

If You Want a Real Digital Commons, Build It Yourself

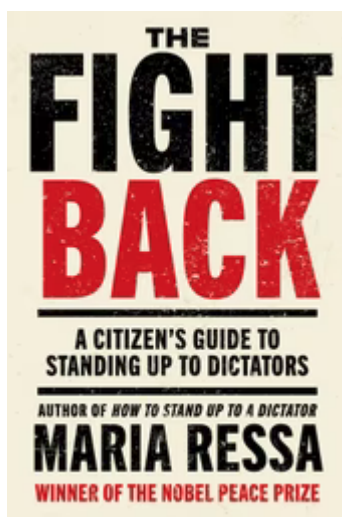
Maria Ressa

For more than a decade, the Philippines has been a test case for how technology enables an authoritarian state to capture and corrode the institutions that make democracy work. The work of Rodrigo Duterte, the autocratic president of the Philippines from 2016 to 2022, would hardly have been possible without that of Mark Zuckerberg, the CEO of what was then the most powerful social-media company.

The Philippine state used Facebook to turn bottom-up social-media attacks into lawfare. I experienced this firsthand as a co-founder and the CEO of the media organization Rappler. Facebook hosted a state-sponsored campaign of disinformation and harassment against us that culminated in criminal charges meant to send me to jail for the rest of my life. We fought back in courts and begged Facebook and YouTube to restore information integrity. After years of this, however, we realized that what we needed to do was to build an alternative to these platforms that would be responsive to the public good.

Infrastructure is law that doesn't pass through a courtroom. Whoever builds it makes the rules that no one ever voted on. The information infrastructure much of the world lives with today was built by tech oligarchs to maximize engagement and profit while concentrating power. For years, Rappler played whack-a-mole with the lies that permeated the digital commons. Then we realized that the only way to fix information integrity was to build our own tech: a virtual community anchored in facts.

This wasn't an easy decision. I had hoped that other, better-resourced companies would create the alternative. They didn't. So we did.



This article was excerpted from Maria Ressa's forthcoming book [The Fight Back: A Citizen's Guide to Standing Up to Dictators](#).

We built Rappler on three pillars: technology, journalism, and community. Remove any one of these and the structure fails. You can't base independent journalism on captured infrastructure. You can't host a community in a space that is designed to manipulate and incite you. You can't make technology serve

democracy unless governments, journalists, and citizens build it together.

We started with technology. Not because it's the most important pillar—though it may well be—but because it's necessary for all of the others. When digital platforms are captured, journalism's distribution is held hostage. When distribution is captured, community dissolves. When community dissolves, institutions lose the base that makes them legitimate. Technology is where democracy's body meets its nervous system.

Facebook failed Rappler. Rappler's eventual answer was to stop asking Facebook or any other platform to moderate better. Instead, we realized that we needed to stop using Facebook as our public square.

Put another way, the arsonist will not save the village. So we need to build a new village, with firebreaks and firewalls. Our method was to start small, protect the facts, and separate from algorithmic and digital manipulation.

In software jargon, a “stack” is the layered collection of technologies that make something work: chip, operating system, application, one on top of the other. Whoever owns the bottom of the stack decides what can be built above it. In the United States, Donald Trump is building an authoritarian stack. The breakneck advances in agentic AI have made this effort even more worrying than it already was.

The president has appointed the CEOs of the major tech companies to his council of advisers on science and technology. Mark Zuckerberg of Meta, Larry Ellison of Oracle, Jensen Huang of Nvidia, and a long list of others on the council are the very people who shape what billions of people already see, feel, and believe. Now they formally advise the president on the technology that will shape what we all see, feel, and believe next.

[From the March 2024 issue: The rise of techno-authoritarianism](#)

The industry's influence was apparent when the White House released its national-policy framework for AI in March. The document seemed to identify the central risk of the new technology as its possible coercion of social-media platforms—the very outlets that themselves coerce citizens through algorithms, surveillance, and engineered outrage.

