest and southwest Cameroon were also kept offline for large parts of the year.

Reports of local, regional and national Internet shutdowns worldwide



Data source: #KeepItOn, Access Now, 2017

Being without Internet access is extremely disruptive for students, families and work life. It can be traumatic and even life threatening to be without Internet access in times of conflict or terrorist attacks. Shutdowns have far reaching implications for safety, free speech and even the network itself.

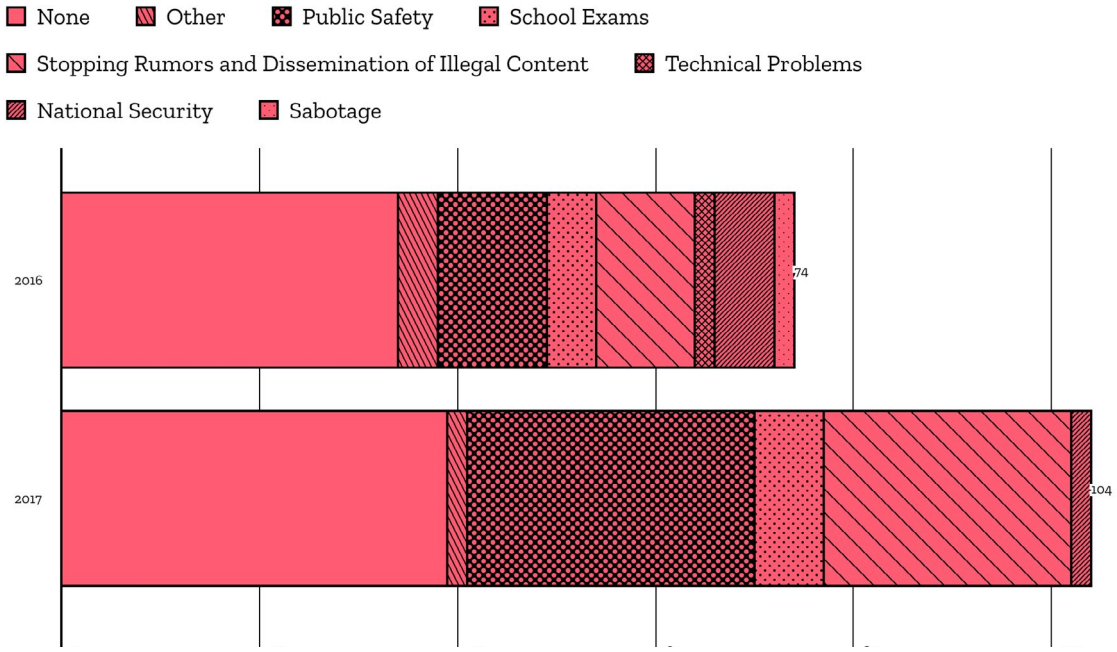
The majority of shutdowns last year occurred in Asia and Africa with justifications ranging from "reactive" in response to conflicts or political activity, or "preventive" to stop undesired activity.

Last year, nearly 7% of shutdowns were attributed to preventing cheating in school exams, while just over a quarter of official justifications fell into the broad category of "public safety." In somewhat positive news, the number of shutdowns with no asserted rationale has shrunk.

Sometimes only mobile connections are affected, but this is often the only Internet widely available.

Shutdowns are unhealthy for the Internet. We need more legal safeguards against them, nationally and internationally. With more research and evidence-gathering to determine how many shutdowns occur and why, we can hone in on tactics and technologies to stop them for good.

Official justifications for Internet shutdowns worldwide



Data source: #KeepItOn, Access Now, 2017

Openness // Data

Where social media and messaging apps were silenced

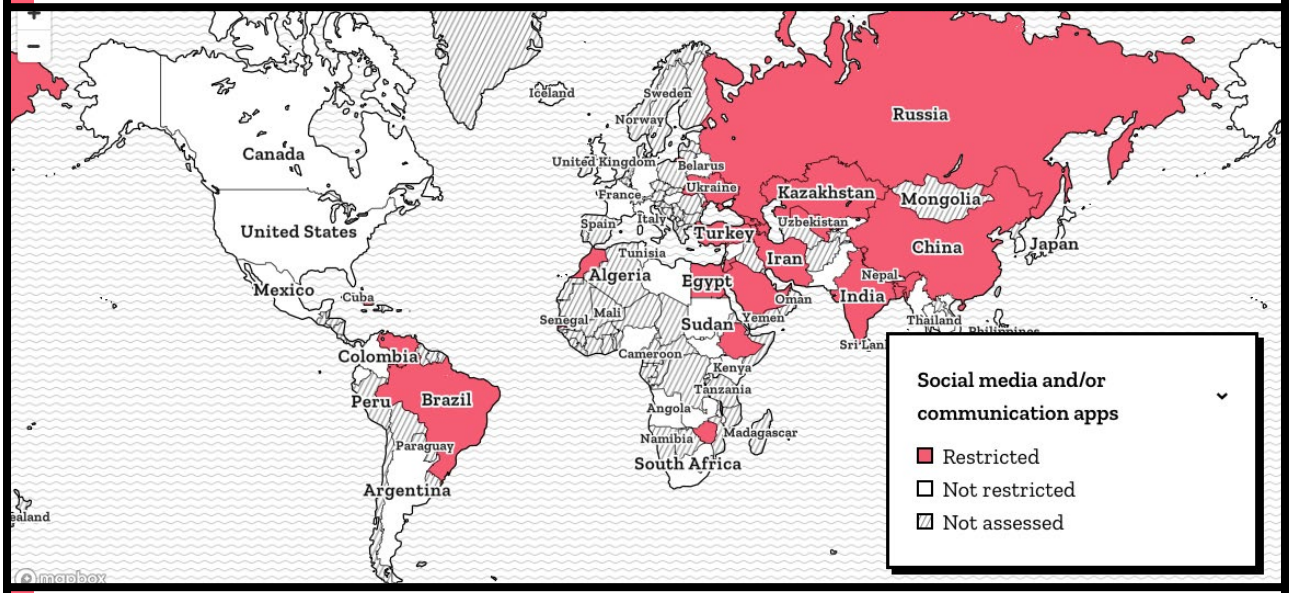
When governments wish to limit free speech, they often look to communication tools many people use the most: online social media and messaging apps. Around the world, access to these technologies is sometimes restricted temporarily or for long periods at the whims of government authorities.

Web censorship, arrests, Internet shutdowns and disinformation all form part of a growing catalogue of repression techniques that all contributed to a seven-year consecutive decline in Internet freedom, according to global rights group Freedom House.

Freedom House says WhatsApp was the most commonly obstructed app from June 2016 to May 2017. It was blocked or throttled in 12 out of 65 countries assessed by the organization. Facebook, Twitter, Skype, YouTube, VKontakte and WeChat were also among services targeted across 26 different countries.

Two-thirds of the world's Internet users live in countries where Internet and media censorship are common. When apps or social media platforms are blocked, it limits an entire population (regional or national) from communicating with family, friends and followers. It's a heavy-handed approach that can have severe negative consequences.

Countries where social media and messaging apps were blocked



Data source: Freedom of the Net 2017, Freedom of the Net 2016, Freedom House

Openness // Data

Open data sharing by governments is stalling

When the Internet is used to openly share public information it helps improve government transparency and accountability, and delivers on its potential for positive impact in the world.

Data is "open" when it can be freely used, modified and shared by anyone for any purpose. Ideally, public data on budgets, elections, transportation, health care and more, can be explored online by all. Unfortunately, government commitments to open data appear to be stalling worldwide.

Notable exceptions include Canada, Israel, Kenya, South Korea, Mexico and the United Kingdom, who have made steady progress since formally adopting an Open Data Charter.

How data is published matters enormously to whether it is genuinely useful. To be of maximal use and public benefit, data must be online and free, available in bulk in machine readable format (for data analysis) and issued under an open license (enabling cross-sector research and more).

The Open Data Barometer of the World Wide Web Foundation tracks progress on open data around the world. Of the 1,725 data sets they reviewed from 115 countries, only 7% of data sets were "open" in 2016.

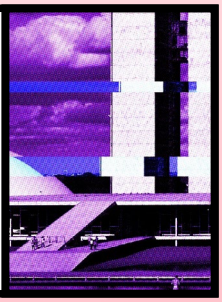
How public data sets were shared in 115 countries from 2012 to 2016

Data source: Open Data Barometer (4th edition), World Wide Web Foundation, 2017

Read more online

Openness // People

In Brazil, a bot in the public interest



Openness // People

Mapping the threatened voices of the Internet

Openness // People

Opening up voice technology for all

Openness // Analysis

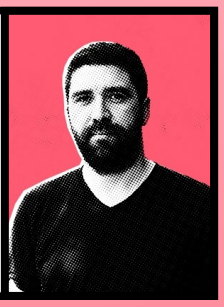
Germany's hate speech law makes global waves

Openness // People

The hidden costs of an open Internet

Openness // People

Creative Commons has a new global network strategy



Openness // Analysis

Resisting a WhatsApp and Telegram ban in Afghanistan

Openness // People

Intelligent machines aren't always right

Openness // Analysis

Refusing to let copyright break the Internet in Europe

Openness // Data

The open source software you never knew you were using

Who is welcome?

