Free Speech is only as Strong as the Weakest Link

Speech on the Internet requires a series of intermediaries to reach its audience. Each intermediary is vulnerable to some degree to pressure from those who want to silence the speaker. Even though the Internet is decentralized and distributed, "weak links" in this chain can operate as choke points to accomplish widespread censorship.

The Internet has delivered on its promise of low-cost, distributed, and potentially anonymous speech. Reporters file reports instantly, citizens tweet their insights from the ground, bloggers publish to millions for free, and revolutions are organized on social networks. But the same systems that make all of this possible are dangerously vulnerable to chokeholds that are just as cheap, efficient, and effective, and that are growing in popularity. To protect the vibrant ecosystem of the Internet, it's crucial to understand how weaknesses in the chain of intermediaries between you and your audience can threaten speech.

Each of the links above represents a link in the chain of intermediaries that directly facilitate or indirectly support speech on the Internet. Click the **names** of the links to learn the role that these intermediaries play, and how and why they may be targeted.

Webhosting Services

Web hosting services provide users with the ability to host their own websites. They can be small, like the free, advertising-supported services Angelfire or Tripod.com, or they can be bigger operations like Go Daddy that provide more extensive services like business software packages and cloud processing.

Web hosting services **are often the receipients of defamation or copyright infringement claims**, demanding the immediate takedown of hosted material. Sometimes these takedown requests come from companies angry that a web host is providing access to allegedly copyrighted material or to a speaker's criticism of their corporate practices. Other takedown requests come from users upset at alleged defamation or what they see as offensive content. Political content can be especially vulnerable with the weight of a big government behind a demand for censorship.

Despite their business relationships with their users, some web hosts may **fail to stand up for the speech rights of their customers** when they receive legal threats – even though the web hosts may have legal protections to insulate them from liability without removing the material.

Web hosting customers should be aware of their rights both as users, per a site's terms of service (if they are favorable), and any relevant law (like the Communications Decency Act § 230 or DMCA safe harbors).

Examples of Targeting Web Hosting Services

When a blogger at www.spockosbrain.com criticized one of ABC's affiliates, the broadcasting company sent a cease and desist letter to the blog's host, 1 & 1 Internet, **which promptly shut down the blog** – even though the host had no risk of liability under U.S. law.

Upstream Providers

Online speech must travel through several "upstream" providers before reaching its audience. Each of these links in the chain may itself rely on its own upstream providers -- for example, smaller ISPs may simply connect users to larger ISPs, or hosting platforms may host their services on servers leased from a commercial datacenter.

When at first they don't succeed, censors try again upstream. The Internet's strength lies partially in the fact that no single entity provides all the services necessary for the network to operate. The downside of this decentralization is that there are multiple intermediary points between any two users at which a third party may attempt to cut off speech. If the party seeking censorship meets resistance at any given link, they may simply move further up the chain and try again.

The further away from the user a service provider is located on the chain, the less incentive that provider has to push back against censorship of the user's speech. And even if an upstream provider wanted to defend its users, the cost of doing a fair use analysis or defending a lawsuit is frequently more than they are charging any customer. As a result, upstream providers will often take the cheaper option of removing content or banning users.

Unfortunately, upstream censorship can silence not only the targeted user but also hundreds or even thousands of uninvolved websites and users. To comply with a takedown request, a web hosting service may be forced to disconnect an entire website because it is not technically capable of removing specific content or web pages. It gets worse if the requester moves upstream to the hosting service's ISP, which could shut down the hosting service's entire connection and take hundreds of "innocent bystander" websites offline in the process.

Users whose speech is stifled by one upstream provider can sometimes switch to a different service after being censored. This solution is not only time- and resource-consuming, however, but probably only temporary as censorship-seeking parties chase them from one provider to the next. Users should look for a chain of providers that is committed to scrutinizing censorship requests, notifying and working with users to assess the situation, and defending customers when a request is illegitimate.

Examples of Targeting Upstream Providers

Unhappy that its global law enforcement guide had been published online by Cryptome.org, Microsoft sent a DMCA takedown notice to Network Solutions, Cryptome's DNS and hosting provider. Even though Cryptome's act was likely a protected fair use, Network Solutions asked Cryptome to remove the guide. When Cryptome refused, Network Solutions pulled the plug on the *entire* Cryptome website -- full of legal content -- because Network Solutions was not technically capable of targeting and removing the single document. The site was not restored until wide outcry in the blogosphere forced Microsoft to retract its takedown request.

