

I helped invent the internet. How did it go so wrong?

- Facebook, Google-YouTube, Netflix, Linked-In and the sociopath Sandhill Road VC's turned it into a sex-trafficking, spy-ridden, election-meddling hell and the politicians that those companies bribe like to keep it that way!

 Silhouette of a male hand typing on a keyboard

Scientists inadvertently created the perfect formula for the “dark” side of the internet to spread like a virus by enabling anyone to reach millions of people inexpensively and anonymously.

(Rafe Swan / Getty Images/Cultura RF)

By Leonard Kleinrock

When I was a young scientist working on the fledgling creation that came to be known as the internet, the ethos that defined the culture we were building was characterized by words such as ethical, open, trusted, free, shared. None of us knew where our research would lead, but these words and principles were our beacon.

We did not anticipate that the dark side of the internet would emerge with such ferocity. Or that we would feel an urgent need to fix it.

How did we get from there to here?

While studying for my doctorate at MIT in the early 1960s, I recognized the need to create a mathematical theory of networks that would allow disparate computers to communicate. Later that decade, the Advanced Research Projects Agency — a research funding arm of the Department of Defense created in response to Sputnik — determined they needed a network based on my theory so that their computer research centers could share work remotely.

My UCLA computer lab was selected to be the first node of this network. Fifty years ago — on Oct. 29, 1969 — a simple “Lo” became [the first internet message](#), from UCLA to Stanford Research Institute. We had typed the first two letters of “login” when the network crashed.

This quiet little moment of transmission over that two-computer communication network is regarded as the founding moment of the internet.

During [its first 25 years](#), the internet grew dramatically and organically with the user community seeming to follow the same positive principles the scientists did. We scientists sought neither patents nor private ownership of this networking technology. We were nerds in our element, busily answering the challenge to create new technology that would benefit the world.

Around 1994, the internet began to change quickly as dot-coms came online, the network channels escalated to gigabit speeds and the World Wide Web became a common household presence. That same year, Amazon was founded and Netscape, the first commercial web browser, was released.

And on April 12, 1994, a “small” moment with enormous meaning occurred: The transmission of the first widely circulated spam email message, a brazen advertisement. The collective response of our science community was “How dare they?” Our miraculous creation, a “research” network capable of boundless computing magnificence had been hijacked to sell ... detergent?

By 1995, the internet had 50 million users worldwide. The commercial world had recognized something we had not foreseen: The internet could be used as a powerful shopping machine, a gossip chamber, an entertainment channel and a social club. The internet had suddenly become a money-making machine.

With the profit motive taking over the internet, the very nature of innovation changed. Averting risk dominated the direction of technical progress. We no longer pursued “moonshots.” Instead advancement came via baby steps — “design me a 5% faster Bluetooth connection” as opposed to “build me an internet.” An online community that had once been convivial transformed into one of competition, antagonism and extremism.

And then as the millennium ended, our revolution took a more disturbing turn that we continue to grapple with today.

By suddenly providing the power for anyone to immediately reach millions of people inexpensively and anonymously, we had inadvertently also created the perfect formula for the “dark” side to spread like a virus all over the world. Today more than 50% of email is spam, but far more troubling issues have emerged — including denial of service attacks that can immobilize critical financial institutions and malicious botnets that can cripple essential infrastructure sectors.

Other dangerous players, such as nation-states, started coming onto the scene around 2010, when [Stuxnet malware](#) appeared. Organized crime recognized the internet could be used for international money laundering, and extremists found the internet to be a convenient megaphone for their radical views. Artificial intelligence, machine learning, facial recognition, biometrics and other advanced technologies could be used by governments to weaken democratic institutions.

The balkanization of the internet is now conceivable as firewalls spring up around national networks.

We could try to push the internet back toward its ethical roots. However, it would be a complex challenge requiring a joint effort by interested parties — which means pretty much everyone.

We should pressure government officials and entities to more zealously monitor and adjudicate such internet abuses as cyberattacks, data breaches and piracy. Governments also should provide a forum to bring interested parties together to problem-solve.

Citizen-users need to hold websites more accountable. When was the last time a website asked what privacy policy you would like applied to you? My guess is never. You should be able to clearly articulate your preferred privacy policy and reject websites that don't meet your standards. This means websites should provide a privacy policy customized to you, something they should be able to do since they already customize the ads you see. Websites should also be required to take responsibility for any violations and abuses of privacy that result from their services.

Scientists need to create more advanced methods of encryption to protect individual privacy by preventing perpetrators from using stolen databases. We are working on technologies that would hide the origin and destination of data moving around the network, thereby diminishing the value of captured network traffic. Blockchain, the technology that underpins bitcoin and other digital currencies, also offers the promise of irrefutable, indisputable data ledgers.

If we work together to make these changes happen, it might be possible to return to the internet I knew.

Leonard Kleinrock is distinguished professor of computer science at the UCLA Samueli School of Engineering.