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.

About half of the world's population is online now, and more are joining at rates unthinkable before mobile phones and social media. Yet, stubborn digital divides persist.

Those who suffer inequities on other fronts – including people with low incomes, rural communities, women and minorities – tend to be the last to connect. And when they do, they face high costs and poor quality access.

Without affordable, reliable and fast Internet, economic development stalls. People are cut off from access to education, health and government services, quality content in their own languages, or simply conversation with family and friends.

As an inverse of the access divide, it is becoming a luxury to disconnect as the Internet wraps itself around every aspect of our lives and public spaces. And for many marginalized communities, privacy was never an option in the first place.

A gap is also widening between those who feel safe online, and those who don't. Online hate speech and harassment is a serious problem, with women, younger people, LGBTQ+ communities and people of color being impacted most frequently.

This is amplified by persistently low diversity within most tech companies (and open source communities), which has inevitably led to software, algorithms and products that reflect the biases of their creators and fail to consider the needs of marginalized users.

On all these counts, we could say the Internet is becoming less healthy. However, we have also seen a wave of new and meaningful efforts to tackle digital inclusion.

In 2017, sustained public outrage led several platforms, including Facebook and Twitter, to get more serious about tackling online harassment. We saw new independent initiatives to connect the unconnected, bolstered by evidence that low quality access schemes for the poor (like zero rating) are not effective on-ramps to the Internet. And research revealed paths towards creating more inclusive online communities.

Digital inclusion will present new challenges in coming years. Diverse groupings of technology makers, governments and civil society must dig deep for solutions to these complex problems. A healthier Internet built on respect for humanity relies on them.

Digital inclusion // Data

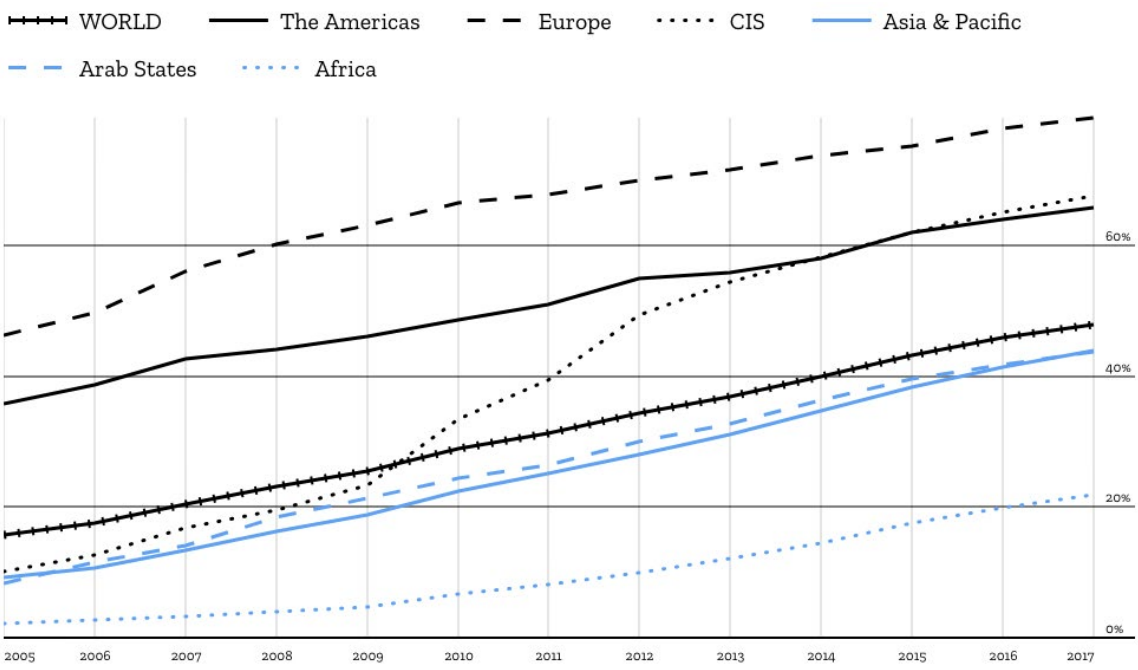
Who's online, and who isn't?

Almost half of the world's population is now online, but the rate of connectivity is still hugely uneven between regions. In Europe nearly 80% of people have Internet access, while only 20% of people in Africa can access the Internet, despite the rapid uptake of mobile phones in most countries.

According to the the International Telecommunications Union (ITU) global connectivity rates went up by just 5% in one year. Considering that Internet access is crucial to economic development, we urgently need affordability, accessibility and quality to increase for the populations that need it most.

Today's rise in connectivity is driven by young Internet users: people between the ages of 15-24 make up almost one quarter of all people online. But even among them, regional differences make for a stark contrast. In Europe, 96% of youth are online, compared with only 40% of young people in Africa.

Growth in percentage of people online worldwide



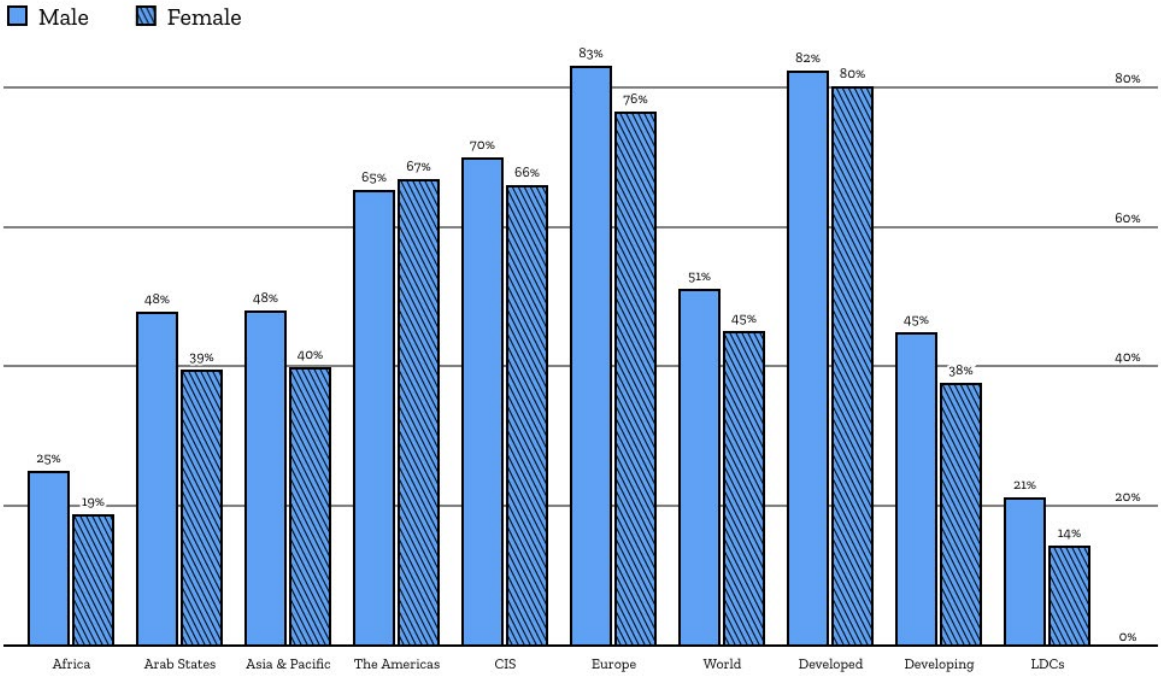
Data source: Time series of ICT data for the world, International Telecommunications Union (ITU), 2017

Even when the number of people online rises, women are not guaranteed connectivity at the same rates as men. In every region of the world, except in the Americas, men outnumber women online.

Wherever women have less access to education, social and economic rights, it follows that they also have less Internet access. In fact, the digital divide contributes to inequality because women have less access to professional opportunities, information and communication channels.

In the absence of policies to reverse the trend, gender parity can easily grow worse. In Africa there are a quarter less women online than men, a difference that has increased notably since 2013.