When the Chamber of Commerce sought to silence a parody website created by activist group The Yes Men, it sent a DMCA takedown notice to the Yes Men's hosting service's upstream ISP, Hurricane Electric. When the hosting service May First/People Link resisted Hurricane Electric's demands to remove the parody site, Hurricane Electric shut down MayFirst/PeopleLink's connection entirely, temporarily taking offline hundreds of "innocent bystander" websites as collateral damage.

Domain Name System (DNS)

The Domain Name System (DNS) is a system for converting human-readable host names and domain names (like www.eff.org) into the machine-readable, numeric Internet Protocol (IP) address of a server or other device (like 64.147.188.3), which is used to point computers and other devices toward the correct servers on the Internet. At the heart of the system are the DNS servers that manage vast databases that map domain names to IP addresses. They are highly centralized, which makes them easy targets for Internet censors.

DNS makes it possible for users and computers to access different places or devices on the

Internet without having to remember millions of different IP addresses and server locations themselves — basically, it is a directory for the Internet. When it is compromised or censored, users will have difficulty **accessing certain sites and domains**, unless, in some instances, they can use alternate DNS servers and proxies.

On a small scale, ISPs may choose to, or be ordered to, **filter content**, like pornography or websites accused of copyright infringement. ISPs do this by preventing DNS servers under their control from resolving users' requests for a website to the proper IP address – the site is still there, but users can't get to it be using the site's domain name. This can prevent users from accessing lawful as well as unlawful speech, in part because it is often easier for ISPs and governments to **prevent access to entire domain names, including lawful speech on** rather than precisely block access to specific objectionable content.

Larger scale DNS censorship is common in countries like Iran and China whose governments use their control over Internet infrastructure to suppress material that they find objectionable, whether **political speech or content they consider immoral**. Many other countries, like Belgium and Norway, use less pervasive (but still questionable) DNS censorship schemes targeting sites that are allegedly used to distribute child pornography. Some countries, including the United States, are considering DNS blocking as a strategy for **attacking intellectual property infringement**.

DNS censorship strategies also cause a great deal of **collateral damage**. For example, in addition to impeding access to lawful speech, interfering with the DNS may cause security problems, in part because it will spur sites to switch to tunneling systems or untrustworthy DNS mechanisms.

Examples of Targeting the DNS

After Wikileaks released its cache of diplomatic documents in December 2010, its DNS provider EveryDNS.net stopped providing DNS resolution services for www.wikileaks.org, severely curbing Wikileaks' ability to disseminate its documents to users seeking to access its website.

Internet Service Providers (ISPs)

An Internet Service Provider (ISP) provides access to the Internet. An ISP can be small, like a local business that connects its users to a larger upstream provider; or it can be a big, corporate operation like AT&T or Comcast.

Even when a country has laws that shield third-party services from liability based on some of their users' activity, such as the United States' Communications Decency Act § 230, and

the notice and takedown provisions of the Digital Millennium Copyright Act, some ISPs would rather get rid of a user (or their allegedly offending content) than be drawn into a legal dispute, even where there is no liability risk to the third-party provider.

In addition, governments and rightsholders can threaten free speech by pressuring ISPs to cut off a user's Internet access. This is showcased by **"three strikes" proposals**. Three strikes laws (and voluntary agreements by ISPs) would require ISPs to **terminate a user's Internet connection** once that user had received a number of notifications of alleged copyright infringement. Several countries have already enacted such laws, including France and South Korea, and others are pushing for similar laws.

Even where a user's activity could be a protected use, copyright holders have the advantage of being able to **pressure an ISP** to cut off that user's Internet access, while ISPs have little incentive to fight back for their users. Laws like three strikes jeopardize users' ability to access the Internet — and thereby to speak and get information online. Other proposals would require intermediaries like ISPs to act as IP police, including blocking access to websites that allegedly facilitate infringement.

Examples of Targeting ISPs

In one of the biggest acts of government censorship ever to focus on ISPs, the Egyptian government forced the country's six ISPs to go offline, thereby knocking out the Egyptian Internet and suffocating all online speech in the country.

Search Engines

Search engines map the incalculably vast territories of the Internet and provide search results to queries, allowing users to easily find what they are looking for.