The technology that mediates our thinking has become a weapon in the hands of the state that was supposed to regulate it. The biggest AI firms are spending billions on tech infrastructure and millions to defeat candidates who support state-level AI regulation in the 2026 midterms. Meta's AI is deployed across U.S. defense contractors, and OpenAI was named to the Pentagon's classified network vendor list in May 2026.

This is the authoritarian stack: regime power and tech power, formally merged. And the fusion didn't happen by accident. It happened because the alternative—a democratic stack, constructed and owned by the people who depend on it—was never built at the scale required. We have to build it now.

That's what we did in the Philippines. I co-founded Rappler in 2011 as a technology company as much as a newsroom. Even then, we understood that the battle for truth would be fought on digital terrain, and that a newsroom that didn't control this terrain would eventually not control its journalism. In 2016, Rappler came under coordinated social-media attack from the Duterte government, and we shifted from seeking to generate traffic through polluted social-media platforms to relying on search engines instead. Optimizing our

content for search visibility allowed us to generate as much as 69 percent of our traffic from what seemed at the time like a more reliable source.

But that loophole would soon vanish as Big Tech sought to choke off digital news distribution. By 2024, Google had launched its AI-driven, zero-click search, which answered queries without sending readers to the sources of the information it displayed. By early 2026, the floor had fallen out from under every search-dependent publisher. So we stopped trying to reform the platforms that were killing us and started building beside them.

We made an archive of everything Rappler had ever published and a structured catalog of the topics, places, and events we covered. In 2024, we rolled out our own fact-based chatbot, which we named RAI, Rappler Artificial Intelligence. Because we owned our own data and combined them with publicly available, vetted databases, our chatbot's error rate was a little more than 1.6 percent—at the time, the error rate of commercial chatbots was about 16 percent. We began to see a path ahead for journalism: Some of our global partners have more than a century of archived reporting, a record of verified facts no commercial-AI system can match.

Rappler developed its own town square, in the form of a chat app that runs on the Matrix protocol. Matrix is open-source and allows users to set up their own communication servers. More important, it isn't owned by any single company. No algorithm decides what users see, and conversations can be encrypted from end to end. Journalists set the rules for Rappler's community, and our own team enforced them, using AI to assist but reserving the final word for humans. The result was a conversation anchored by facts instead of engagement-driven outrage.

In September 2025, our one-newsroom experiment expanded into Rappler Communities. We created a network of trusted newsrooms, including the Philippine Press Institute, which encompasses 65 newspapers; SunStar Cebu, the flagship of a community-news network across 12 Philippine cities; and the *Daily Guardian*, the leading newspaper of Western Visayas. Rather than depending on platforms that monetized journalism's decline, we shared a distribution infrastructure that we owned ourselves.

Now a reader in Iloilo could follow a *Daily Guardian* story, join a SunStar thread in Cebu, and surface in a Rappler national discussion—all without changing apps, surrendering data, or being sorted by an algorithm into the part of the conversation that would make them angriest. Local journalism reached a national audience. National journalism gained local depth. Readers were no longer a product: They were citizens in a shared civic space.

The authoritarian stack isn't going to disappear. But independent news organizations can work together to build a true digital commons alongside it. The key is federation—the structural opposite of monopoly. Each member of a federated network governs itself. But using open standards, all of them communicate with one another, so that users can move among them without losing their data or their connections.

[Maria Ressa: How to fight fascism before it's too late](#)

This is how email works, and the way the early internet worked. The model has recently spread to social

media, where decentralized platforms, built on open standards rather than owned by a single company, are entering the mainstream. Three years ago, Bluesky was a technical experiment. Now it's a parallel public square, with nearly 44 million users as of April 2026, many of them newsrooms and journalists.