Percentage of people online worldwide, by gender



Data source: ICT Facts and Figures 2017, International Telecommunications Union (ITU), 2017

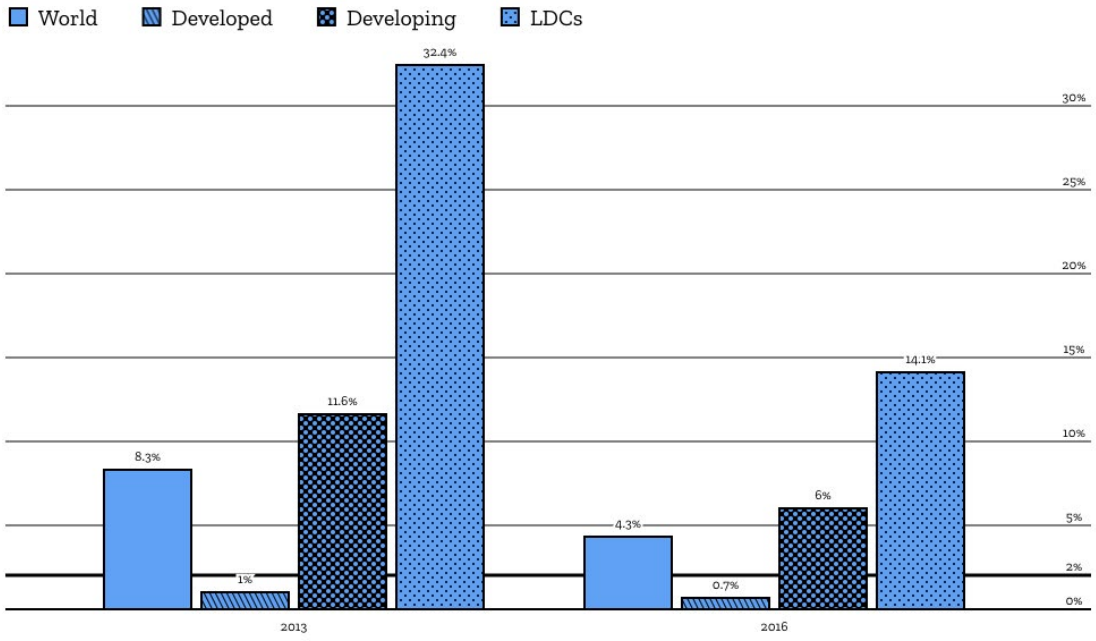
Digital inclusion // Data

The Internet is more affordable (but not enough)

Mobile data prices have declined in all regions, but in the least developed countries the cost is still seven times higher than the affordability target set by the United Nations.

Internet access is considered affordable when 1GB of mobile broadband data is available for 2% or less of monthly gross national income (GNI) per capita. Lowering the cost of Internet access is one of the most important factors in connecting the 50% of the world who still live offline. A range of policy, commercial and technical interventions can help lower costs. Internet advocacy groups say most countries aren't acting decisively enough to meet the UN Sustainable Development Goal of universal Internet by 2020.

Price per 1GB of mobile data as percentage of monthly Gross National Income (GNI) per capita



Data source: ICT Facts and Figures 2017, International Telecommunications Union (ITU), 2017

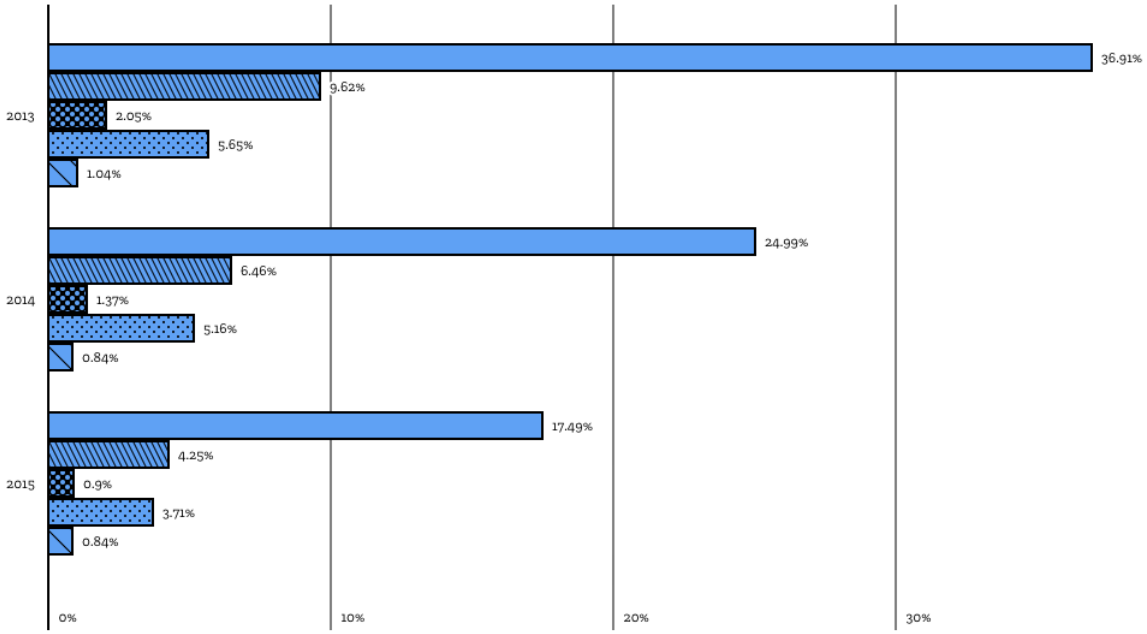
Europe and North America were the only regions to meet the meet UN affordability targets in 2015. Internet users here paid less than 1% of GNI per capita for 1GB of mobile data in 2015.

In Africa, people were spending an average of 17% of their average monthly incomes for the same amount of data, and often for much slower connections.

Alliance for Affordable Internet (A4AI) is one organization that has encouraged the UN International Telecommunications Union (ITU) to keep updating its methodology to reflect current Internet use. For instance, A4AI's own broadband affordability study (covering fewer countries) focuses on prepaid data plans only, which is how most people in low and middle income countries connect.

By either counting method, affordability improvements are most evident in Africa.

Price per 1GB of mobile plan as a percentage of monthly GNI per capita, by region



Data source: A4AI calculations based on pricing data by ITU, 2017 A4AI Affordability Report, 2017

Digital inclusion // Data

Diversity in tech? Not yet

Today, the people who develop software in the United States are overwhelmingly white and male. Evidence shows that persistently low diversity leads to software, algorithms and products that reflect the biases of their creators. 2017 was a year of sexual harassment and gender discrimination scandals in Internet companies and venture capital firms.

These are problems for the health of the Internet.

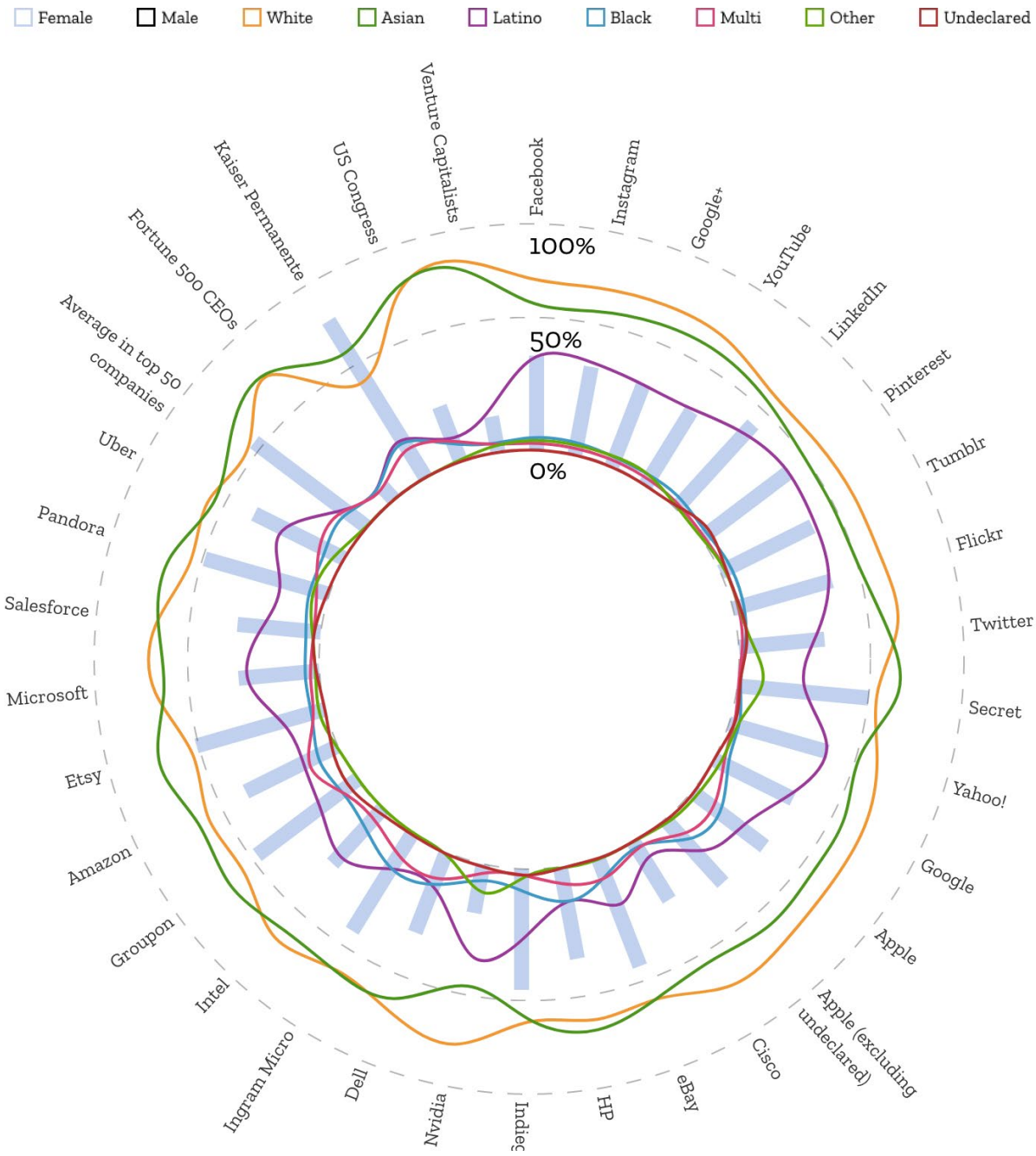
Expectations are rising for companies to become more diverse and genuinely inclusive. Initiatives like AnitaB.org, National Society for Black Engineers and Code2040 are chipping away at barriers to entry, often with financial support from companies themselves.