Because search engines have now become virtually indispensable, they are increasingly magnets for censorship. This damages search neutrality, which ensures that users get the results they were looking for (as opposed to what governments or private actors want them to see), and makes it harder for online speakers to disseminate their views.

Authoritarian governments often block search engines or force them to blacklist certain queries to limit access to what the governments perceive as threatening or subversive materials. **Industry groups** that lobby for increased copyright holder control, like the MPAA and the RIAA, have also realized the power of search censorship, for example, challenging torrent search indices such as isoHunt. In addition to these large players, **individuals may claim that search engine results are defamatory** or otherwise illegal and seek to have them taken down.

Depending on the jurisdiction, such efforts may or may not enjoy the support of law. In the United States, for example, the First Amendment and Section 230 of the Communications Decency Act make efforts to remove non-copyrighted material difficult, although notices of copyright infringement (valid or not) are facilitated by easy to use (and easy to abuse) procedures provided by the DMCA. Processes initiated in other countries with weaker legal protections may lead to easier removal of speech.

Examples of Targeting Search Engines

The Chinese government forces search engines like the immensely popular Chinese search engine Baidu.com to edit certain search results. Without an easy way to find it, the blocked information may as well not exist.

Payment Service Providers

Online payment service providers make it possible for users to send and receive payment online by acting as intermediaries among money senders, financial institutions, and payment recipients.

Online donations made through payment services can provide necessary financial support for a political cause, candidate, or activist group. Payment services can also ensure that consumers can purchase media online – like books or pamphlets from political critics – and that websites can process payments for their services, allowing them to continue operating.

Since payment service providers may provide vital financial pathways for activists, dissidents, and other controversial figures, they are attractive **points of control** for anyone hoping to use Internet intermediaries as censors — especially governments seeking to censor speech.

Payment services are also targets for powerful actors who want to shut down controversial sites under the guise of **preventing IP infringement**. Such proposals could halt the operations of controversial web services, including popular hosting sites like Rapidshare and Mediafire (neither of which has been found liable for copyright infringement), by cutting off their means of financial support.

Payment services might also decide **voluntarily** to stop processing certain sites' payments as capitulation to government or industry, thereby putting small companies at risk and endangering their ability to speak online. This would not extend only to those convicted of crimes. Any online venue under scrutiny for controversial practices could be at serious financial risk if a big payment service decides to stop processing payments for it.

Examples of Targeting Payment Service Providers

Wikileaks' ability to pay its operating costs suffered a serious blow when PayPal and other payment intermediaries caved to pressure to stop processing donations to the controversial journalism group – an obvious case of payment intermediaries being pressed into the service of government censorship.

Third-Party Platforms

Third-party platforms like Blogger, Facebook, Twitter, and online email clients like Hotmail, Yahoo, and Gmail offer a wide variety of services to Internet speakers. They generally enable users to send messages, post content, participate in group discussions, and present their own websites and blogs online.

Popular third-party services like Facebook and Gmail have millions of users and are many speakers' principal means of online communication. However, many such platforms, when pressed with takedown requests or legal threats, often opt for the cheap solution of **taking down speech or banning users** instead of risking expensive legal battles. Moreover, third-party services' popularity also means that more and more people store huge amounts of private data and communications online, making these sites ripe for governments and civil lawyers seeking information about citizens, whether for law enforcement purposes or more nefarious reasons.

Governments – as well as private actors – seeking information about unpopular speakers often target third-party platforms in order to create surveillance profiles of dissidents and activists. In particular, **speech-repressive regimes mine third-party sites like Facebook or Twitter for information about protest organizers and movement leaders**. These sites are popular among activists for their wide user base and ease of use – but they are equally attractive to governments seeking to silence speakers, keep tabs on opposition figures, or even figure out where dissidents live (and who their friends are). Some governments may ban the use of these services altogether, as China banned Google and Gmail, in order to prevent any speech via these services whatsoever.

Even when a country has laws that shield third-party services from liability based on some of their users' activity, such as the United States' Communications Decency Act § 230, and the notice and takedown provisions of the Digital Millennium Copyright Act, some third-party services would rather get rid of a user (or their allegedly offending content) than be drawn into a legal dispute, even where there is no liability risk to the third-party provider.