A growing ecosystem of public-interest technology organizations has been working to build alternatives to monopoly-owned tech—to defend civil liberties in courts and policy, preserve the public record, protect journalists and dissidents from surveillance, and keep open the parts of the internet that Big Tech has no commercial interest in maintaining. The encrypted-messaging app on your phone, the browser that doesn't sell your data, the archive that remembers what was deleted, the lawsuits that challenge mass surveillance—all of these things come from this small coterie of companies. Among its members are Signal Foundation, Mozilla, Wikimedia Foundation, Internet Archive, Electronic Frontier Foundation, Tor, Open Technology Fund, Access Now, Knight Foundation, Global South Alliance, Innovation for Change, Civic Tech Lab, and many more. They have small budgets but carry enormous weight.

Rappler, of course, is part of this ecosystem. In 2023, the year that Twitter became X, we rolled out Rappler Communities, now called MUNI. On February 10, 2025, two years after Elon Musk began firing 80 percent of his platform's safety engineers, the digital-safety expert Camille Francois at Columbia University's School for International and Public Affairs spearheaded an engineering nonprofit called Robust Open Online Safety Tools. ROOST supplies organizations with free, open-source software to detect, report, and remove material they define as harmful, such as child-sexual-abuse material, from their AI and social-media platforms. It also furnishes the means to handle online harassment: software to flag bad behavior automatically, queues for human reviewers, and consoles for the moderators who make the final call.

A small newsroom or a new platform that could never have afforded its own safety team can now download and run the same tools the biggest platforms use. Many major platforms that are normally competitors chose to join ROOST as partners, whether by donating funds or technology or by using its safety tools: Discord, Google, OpenAI, Microsoft, Roblox, Bluesky, Mozilla, Hugging Face, Wikimedia, Matrix, Common Crawl. The problem of online safety is bigger than any one of these companies—and everyone benefits from a safety baseline that is open, shared, and built by people whose first loyalty is not to shareholders or authoritarian regimes.

What is needed for information platforms is that much more urgently required for AI. That's because the new-frontier AI models don't just shape what you read and influence your opinions: They act on your behalf, reading your email and deciding what's important, booking your travel, answering your messages, making purchases. AI schedules your week and negotiates with vendors, airlines, and other people's agents. It becomes *you* in digital space.

This is the deepest, and scariest, form of infrastructure capture of all. If you rent your chat platform, you outsource your public square. If you rent your agent, you outsource your judgment.

[David Robinson: I quit OpenAI because its culture is broken](#)

The question is not whether the agents will be powerful. They already are. The question is, who will they be loyal to? To you or the company that built them, the platform that hosts them, the advertiser that paid for

placement, the state that subpoenaed access? Or to themselves? The handful of companies that own and build these agents now sit on the council advising the U.S. president on AI policy. No independent body checks their work.

Civic actors must construct an alternative infrastructure rather than waiting for the corporate one to reform. This means acting on three levels at once. AI is built on a training layer, involving decisions about what the models learn from. Then comes the deployment layer, addressing questions about how the technology is used and under what limits, decided by whom. The third layer has to do with accountability: To whom do AI agents answer—what happens, and who is held responsible, when they escape human control?

We should have asked these questions about social media in its infancy. Most of us failed to, until it was too late. This time, however, the work has begun. Public-interest AI projects—ROOST’s open-source safety infrastructure, the Allen Institute, Hugging Face’s open-model work, Mozilla’s AI initiatives—are punching far above their budgets. Open-source agentic frameworks are flourishing—and could eventually become conduits for journalism, civic information, legal aid, and health-care navigation in the public interest.

The danger, though, is that agents are moving faster than the safety work around them. OpenClaw, an open-source AI assistant you can host on your own computer, went from launch to nearly a quarter of a million GitHub stars in four months. The window between “this is a hobby project” and “this is global infrastructure” is now measured in weeks. But though it is narrow, that window is still open—which is why the time to act is now.

This article was excerpted from Maria Ressa’s forthcoming book [The Fight Back: A Citizen’s Guide to Standing Up to Dictators](#).



By Ressa, Maria

When you buy a book using a link on this page, we receive a commission. Thank you for supporting The Atlantic.