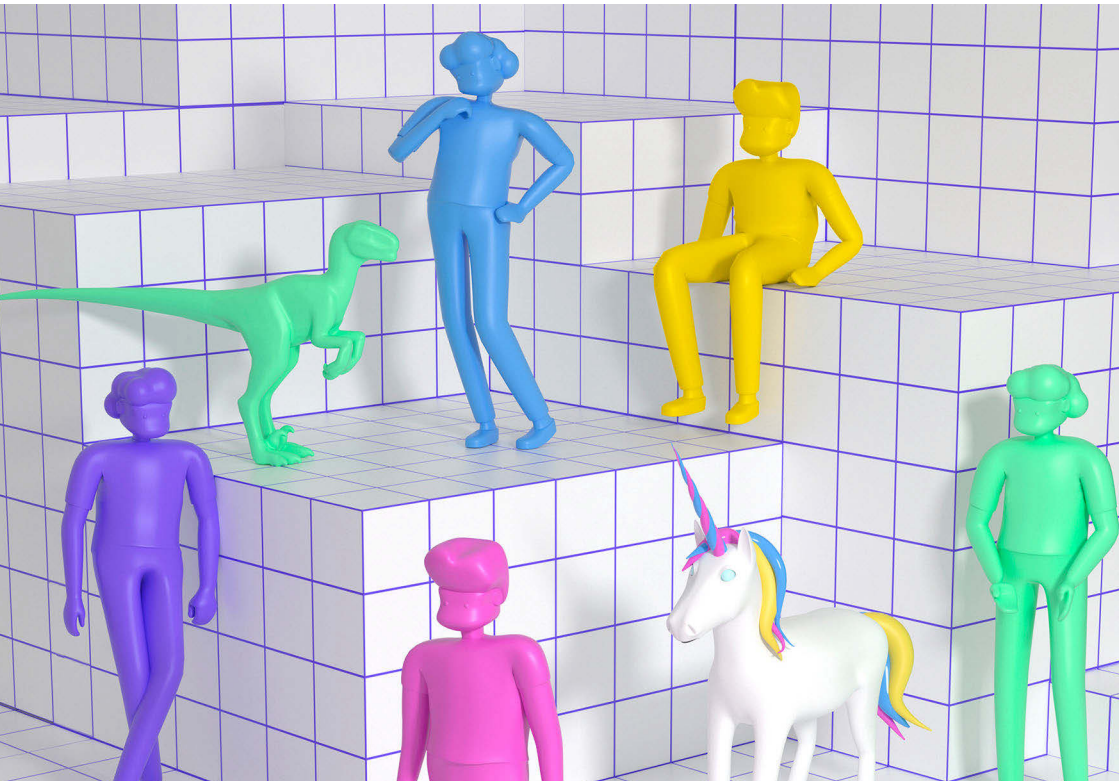
## Who is welcome?

### 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/