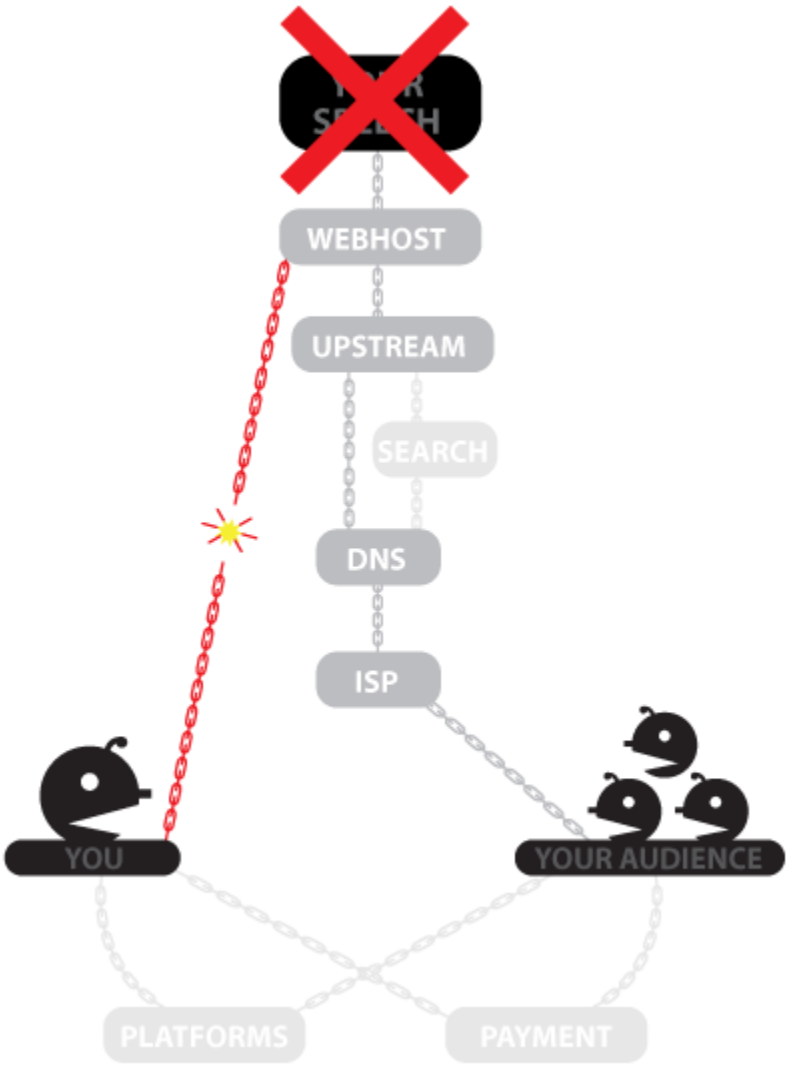
Examples of Targeting Third-Party Platforms