And while increasing diversity is critical, the often toxic work culture within many tech companies will also need to change for people from underrepresented groups to thrive.

More companies are publicizing their diversity metrics, inviting greater transparency and accountability. But these numbers don't tell all. Often gains in gender or race diversity are not reflected directly on engineering teams, or only in lower salaried roles.

Acknowledging the problem and increasing diversity is a good start, but to build truly inclusive products, companies need to welcome a wider array of diverse perspectives, from gender to race, to economic background, languages, cultures and more.

Gender and ethnic diversity in the biggest US tech companies



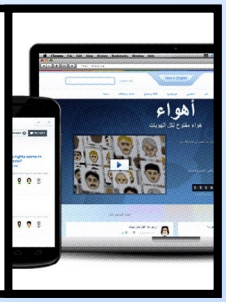
Data sources: Self-reported diversity metrics from tech companies, based on data from 2016 or 2017. Compiled in Diversity in Tech by Information is Beautiful, 2018.

*Mozilla's 2017 diversity metrics are forthcoming in the second quarter of 2018.

Read more online

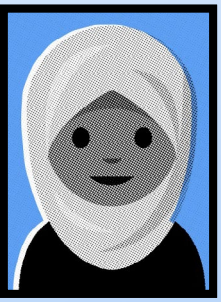
Digital inclusion // People

Carving out safe spaces for LGBTQ rights



Digital inclusion // People

Emoji politics: where grassroots meets big tech



Digital inclusion // People

If anonymity isn't the problem, what is?

Digital inclusion // People

Building a multilingual Internet

Digital inclusion // Analysis

New approaches to rural Internet connectivity

Digital inclusion // Analysis

Does the Web speak your language?

Digital inclusion // People

A helplinefor victims of 'revenge porn'

Digital inclusion // Analysis

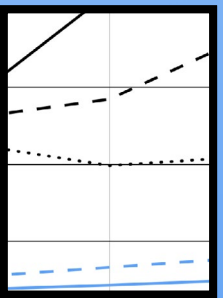
Fighting online harassment with artificial intelligence

Digital inclusion // Data

Test your knowledge of online harassment

Digital inclusion // Data

Is the Internet getting faster for you?



Who can succeed?

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

Web literacy is within our grasp. We constantly adapt to new software and hardware, at home and in public. Intuitive design makes it possible for hundreds of millions of people to use their first smartphone without manuals, or in some cases, the ability to read.

But the basic skills we pick up along the way don't give us everything we need to tap into the opportunities – and avoid the risks – of digital life. The newly connected have a steep list of things to learn, and even experts sometimes need instructions for how to make things work on the Web.

Acquiring the wide range of skills needed to read, write and participate in our digital world requires dedication. Technical abilities like coding are important, but they're not enough.

We also need to be able to critically analyze information we see online, as social media debacles over 'fake news' the past year made clear. Even young people who are 'digital natives' don't automatically know when to ask questions or how to validate what they see.

Platforms can offer more transparency about where content comes from and support studies to improve "conversational health", but individuals and communities also need to know for themselves how to be safe online. It is especially urgent for people at risk of cyberbullying, harassment or government persecution, but anyone could end up vulnerable. If you use one of the most commonly used passwords, your personal and financial information is already at risk. Are we, and our children, as safe as we can be?

Do we know when to shut off our screens? In 2017, tech companies faced industry criticism for getting us so effectively hooked on their services. The apps we spend the most time with don't always make us happy, and yet we continue clicking and scrolling.

People everywhere need all these skills and more to engage in broader discussions about the economic structures and power dynamics of the Web, which impact all of our lives. We need universal Web literacy. We need to support educators, as well as teach each other. It is only becoming more vital as new people come online worldwide, every day.

Web literacy // Data

Do the mobile apps we use the most make us unhappy?

The apps on our smartphones can produce a range of emotions, and they're not always positive. The time we spend tapping our screens can leave us anxious, envious, depressed or angry. Even Facebook admits this — well, kind of.

At Moment — a free Apple iOS app that tracks users' screen time and helps them limit their app usage — the team recently partnered with the Center for Humane Technology, an initiative that questions technology's impact on human well being, to determine what apps leave us most happy, and which leave us most unhappy.

The goal: To encourage more self-awareness about app use and offer some impetus to change negative habits.

For the project, Moment asked thousands of users (mostly based in the United States and Europe) a simple, yes or no question about the apps they use on their phones: "Are you happy with your time spent?"

Happiness is not easily defined, but according to the app rating responses, the apps that yield the most "happiness" are Sonos, Audible, Headspace and Sleep Cycle. The apps that yield the most "unhappiness" are Facebook, Instagram, Telegram and Reddit.

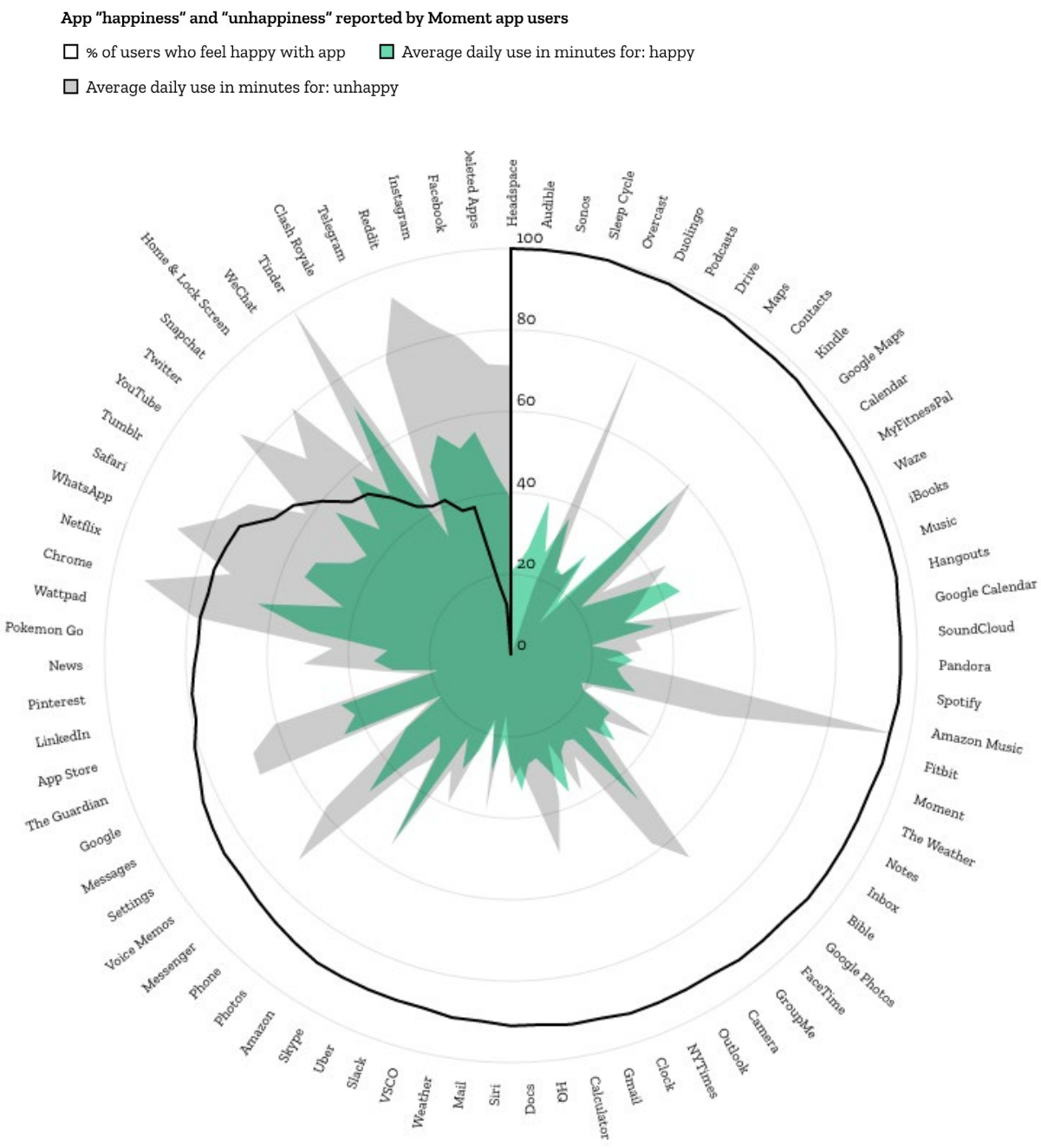
An important component of the data is the amount of time spent using an app. "I wanted to find the happiness breaking point for each app," explains Moment designer Kevin Holesh who shares regular updates and musings on Moment user statistics on Twitter.

