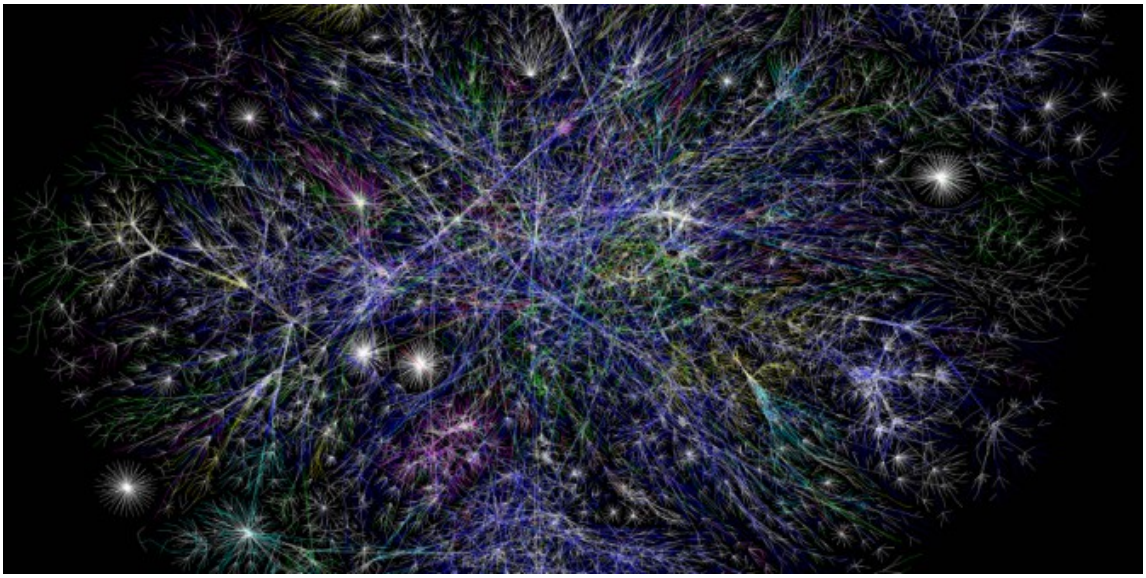
# Where is the internet headed?



Over the past few months, you've almost certainly heard someone lament the state of the internet.

It might have been a friend or family member, who learned the Facebook-Cambridge Analytica breach was worse than originally thought. Or maybe it was Twitter CEO and co-founder Jack Dorsey, who recently acknowledged his platform had been compromised by bots and trolls. Or perhaps you heard it from Tim Berners-Lee, inventor of the world wide web, who earlier this year wrote the web is "under threat" from big tech.

But it's not all bad news. The internet's original promise — a global public resource by and for its users — hasn't flickered out. Peer past the troubling headlines and you'll find positive ones, like new, strong data protection rules in Europe, bots that fight government corruption in Brazil, and free coding workshops for girls around the world.

In stories both good and bad, this much is certain: The internet is a force tied to all aspects of life. What happens online impacts our economies, our governments, and us personally. This connection is only growing deeper: In the coming years, billions more people will come online, and tens of billions more devices will further link the internet to our homes, cars, and relationships. Today, questions like "is the internet healthy or unhealthy?" aren't academic — they're existential. To ignore these questions is to jeopardise everything from our democracies to our economies our personal wellbeing.

So — *is* the internet healthy? And if not, what parts need immediate attention? These are complex questions. But the nonprofit I work at, Mozilla, is among the people and organisations seeking answers. We published the Internet Health Report on April 10, a sweeping survey of what's helping and hurting the internet. We compiled data from organisations like Access Now and the International Telecommunications Union. And we spoke with a diverse roster of experts: an engineer in Brazil, a cryptographer in Egypt, a cyber violence expert in Toronto, a journalist in Afghanistan. Through those conversations, a handful of the internet's most pressing issues — and potential solutions — emerged:

**Intelligent machines aren't always right**

Artificial intelligence is all around us — tucked into our car dashboards, living in home assistants like Alexa, or hard at work in our web browsers. AI is currently revolutionising everything from medicine to transportation.