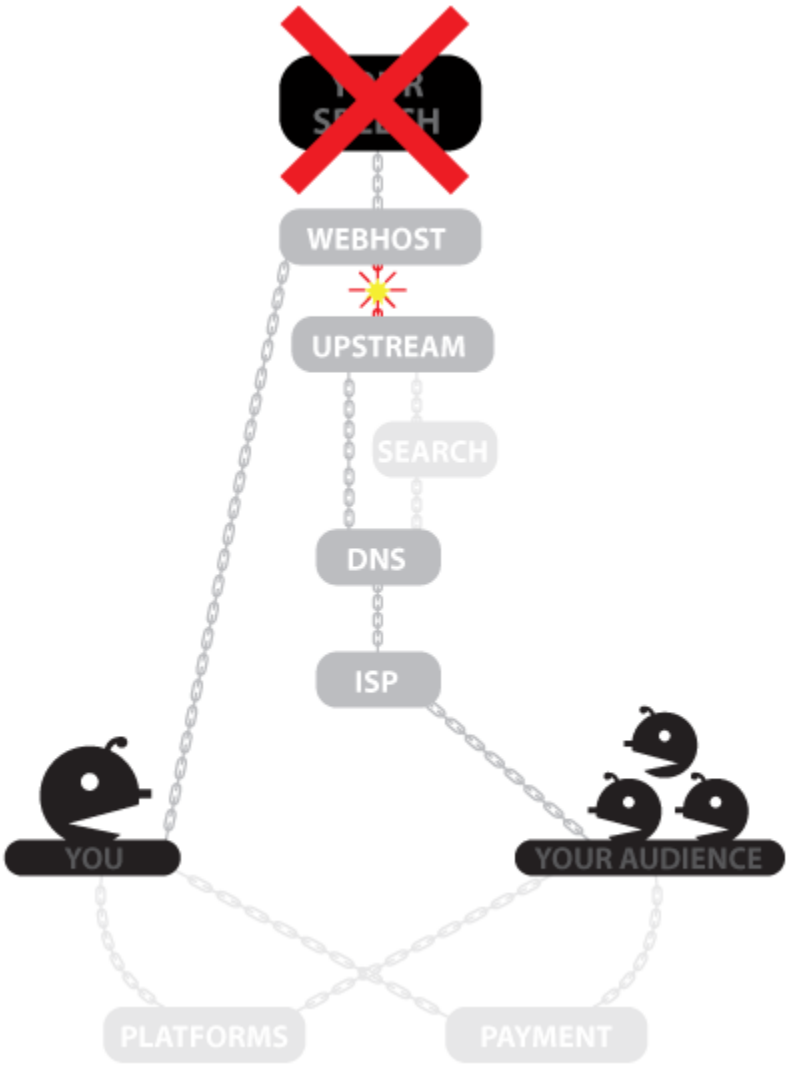
When the Chinese government requested information – including private emails – about several dissidents whom it sought to silence, Yahoo complied with its demands, supplying data that led to the prosecution and imprisonment of dissidents.

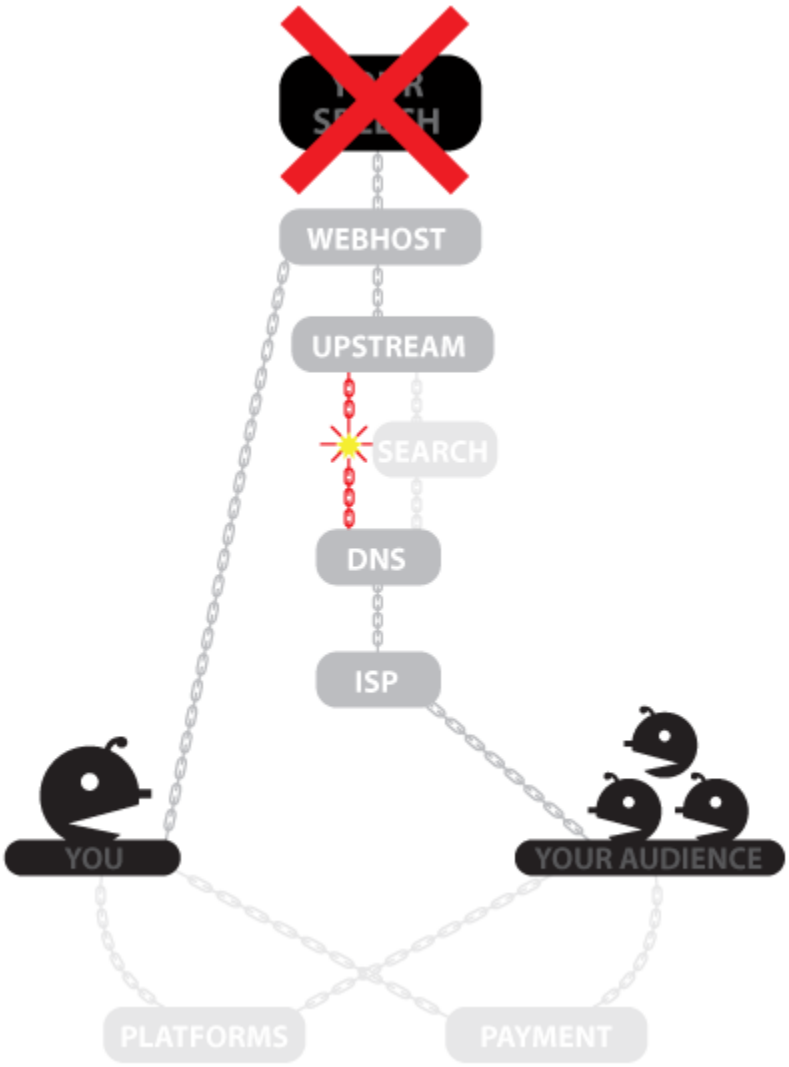
After registering the generic terms “urban homesteading” and “urban homestead” as trademarks, a group called the Dervaes Institute managed to convince Facebook to take down several pages that used those terms, including one supporting a handbook for urban homesteaders.