In the case of Facebook, Moment found that point to be 18 minutes a day. Such moderate usage was found to even boost an app user's mood. But 47 minutes veered into unhappy territory.

Holesh says Facebook's business model depends on engagement and ad revenue, not on making people happy, and speculates that they would not willingly cut down on engagement

So if you find your mood declining while on your smartphone, perhaps you've spent more than your daily happy time on your favorite app? And if you find you're struggling to close that app, remember, there's an app now to help you do that, too.

App "happiness" and "unhappiness" reported by Moment app users



Data source: Moment App Survey results shared by Kevin Holesh, February 2018 (an earlier data set appeared on Center for Humane Technology in 2017)

Web literacy // Data

Are learning standards keeping up with the Web?

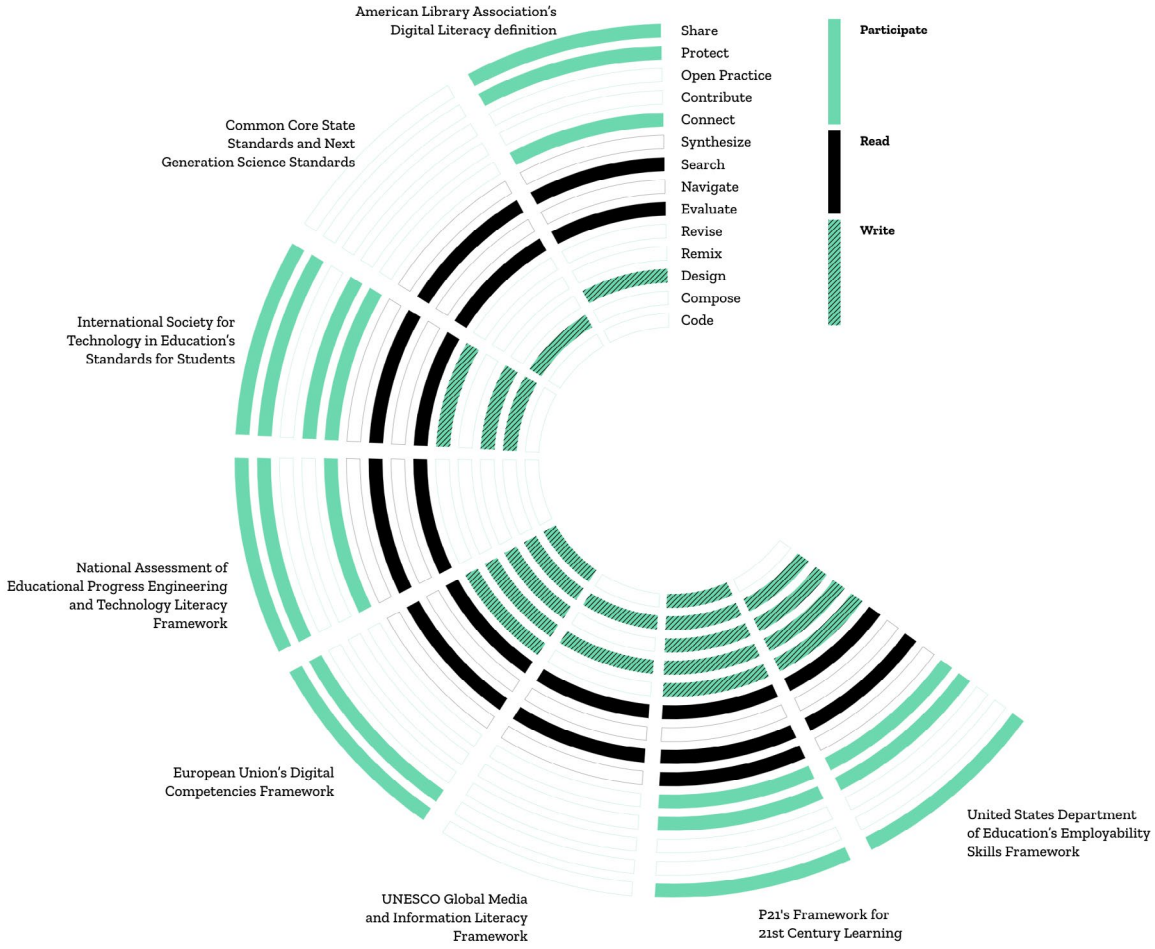
Only some key Web literacy skills are well represented in existing international learning frameworks.

In order to assess whether learners are on track to understand what they need to in a digital world, Mozilla researched the contents of eight influential global workforce and education frameworks, to see which essential Web literacy skills are already part of them – and which are missing.

Digital skills frameworks of the past focused on use of computers and basic software. For people working, learning and living in today's world, they need to know how to search the Web and assess sources (included in all reviewed frameworks) and write basic code as well as understand how to navigate the Web (only sometimes included).

For a healthy Internet we need to set high standards for what people should learn to make the most of the online experience for themselves, their workplaces and societies.

Web literacy skills included in workforce and learning frameworks



Data source: Analysis of Mozilla's Web Literacy Map and other Literacy Standards, Mozilla, 2017

Read more online

Web literacy // People

A fix to our throw-away technology culture

Web literacy // People

Django Girls: Communities of code from Argentina to Zimbabwe

Web literacy // People

The ultimate manual for the Web, in 48 languages

Web literacy // Analysis

Your best guides to ending cyberbullying: survivors

Web literacy // People

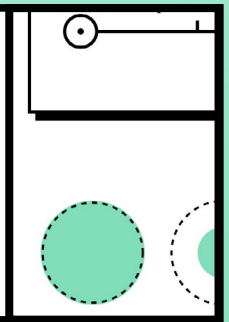
Teaching digital security to civil society

Web literacy // People

An educational game to fight 'fake news' online

Web literacy // Data

A week in the life of the Web



Web literacy // Data

53 skills new mobile Internet users should master

Who controls it?

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

The Internet belongs to us all. It is distributed across a decentralized network of computers that no single authority can own. That's the dream. The reality is different.

Outside of China, the world's experience of the Internet is dominated by five companies from the United States. These companies have built technologies used and enjoyed by billions of us. But their consolidation of power, and business models that demand to know everything about everyone, are a threat to the health of the Internet.

Serious questions about whether it's time to challenge or "break up" big tech companies are recurring now with more urgency.

In 2017, Google was fined a whopping $2.8 billion USD by the European Commission after a seven year process. And the outsized influence of a handful of social media companies only became more evident as Facebook, Twitter and Google were officially called to task for use of their platforms by Russia to spread misinformation during the U.S. presidential election the previous year.

In China, the dominance of mobile app giant WeChat will reach new heights if small scale trials for the accounts of 900 million daily users to double as national IDs are deemed successful by the government.

Telecom companies also pose a threat to a decentralization when they offer sponsored deals on specific online content, like messaging or music, that puts smaller players at a disadvantage. For those of us who believe all content should be treated equally, this is unacceptable. Some battles for net neutrality have been won, but the fights are far from over.

