

# Moral Suasion

## THE LIFE OF A MODERN-DAY MAKER

is greatly eased by the abundance of free or cheap services for hosting communities, files, communications, and computation. But for all the promise of cloud computing, there's plenty of peril, too, especially for anyone doing anything disruptive.

Will your "cloud" evaporate the second your project starts attracting legal threats? Does a service provider with a million customers care about your customs enough to keep you online even if it means risking a police raid, subpoena, or denial-of-service attack?

The ongoing WikiLeaks fight is a wake-up call for anyone who's been blithely relying on the cloud. It only took a few days for WikiLeaks to become a digital refugee, slogging from one service provider to the next, trying to find someone with enough backbone to keep it online in the face of legal threats, political intervention, and mysterious traffic-floods from persons or governments unknown.

But WikiLeaks wasn't without its defenders. "Hacktivists" operating under the Anonymous banner organized mass denial-of-service attacks on Amazon, PayPal, Visa, MasterCard, and other firms that kicked WikiLeaks out or refused to process their payments.

Distributed denial-of-service (DDoS) attacks are a strange beast, unique to the online world. Some DDoSes are the work of millions of users acting in concert to flood a server with so much traffic that it falls over. More commonly, DDoS attacks are the work of vandals or crooks who use clouds of hacked PCs to attack their targets.

Some hacktivists argue that their DDoS attacks are comparable to the civil-rights-era sit-ins — after all, a wall of activists blockading the doors to a "whites-only" lunch counter is a kind of denial-of-service attack.

I think they're wrong. I grew up in the antiwar

movement and participated in my first sit-in when I was 12. Sit-ins are a sort of denial of service, but that's not why they work. What they do is convey the message: "I am willing to put myself in harm's way for my beliefs. I am willing to risk arrest and jail. This matters."

This may not be convincing for people who strongly disagree with you, but it makes an impression on people who haven't been paying attention. Discovering that your neighbors are willing to be harmed, arrested, imprisoned, or even killed for their beliefs is a striking thing.

---

## A wake-up call for anyone who's blithely relying on the cloud.

---

And that's a crucial difference between a DDoS and a sit-in: participants in a sit-in expect to get arrested. Participants in a DDoS do everything they can to avoid getting caught.

If you want to draw a metaphor, DDoSers are like the animal rights activists who fill a lab's locks with super glue. This is effective at shutting down your opponent for a good while, but it's a lot less likely to draw sympathy from the public, who can dismiss it as vandalism.

One thing is clear: those of us who don't supply our own digital infrastructure depend on intermediaries who are increasingly willing to roll over at the slightest pressure.

It's time to start devoting some of our creative attention to ways of clearing away the choke-points and leaning back on those companies that are getting leaned upon by powerful, established forces. [▶](#)

---

Cory Doctorow's latest novel is *Makers* (Tor Books U.S., HarperVoyager U.K.). He lives in London and co-edits the website Boing Boing.