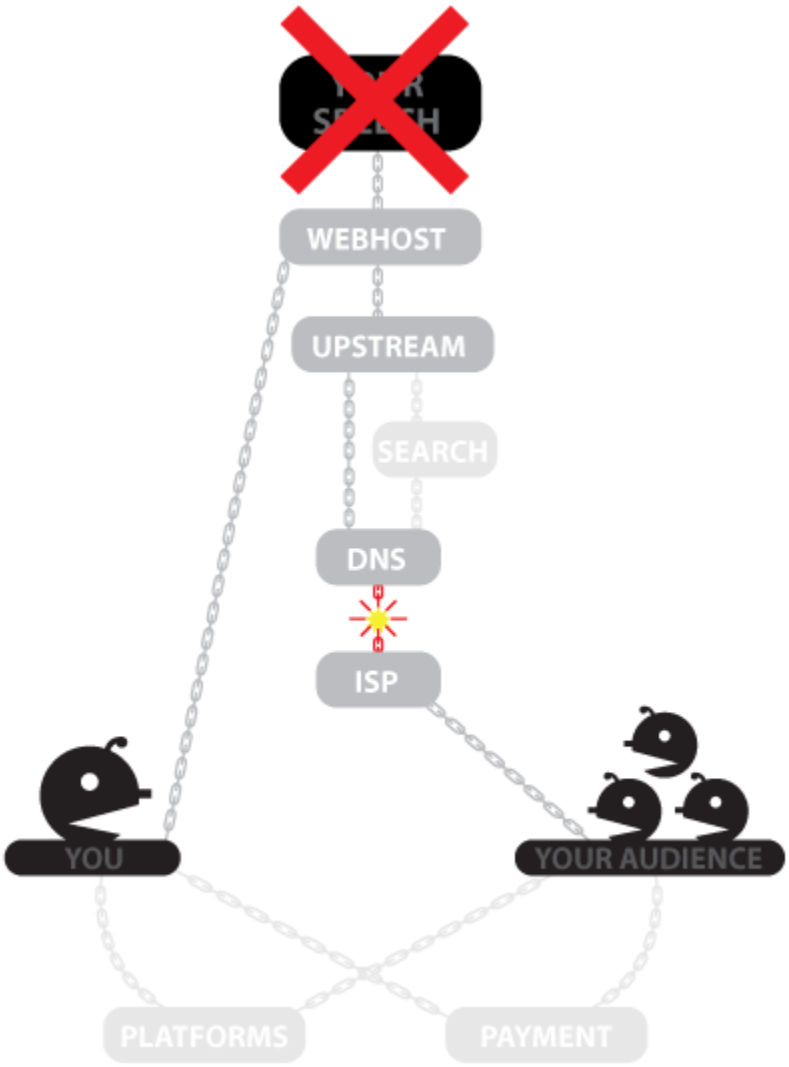
Total respect of course, but this page requires javascript.