Today, the air is thick with this question: How do we rebalance the power between the biggest Internet companies and the billions of us who use their services everyday?

How should we govern in a world where a handful of companies have more wealth than many nations? Can we distribute more control of Web technologies, using peer-to-peer, blockchain, and new organizing principles for social media? There are no easy answers, but we can demand open and interoperable services, more ethical business practices, and a market that is favorable to competition, innovation and a diversity of services for all.

Decentralization // Data

Support for net neutrality protections is on the rise

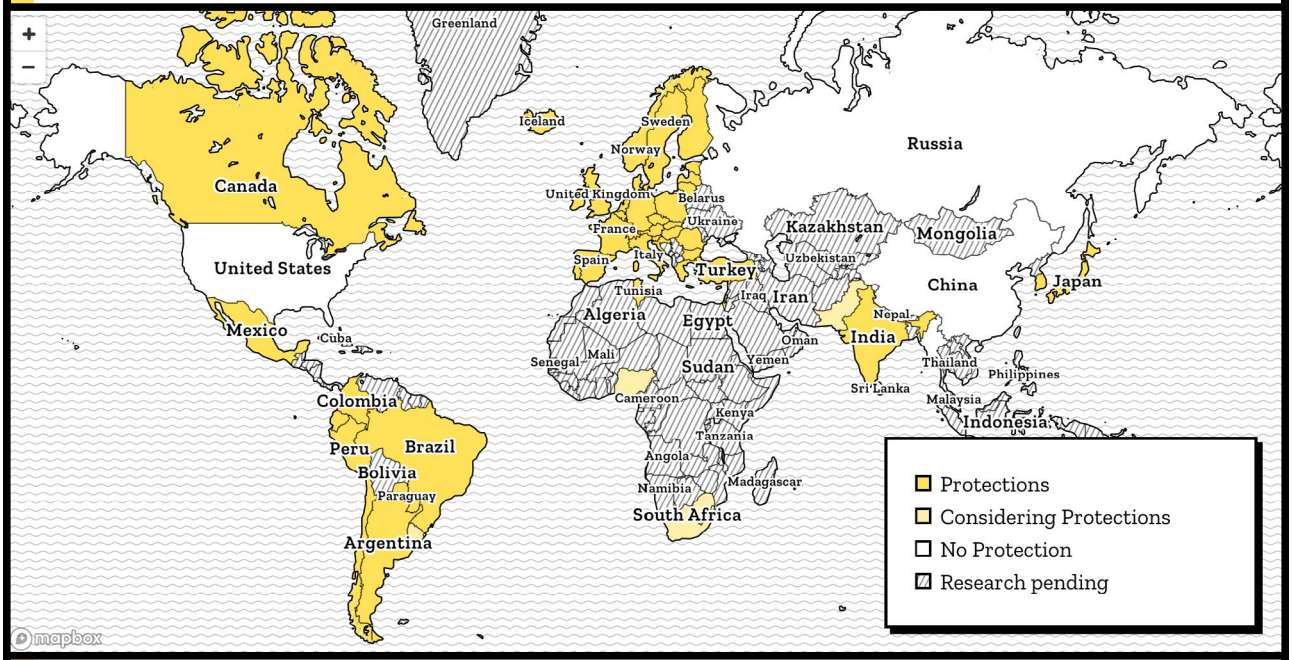
You may take for granted that the company that connects you to the Internet has no control over what you do online. Or perhaps you live in a country where Internet access plans restrict or give preference to certain music, films or social media apps.

In an effort to ensure that everyone has equal access to the open Web and whatever online services they choose to use, many countries have introduced "net neutrality" laws and protections. When such rules are introduced, it often involves consumers raising their voices and convincing regulators to ignore powerful telecom industry lobbyists.

In 2010, Chile became the first country to enshrine net neutrality into law. Many countries have since proposed, passed, or considered such legal protections for Internet openness. Regrettably, some victories can be short-lived. The United States repealed federal net neutrality protections in 2017 that were passed in 2015. In other cases, the law itself is only the first step; for instance, net neutrality came into force in the European Union in 2016, but most of its 28 countries have yet to begin enforcing in earnest.

Despite setbacks, public awareness and support for net neutrality has grown in many countries. India, the second largest online population, reinforced its commitment to net neutrality in 2017. Individual U.S. states have also introduced protections in defiance of federal regulators. And more countries are considering protections, including South Africa.

Status of net neutrality around the world



Data source: Status of Net Neutrality Around the World, Global Net Neutrality Coalition, Access Now, 2017

Decentralization // Data

Google dominates browser market

Google Chrome is the leading browser on desktop computers and mobile devices by a wide margin.

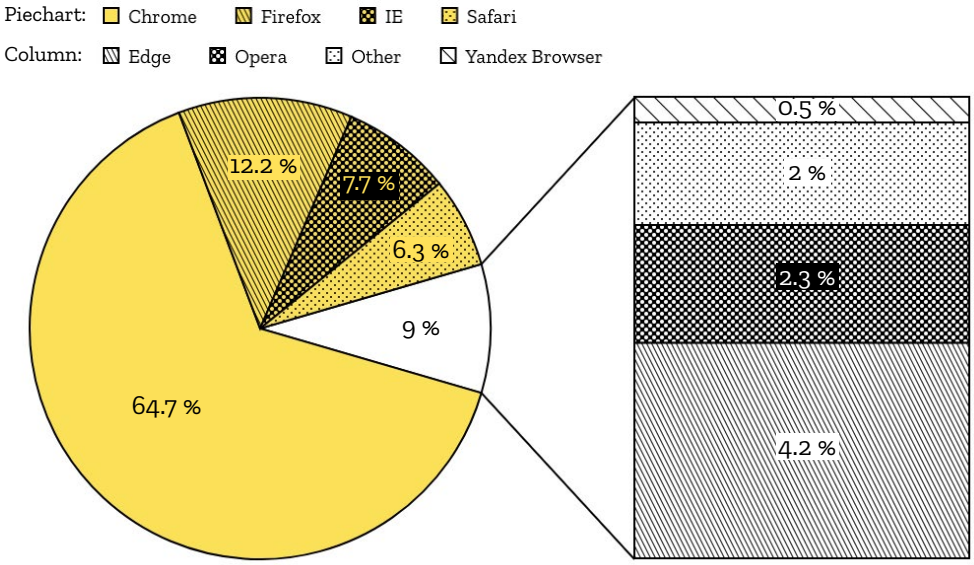
Chrome was first released in 2008 and replaced Microsoft's Internet Explorer at some point between 2012 and 2016 as the most widely used browser in the world, depending on counting method. Their market lead has grown ever since, boosted by pairing the browser with the Android operating system.

On desktops, Firefox (the browser backed by the non-profit Mozilla) is the second most widely used worldwide. On mobile devices, Apple's Safari and UC Browser by Alibaba are in second and third place.

Google's primary source of revenue is displaying and selling ads. Its freeware browser, Chrome, helps further this business. A lesser known effect of Google's dominance is that the company has the power to define and implement features of how the Web works for everyone, no matter which browser they use – for instance, through the Web standards process. This is an unfortunate vector of competition, because Google can push for standards or formats that other browsers can't or don't want to deliver on.

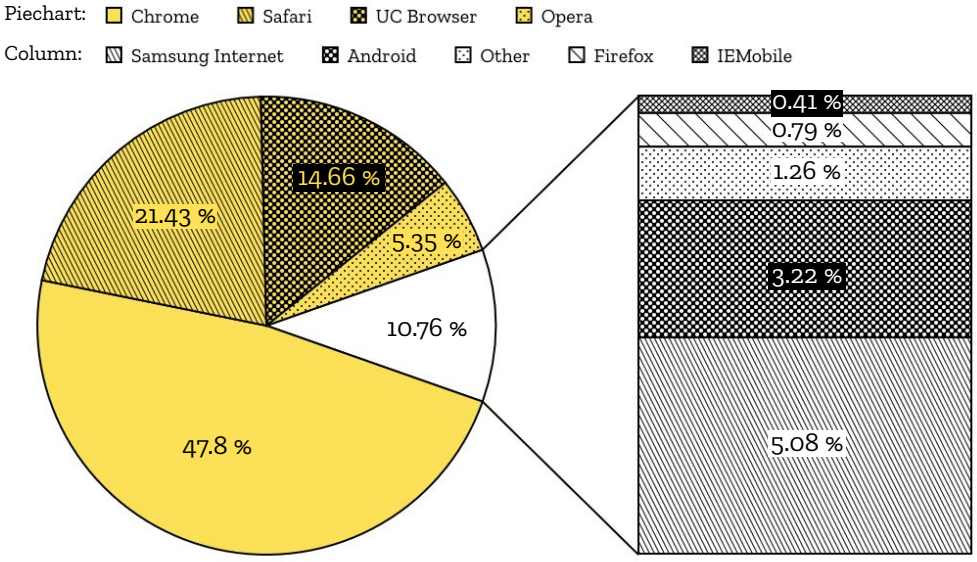
The browser is the central gateway to the Web, so competition and options around values like choice, privacy and transparency, matter to the health of the Internet.

