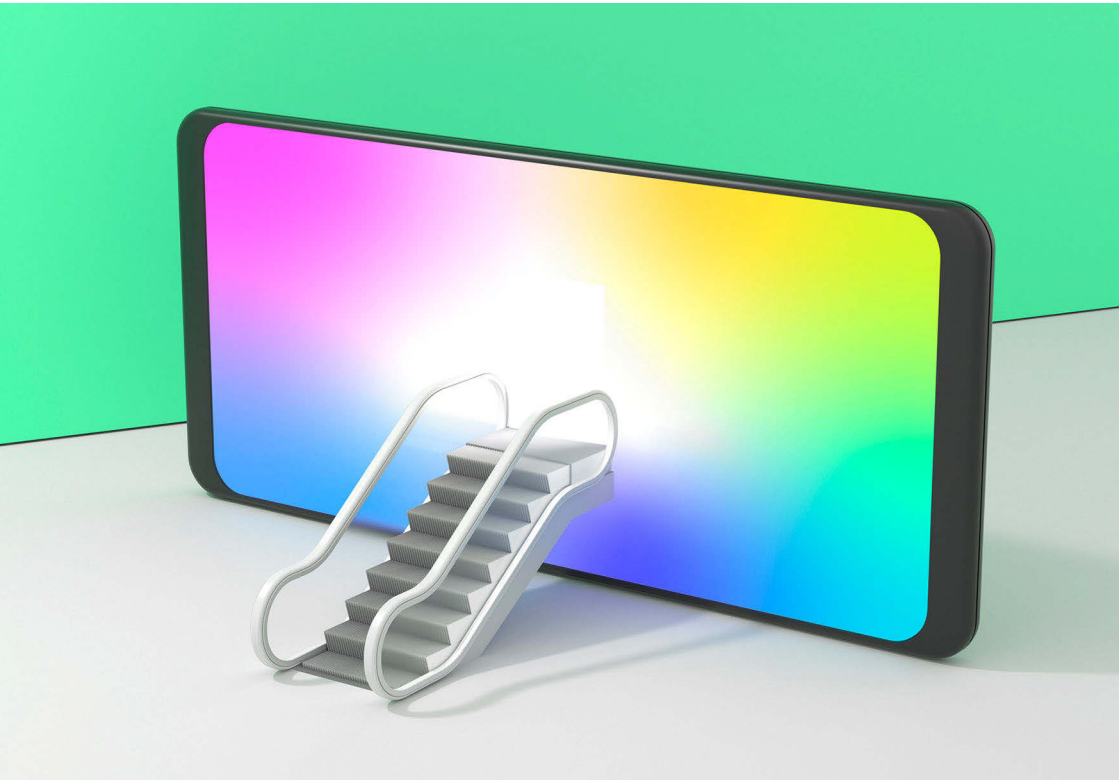
Who can succeed?

Understand the issue: Web literacy



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

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

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

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

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

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

It's critical that we understand how the internet is impacting our societies – and are ready to demand change when necessary. In most countries, the internet is both helping and hurting democratic processes. There is greater access to information about candidates, more transparent public data and new avenues for grassroots organizing. But it also facilitates election interference and the spread of harmful disinformation.

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

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

We can imagine different worlds. We can demand change.

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

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

Sex education in the digital age

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

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

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

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

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

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

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

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

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

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

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

"If they were flush with knowledge when they first encounter pornogaphy, they would be inoculated against some of the worst potential influences," says Rothman.

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

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

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

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

► Further reading

- 10 years on: why we still need better sex education for the digital world, Jessica Ringrose, Amelia Jenkinson, Sophie Whitehead, IOE London Blog, UCL Institute of Education, 2019. https://ioelondonblog.wordpress.com/2019/03/17/10-years-on-why-we-still-need-better-sex-education-for-the-digital-world/
- What Teenagers Are Learning From Online Porn, New York Times, 2018. https://www.nytimes.com/2018/02/07/magazine/teenagers-learning-online-porn-literacy-sex-education.html
- Porn and sex education, porn as sex education, Kath Albury, UNSW Sydney, 2014. https://www.researchgate.net/publication/264558246_Porn_and_sex_education_porn_as_sex_education
- Adolescent Pornography Use and Dating Violence among a Sample of Primarily Black and Hispanic, Urban-Residing, Underage Youth, Emily Rothman and Avanti Adhia, Behavioral Sciences, 2016. https://www.mdpi.com/2076-328X/6/1/1

Who babysits your children's data?

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

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

A 2018 report by the Children's Commissioner for England, "Who knows what about me?", found that the average person in the United Kingdom will have 70,000 posts shared about them online by the time they turn 18. Highlighting the risk of this, Barclays Bank forecasts that "sharenting" (meaning parents who share info about their children) will be the cause of two-thirds of identity fraud and financial scams facing young people by the end of 2030.

Children themselves are growing up to discover information about themselves online they wish could be erased. From the Austrian teen who sued her parents for posting hundreds of photos of her with their 700 social media contacts (including of her using the bathroom) to the fourth grader who asked her columnist mother to stop sharing private stories and photos.

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

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

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

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

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

Perhaps the simplest of all? Think hard before you post anything about children online. Is this something their future friends or employers might see? A healthy internet is one where we feel comfortable with the information shared about ourselves and our families, whether we are children or adults.

► Further reading

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

Decoding images of war in Syria

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

► Further reading

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

The challenge of democracy in the digital era

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

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

Today, this optimism has been tempered by the steady drip of news about election interference over the internet in the United States and countless other countries. It has awoken democratic institutions to new levels of concern. What happened in the 2016 presidential election in the United States

may have surprised many Americans, but it was hardly unique on the world stage.

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

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

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

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

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

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

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

In 2017 and 2018 Cambridge Analytica was also found to have collected data from users in India, Brazil, Indonesia and Mexico for campaign work.

The consulting firm also put down roots in Kenya. In a case study from current President Uhuru Kenyatta's 2013 election campaign, Cambridge Analytica described having built a strategy for the candidate "based on the electorate's needs (jobs) and fears (tribal violence)." This struck a chord for Kenyans, who have grown accustomed to social media sparking violence between different ethnic groups.

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

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

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

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

► Further reading

- Our Data, Ourselves: Politics and Data, Tactical Tech, 2019. https://ourdataourselves.tacticaltech.org/projects/data-and-politics/
- Digital Deceit: The Technologies Behind Precision Propaganda on the Internet, Dipayan Ghosh, Ben Scott, New America, 2018. https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/
- A multi-dimensional approach to disinformation, Independent high level group on fake news and online disinformation, European Commision, 2018. https://publications.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en
- Elections – Global Voices. https://globalvoices.org/-/topics/elections/

Spot the surveillance with virtual reality

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

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

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

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

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

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

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

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

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

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

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

► Further reading

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

Breaking free of the addiction machine

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

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

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

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

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

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

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

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

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

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

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

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

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

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

► Further reading

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