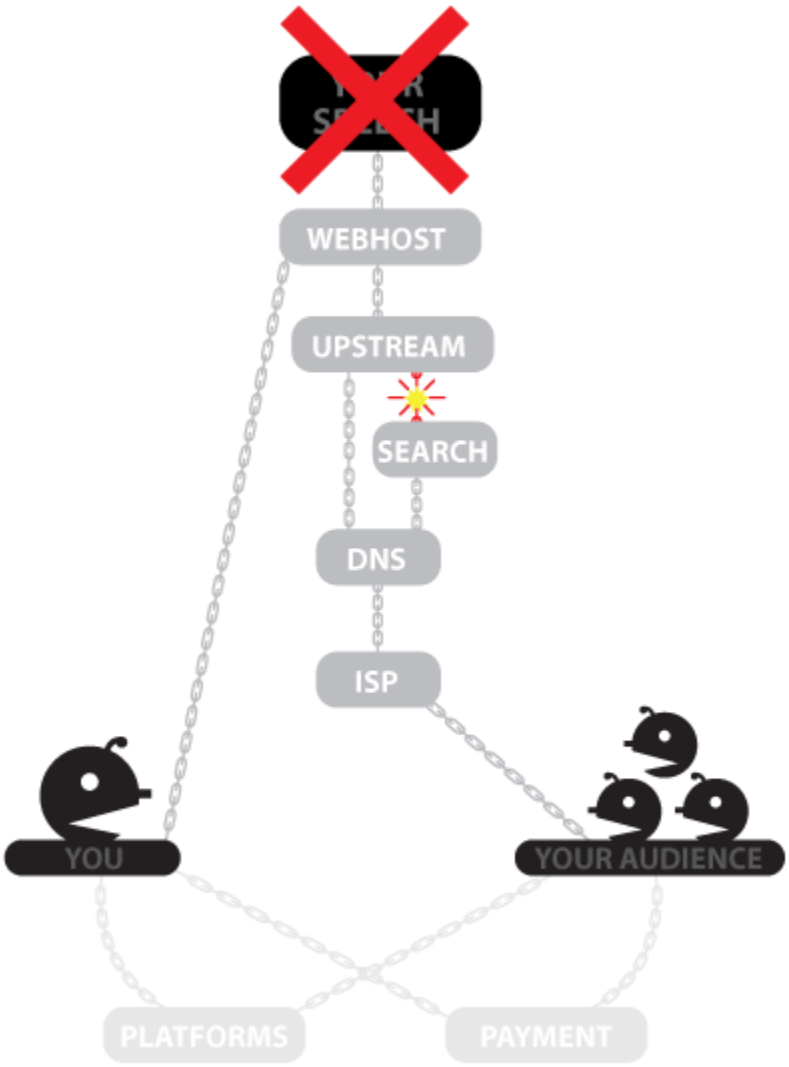

YOUR SPEECH
WEBHOST
UPSTREAM
SEARCH
DNS
ISP
YOU
YOUR AUDIENCE
PLATFORMS
PAYMENT

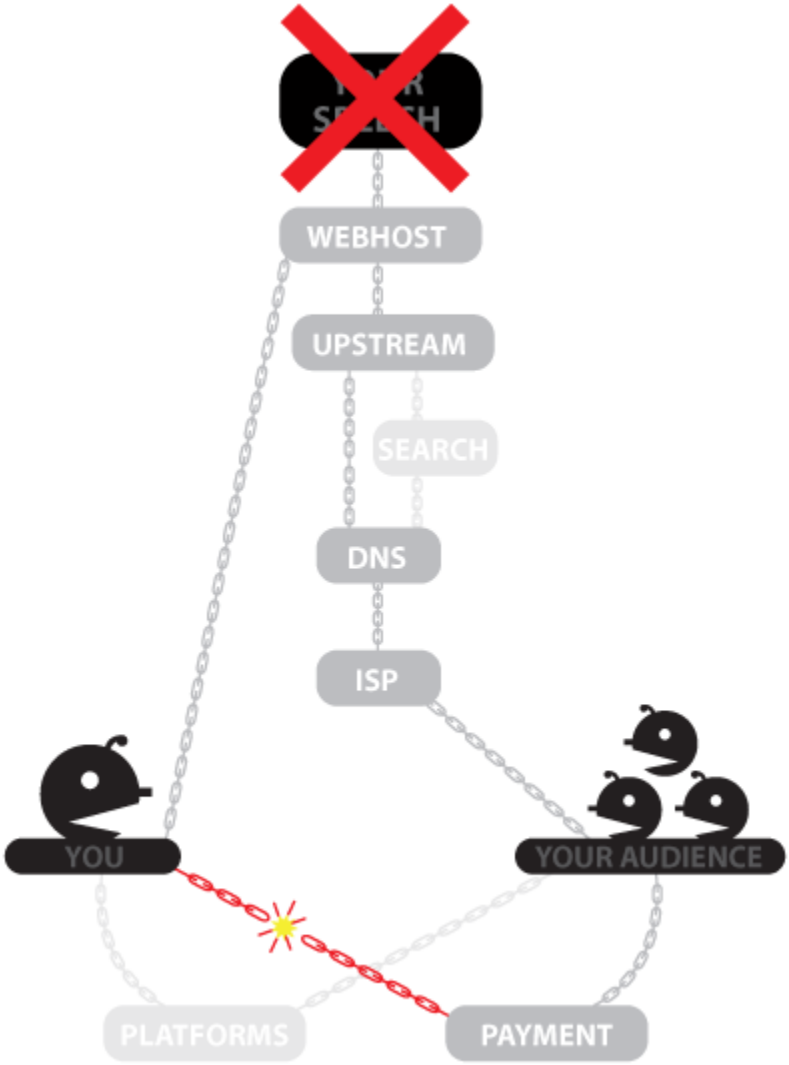

WEBHOST
UPSTREAM
SEARCH
DNS
ISP
YOU
YOUR AUDIENCE
PLATFORMS
PAYMENT

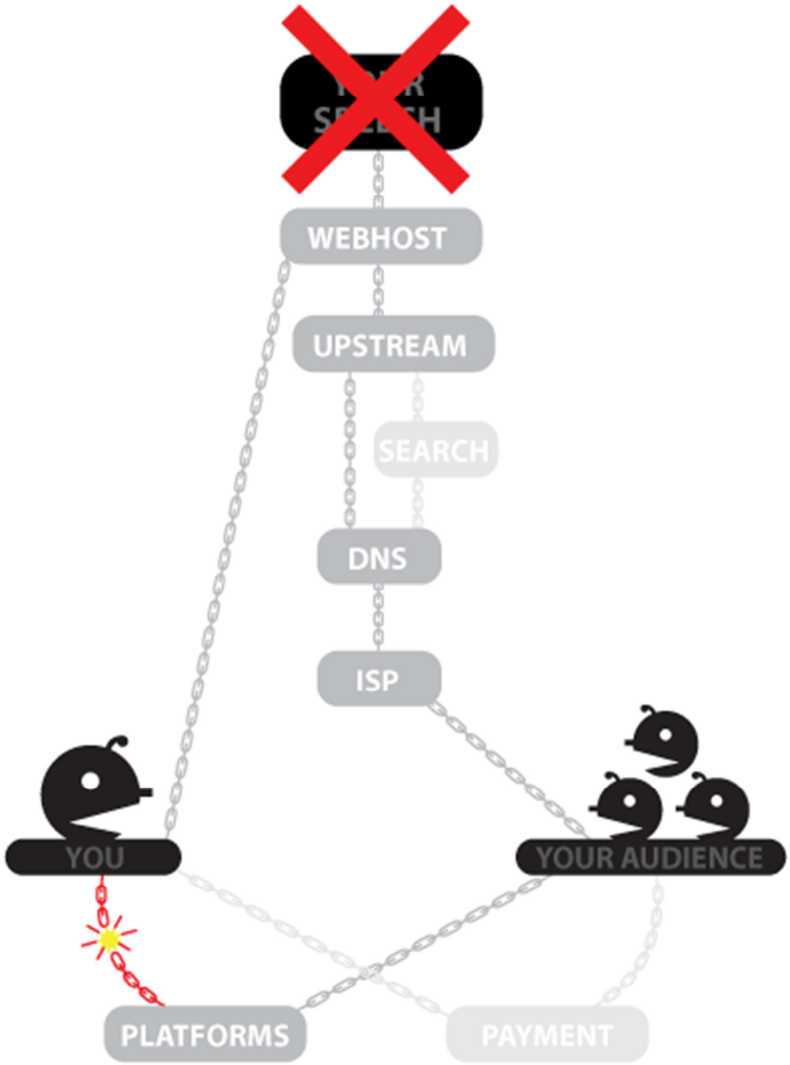

WEBHOST
UPSTREAM
SEARCH
DNS
ISP
YOU
YOUR AUDIENCE
PLATFORMS
PAYMENT


WEBHOST
UPSTREAM
SEARCH
DNS
ISP
YOU
YOUR AUDIENCE
PLATFORMS
PAYMENT


WEBHOST
UPSTREAM
SEARCH
DNS
ISP
YOU
YOUR AUDIENCE
PLATFORMS
PAYMENT


WEBHOST
UPSTREAM
SEARCH
DNS
ISP
YOU
YOUR AUDIENCE
PLATFORMS
PAYMENT


WEBHOST
UPSTREAM
SEARCH
DNS
ISP
YOU
YOUR AUDIENCE
PLATFORMS
PAYMENT


WEBHOST
UPSTREAM
SEARCH
DNS
ISP
YOU
YOUR AUDIENCE
PLATFORMS
PAYMENT