Date originally posted: 2018-05-08

Permalink: http://blogs.lse.ac.uk/businessreview/2018/05/08/where-is-the-internet-headed/

Blog homepage: http://blogs.lse.ac.uk/businessreview/

But too often, cutting-edge AI technology is monetised and introduced to mass markets without a thorough understanding of its risks. The consequences can be dire: An algorithm meant to populate news feeds can instead promote lies and conspiracy theories. Or an algorithm meant to aid law enforcement can instead discriminate against African Americans. Compounding this problem: The realm of AI is highly centralised. The vast amounts of money and training data needed to develop intelligent machines mean only a few companies — Google, Facebook, Baidu — control most of the technology. Start-ups are left out, and Big Tech grows bigger.

There are solutions: By making the datasets that train AI open source, we can give newer, smaller AI companies a leg up. We should also hold AI accountable — we need diligent watchdogs and strict regulations to ensure it isn't discriminating. New York City is an exemplar: A new law is putting the algorithms the city uses to dispatch its public services under the microscope.

**Encryption is under siege**

As more and more personal data migrates online — from medical records and tax returns to family photos — strong security becomes paramount. And in the fight against thieves and snoops, encryption is a first line of defence. Cyber attacks affected hundreds of millions of people in 2017; without strong encryption, that number would be far higher.

Yet governments around the globe are actively *undermining* encryption. Anxious that encryption "enables criminals and terrorists," policymakers are pushing for backdoors — methods for law enforcement to circumvent encryption. Governments are also seeking out software vulnerabilities, and using those flaws to gain access to encrypted data. Countries that recently passed laws that erode encryption include China, Hungary, Russia and the United Kingdom.

Here's the problem: If governments mandate encryption backdoors, the bad guys will find them — and exploit them. Also, if governments hoard software vulnerabilities without giving companies the chance to fix them, the door is wide open for the bad guys to find and exploit these vulnerabilities, too. Policymakers around the world should be passing laws that strengthen encryption, not undermine it. And policymakers should inform technology companies if they find a flaw, so it can be fixed immediately.

**'Fake news' is a symptom; treat the cause**

Fraud on social media — or "fake news" — has reached a fever pitch. Conspiracy theories and blatant lies thrive on social media, sowing discord, deepening partisan divides, and disrupting elections.

Governments are scrambling to find solutions. In Germany, a 2017 law requires major social media platforms to block or delete unlawful content — or face steep fines that range from 2.5 million to 40 million euros. Germany's law is already rippling across the world, with similar regulations taking shape in Russia, Kenya, and Venezuela.

While these laws aim to reduce misinformation, they also enshrine big technology companies as gatekeepers. Suddenly, corporations like Facebook and YouTube determine what constitutes "fake news" or "hate speech." The result might be less free expression, and more censorship, online.

Further, these laws treat the symptom — misinformation — and not the cause: the internet's hyper-targeted, ad-driven business model. Outrageous content generates more clicks and engagement. And more clicks and engagement generate more money. By building technology that values truth over outrage, or by teaching students how the internet really works, we can address misinformation more effectively.

These are just three trends shaping the internet in 2018. There are countless others, from global net neutrality laws to the proliferation of the Internet of Things. Every new technology and policy we introduce alters the internet ecosystem — and, in turn, ripples into billions of lives. As a result, technologists, policymakers, and everyday internet users need to ask the right questions — "is this healthy?" — early and often. And we need to commit to technologies and laws that uphold the internet's original promise: a global public resource by and for its users.

*Notes:*

- *This blog post is based on Mozilla's Internet Health Report.*
- *The post gives the views of its authors, not the position of LSE Business Review or the London School of*

Date originally posted: 2018-05-08

Permalink: http://blogs.lse.ac.uk/businessreview/2018/05/08/where-is-the-internet-headed/

Blog homepage: http://blogs.lse.ac.uk/businessreview/

*Economics.*

- *Featured image credit: Internet map, by Matt Britt, under a CC BY 2.5 licence, ()], via Wikimedia Commons*
- *When you leave a comment, you're agreeing to our Comment Policy*

---

**Solana Larsen** is the editor of Mozilla's annual Internet Health Report, a sweeping survey about what's helping and hurting the internet. She's a Danish-Puerto Rican journalist, editor and activist based in Berlin. For seven years, she was the managing editor of Global Voices, overseeing a virtual newsroom and online community of hundreds of volunteer writers and translators operating websites in 30 languages. She's a prolific public speaker on Internet health and digital rights.

Date originally posted: 2018-05-08

Permalink: http://blogs.lse.ac.uk/businessreview/2018/05/08/where-is-the-internet-headed/

Blog homepage: http://blogs.lse.ac.uk/businessreview/