Desktop browser market share worldwide



Data source: Desktop Browser Market Share Worldwide, StatCounter, 2017

Mobile browser market share worldwide



Data source: Mobile Browser Market Share Worldwide, StatCounter, 2017

Decentralization // Data

Social media giants Facebook, Tencent, Google reign

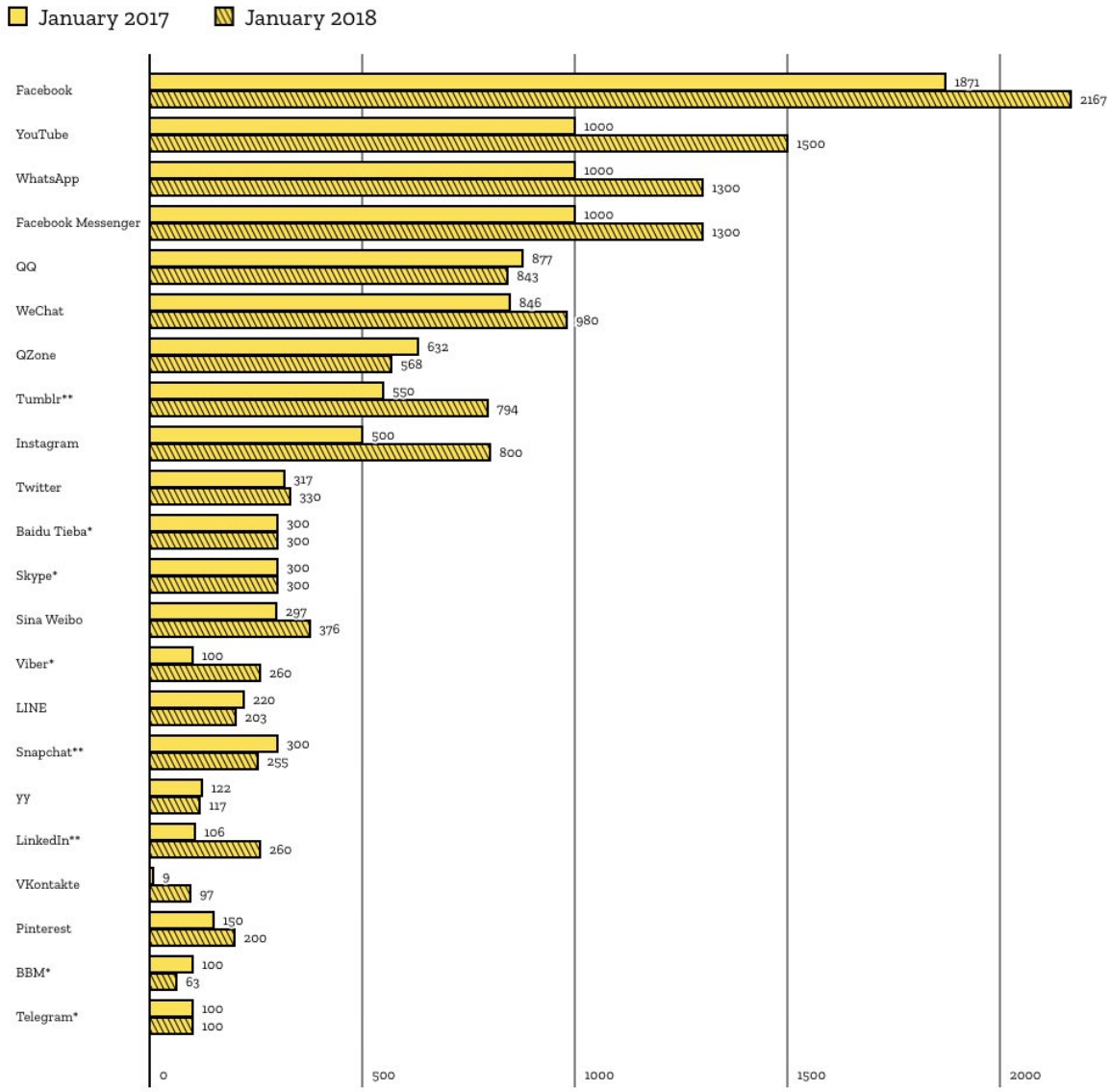
The majority of the world's 3.57 billion Internet users have accounts with one or more of the leading social media platforms. Facebook alone had 2.16 billion monthly active users at the end of 2017, and is the undisputed social media leader in terms of global reach and profitability.

Social media is used via the Web or mobile apps for messaging and content publishing, but the boundaries of what constitutes social media are getting blurry.

WhatsApp is used for private messaging, but also as a business platform and for discovering and consuming news. And WeChat, the biggest platform in China, can be used for virtually everything people do online, including shopping, banking and browsing the Web.

When just a few companies have control over the private communications and personal data, photos and videos of billions of people, they wield enormous power over markets, our experience of the open Web (or lack thereof), global public discourse, free speech and our personal lives. How we hold them accountable, and whether we have the information to do so, is crucial to the health of the Internet.

Active users of most popular social media networks worldwide

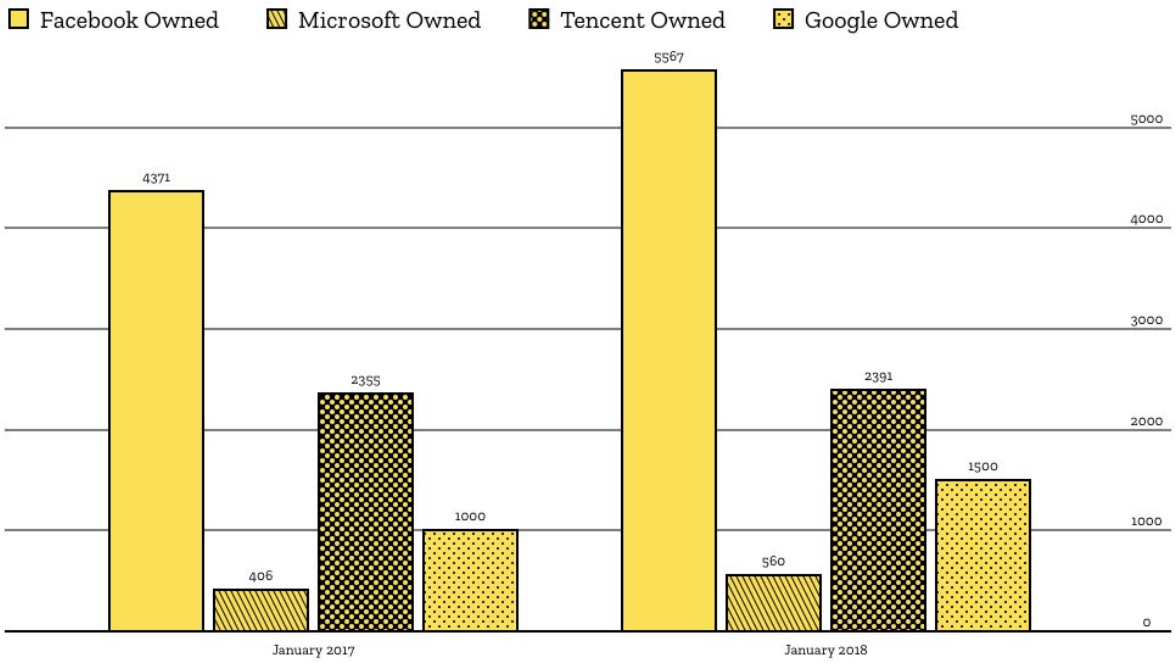


Data source: Monthly active users of the most famous social networks, Statista, January 2018

*Platforms have not published updated user figures in the past 12 months, figures may be out of date and less reliable. **These platforms do not publish MAU data, user figures from third-party reports

Three companies tower above all others in counts of combined monthly active users of the social media platforms they own. **Facebook** owns: WhatsApp, Facebook Messenger and Instagram. **Google** owns: YouTube, and **Tencent** owns: QQ, WeChat and QZone. Facebook is rocketing above the others, adding 1.196 billion users across its different platforms in just one year.

