# Why the Internet's Infrastructure Is About to Be Disrupted

And how that could create opportunity for savvy entrepreneurs.

September 23, 2019 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

The internet was originally designed by U.S. military researchers to establish a communications channel in case of nuclear war. Sixty years later, the indexed web has spawned more than five billion pages, and American adults now spend 11 hours a day staring at screens, according to Nielsen.

The web intersects every area of modern life, but there are problems with the decades-old infrastructure, and it's creating opportunities for entrepreneurs who want to architect an Internet 3.0. Here are some of the catalysts (hopeful and worrying) for change, along with how savvy companies have capitalized on them.

## Discomfort With Human-Data Farming

In today's 24/7 connected world, the internet is no longer just an information highway. Big tech uses it to farm human data, creating friction between commercial interests and individual privacy. Take Facebook's Cambridge Analytica scandal in 2018, where the data of 50 million users was collected and used without consent. Facebook may be a free service, but people are uncomfortable being sold as human data products to advertisers.

Entrepreneurs are already creating solutions to protect privacy. Virtual Private Network (VPN) startups such as NordVPN, TunnelBear, TorGuard and Proton are considered among the elite at securing online privacy and safety. Each of these can be activated to anonymize a person's identity, data and geo-location when using public Wi-Fi, which are easily compromised by hackers.

**Related: Is Your Business Ready for the Internet of Things?**

ProtonVPN integrates with Tor anonymity network. Swiss-based Proton has also built ProtonMail, which protects data under strict Swiss privacy laws. It's perhaps the most secure email platform for civilians. The firm provides end-to-end encryption of all communications and anonymizes email by not keeping internet protocol (IP) logs.

So how prudent are VPN tools? Consider that internet service providers can actually sell your browsing history, and the wealth of data found therein that can be used to advertise products, but also to steal sensitive info. Google is reportedly developing a privacy-focused dashboard on its Chrome browser that allows users to reject tracking cookies. That seems way too late given where we are with privacy and data security. For now, users can take extra precaution when using social networks by not publicly disclosing sensitive data that could jeopardize one's identity or safety.

# Decentralization Disruption

Many technologists no longer see a centralized internet as an appropriate one-size-fits-all approach. Decentralized blockchain networks are shaping Internet 3.0. These remove the need for trust in third parties. San Francisco-based blockchain startup NOIA Network, for instance, has an ambitious mission: to revamp the internet's underlying routing protocols, which the founders believe have grown inefficient and ineffective. So what's the problem? The internet is made

up of thousands of physically interconnected cables. It’s fragmented because networks differ in size, capacity, density and distances. Therefore, NOIA proposes a “programmable internet” that uses IPv6 protocol (which expands packet size), as well as segment routing. The combination allows for the programming of routing information at the packet level.

There’s not much retail internet users can do at this juncture, although a clear long-term preference for decentralized services would create a customer mandate for the marketplace to move in the same direction. The currently fragmented and old-school web designs are limiting performance. Ventures such as NOIA want to use blockchain to architect a decentralized internet transit exchange where providers and data centers can make the web more efficient through the buying and selling of internet access points. If successful, such a disruption could reverberate throughout the industry.

**Related: Beef Up Your Online Privacy With VPN**

# The Rise of Censorhip

Online censorship is a growing concern outside of Western democracies, which leads to a few problems. As an information highway, the internet can be manipulated as a source of inaccurate information as governments push their propaganda. Secondly, censorship coerces people into silence, to communicate false views and/or to (negatively) alter behavior, rather than sharing knowledge or authentic views on topics that shape their lives, such as an election or policy referendum.

That’s why Unstoppable Domains is creating new infrastructure and ecosystem around blockchain domains, which the founders envision will lead to a free-speech internet. Such domains are similar to cryptos in that they’re fully controlled by passwords. The California-based venture, which has offices in

Europe, received $4 million in funding by Silicon Valley investor Tim Draper.

If users widely adopt such technologies, it’ll spawn copycat projects that will lead to growth of uncensorable privacy platforms. Interestingly, such tech may often clash with entrenched bureaucracies whose interests lay in monitoring information 24/7, presumably to stop money laundering and terrorism.

At this time, unregulatable platforms are gradually attracting more users, but they aren’t going viral, either. Bad user experience, lack of education and complexities in using such platforms are limiting adoption to hardcore enthusiasts. Moreover, there’s much resources devoted to surveillance systems. Detection technologies can identify the use of VPNs and TOR browser, making it harder for individuals to circumvent internet firewalls. And regulatory bodies are requiring enhanced due diligence and electronic know-your-customer protocols that ascertain user identities. U.S. lawmakers are unlikely to roll back these practices. Technological advances are improving internet designs and practices, but today’s regulatory environment risks slowing the pace of change.

https://www.entrepreneur.com/article/337205