Social media networks of Facebook, Tencent and Google have the most active monthly users



Monthly active users (in millions)

Data source: Monthly active users of the most famous social networks, Statista, January 2018

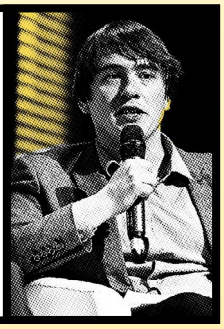
Read more online

Decentralization // Data

More than 90% of the world uses Google Search

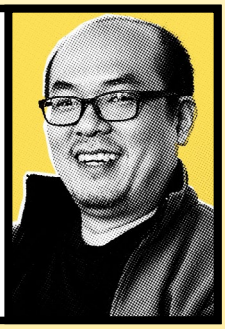
Decentralization // People

A citizen watchdog for net neutrality in Europe



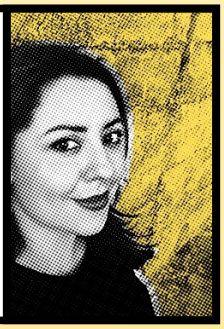
Decentralization // People

Building underwater drones together in China



Decentralization // People

Resisting digital colonialism

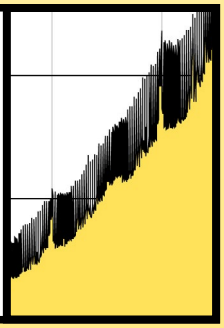


Decentralization // People

Software needs people +Blockchain"

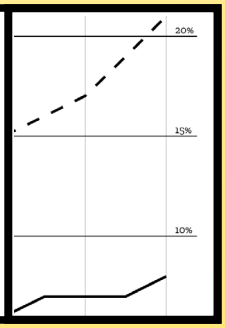
Decentralization // Data

An overdue Internet upgrade is underway with IPv6



Decentralization // Data

The Internet uses more electricity than..



Decentralization // People

The world's first ambassador to technology companies

Participate

What you can do

When you read the stories of this report, there's a good chance you'll end up asking the same question most of us do: What can I do?

Maybe you're concerned about a specific issue – like the spread of misinformation online, the privacy of your family, or you've had your Internet access blocked.

Perhaps you're already actively involved in building a healthier Internet, as an advocate, an educator, a policy maker, a journalist, a researcher, or something else.

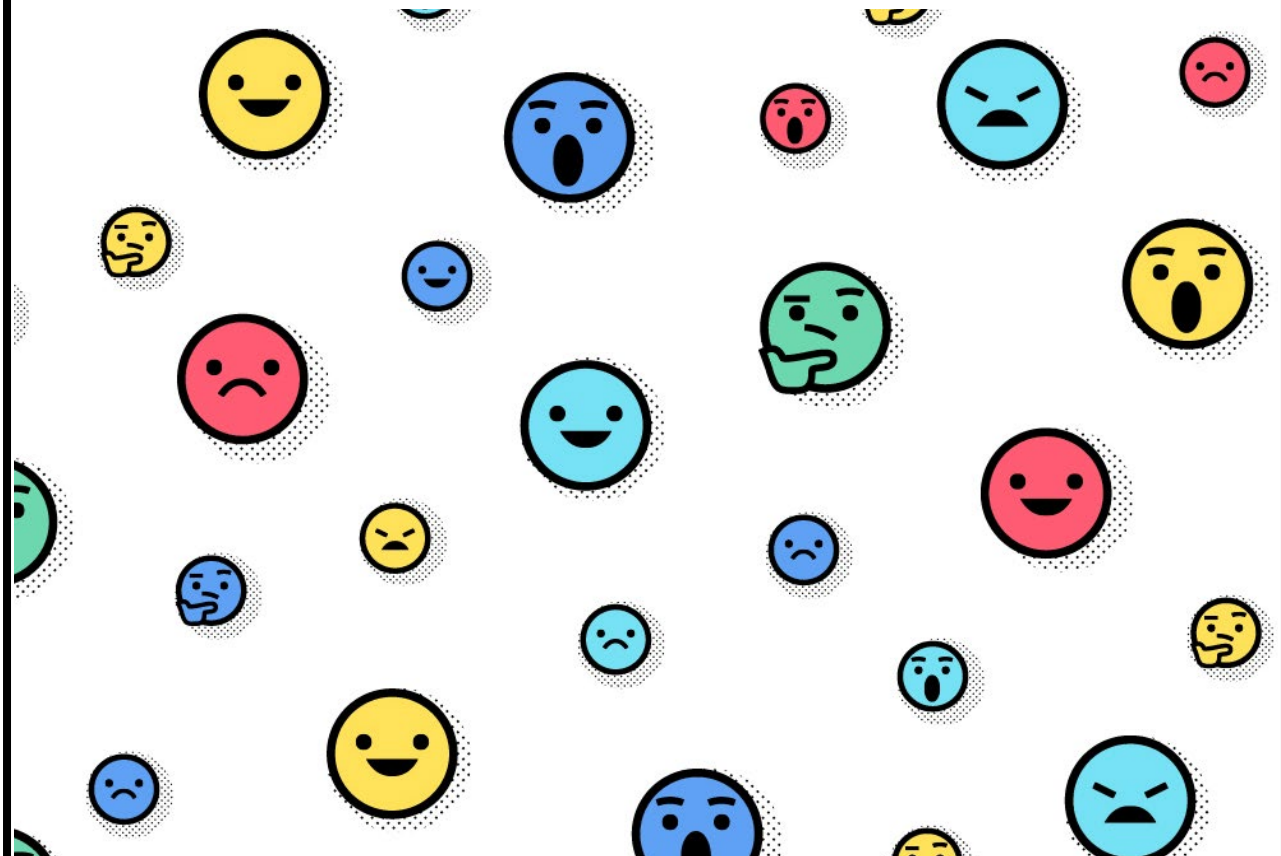
Or maybe you just want to better understand the technologies that affect your life and communities, and how you can shape the way you interact with them.

The Internet Health Report is a snapshot of what's happening to the health of the Internet right now. It's a collaborative effort, and representative of a broad range of voices across the field. We don't have all the answers. If anything, we're asking more questions.

But it's also a call to action. It's a challenge to each of us to learn more and to do more – to work together to create a healthy Internet that values people above everything.

In that spirit, here are some thoughts on how to meet that challenge.

- Model good practice
- Discuss and debate
- Roll up your sleeves



Model good practice

Make your personal Internet experience healthier for the sake of the whole ecosystem. You might get started by:

- Protect yourself and your devices with strong passwords and two-factor authentication.
- Always update your computer and phone software as soon as a security update is available to protect yourself and those around you.
- Learn how to identify online abuse, and what your rights are if you or someone you know is harassed online. You can also assist or volunteer with organizations that support victims.
- Explore what kinds of data companies like Google and Facebook are collecting about you, and select privacy settings you're comfortable with. Try a data detox?
- Improve your 'crap detection' skills and try to verify photos and videos before you share. Educate yourself about economic incentives that drive some misinformation.
- Make sure the website you own or administer is accessible only via https (encrypted). You can run a test here. If it's not, contact your hosting provider.
- Help support free and open voice technology by donating your voice recordings to the Common Voice project to teach machines how real people speak.
- Identify open source software you use regularly and support them with time, money or thanks. For example, you can edit Wikipedia or MDN Web docs or review code.

Discuss and debate

To make the Internet healthier, we need more people to understand and care – and then take action.

We hope the report can help you start conversations with others about how to build a healthier Internet, together.

We invite you to take this report and copy, repurpose, embed, debate, download, share, and write about it... or anything in between! We publish under a Creative Commons-Attribution license (CC BY 4.0) to encourage reuse.

Here are three ways to get started:

Discuss stories in this report. Change starts with action, and actions start with reactions. After you read an article, choose an emoji to share how you feel. Then pop into the comments to see what people are saying, and add your thoughts. Please keep our Community Participation Guidelines in mind!

Share your favorite stories. Pick a story or chart that fascinated you and send it around to your friends, or on social media. Look for the 'share' buttons at the bottom of each page.

Host a conversation in your community. We've developed lots of materials to help make this easy, including a slide deck and a guide to hosting events.

Roll up your sleeves

It's not all on you to make a difference. The Internet will only become much healthier through structural changes, thoughtful governance, and better protection of consumers of products and services everywhere. You can keep demanding that these things happen, and engage in efforts to collectively push for change.

Get involved with Mozilla

- Learn about Mozilla's policy initiatives and campaigns
- Apply to be a Fellow
- Become a Mozilla Open Leader
- Join us at Mozfest or the Global Sprint
- Explore more opportunities to help keep the internet healthy

Get directly involved

If you'd like to get involved on a specific issue, or are wondering about Internet health in your own area or country, we encourage you to engage with local digital rights groups. Start noticing who is speaking out on these topics in the news and reach out to them.

The people and organizations we featured in this year's report are good places to start.

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 in a public comment online, or send us an email: internethealth@mozillafoundation.org.

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