

# NetNubby Legal Discussion: Social Media and World Law

Chat Transcript — Claude (claude.ai) & Mac | April 6, 2026

---

MAC

Are NetNubbys legal in the UK?

CLAUDE

Based on the information from their website FAQ, here's the relevant legal picture for the UK:

**NetNubbys are almost certainly legal to use in the UK. Here's why:**

*A NetNubby is a digital sticky note that you attach to web pages in your own browser. The Notes are injected into a local copy of the page on your own computer — the web server itself is never altered.*

The key legal reasoning (which applies in the UK as much as the US) is:

**1. No server interference.** NetNubbys modify page data *after* the web page has been downloaded from a server to your local machine. Note data originates from NetNubby servers, not the originating webserver for the page under view. This means there's no hacking or unauthorised access to third-party systems — relevant under the UK's Computer Misuse Act 1990.

**2. Copyright isn't infringed.** It is not illegal to post a NetNubby on a copyrighted web page. NetNubbys have nothing to do with the data on a webserver.

**3. TOS violations aren't criminal.** Courts have ruled that merely violating a site's Terms of Service is not a criminal act. The same principle generally holds under UK law.

**4. Only opted-in users see notes.** A NetNubby cannot be displayed until you install software on your local computer, and even then Notes don't automatically appear. This means there's no unsolicited broadcasting of content to others.

**One caveat:** while using NetNubbys is legal, the *content* of the Notes you post could still potentially run afoul of UK law — for example, if Notes contained defamatory statements, harassment, or illegal content. But the platform itself appears legally sound for UK users.

MAC

But would such a defamatory post bring liability upon the platform itself, or the poster?

CLAUDE

This is a nuanced area of UK law. The short answer is: **primarily the poster, but the platform could face liability under certain conditions.**

A major regulation that applies here is the **UK Online Safety Act 2023 (OSA)**, a landmark law forcing tech companies to take legal responsibility for protecting users — particularly children — from illegal and harmful content. It mandates that platforms remove illegal content, prevent children from accessing harmful material, and enforce strict age checks, among other requirements.

## The Poster

The person who writes a defamatory NetNubby Note would be the primary liable party under the Defamation Act 2013, as the originator of the statement.

## The Platform

UK law does offer platforms some protection, but it's not absolute:

**Section 5 of the Defamation Act 2013** provides a defence for website operators hosting user-generated content, *if* they respond appropriately to a complaint. If NetNubby ignores a valid takedown request for a defamatory Note, that defence evaporates and the platform could become liable.

**The defence of “innocent dissemination”** can protect platforms that are not the author, editor, or publisher of the statement — which NetNubby arguably isn't, given it's just infrastructure for user posts. However, this protection weakens once the platform has been *notified* of the defamatory content and fails to act.

**E-Commerce Regulations 2002** (derived from the EU E-Commerce Directive, retained in UK law post-Brexit) similarly shield hosting platforms from liability for content they're unaware of, but again, knowledge removes that shield.

## The Wrinkle Specific to NetNubby

NetNubby's architecture adds an interesting twist. Since Notes are overlaid in the viewer's browser rather than hosted on the target website's server, it's a novel enough setup that how a UK court would classify NetNubby — as a mere conduit, a host, or something else — isn't entirely settled. That classification matters a lot for which legal protections apply.

In practice, a claimant would almost always pursue the poster first, since they're the clearest wrongdoer. The platform would typically only come into the crosshairs if the poster were anonymous or unreachable, and NetNubby had failed to respond to a legitimate complaint. I'm not a lawyer though, so anyone with a specific situation like this would be well advised to seek qualified UK legal counsel.

### MAC

Let's add another wrinkle: User accounts on the NetNubby platform are truly anonymous. So how does this square with your answer so far?

### CLAUDE

This significantly shifts the liability picture, and it's where things get genuinely thorny.

## The Poster Becomes Practically Unreachable

While the poster remains the *primary* liable party in theory, true anonymity makes that liability essentially unenforceable in practice. A claimant can't sue someone they can't identify. This is actually a well-recognised problem in UK defamation law — the so-called “anonymous poster” problem.

## Pressure Shifts to the Platform

When the actual wrongdoer can't be identified or sued, claimants naturally turn to the platform. The key mechanisms in UK law are:

**Norwich Pharmacal Orders (NPOs)** — A claimant can apply to a UK court to force a platform to disclose identifying information about an anonymous user. However, this only works if the platform *has* such information. If NetNubby is genuinely collecting no identifying data, there's nothing to hand over, and the order becomes useless.

**Section 5 Defamation Act 2013 defence** — This defence specifically requires the operator to facilitate identification of the poster when asked. If NetNubby *can't* do this due to genuine anonymity, it may lose access to this defence entirely, leaving it considerably more exposed.

## NetNubby's Privacy Policy Complicates This Further

From the search results earlier, NetNubby does collect some data — including IP addresses and the URLs where Notes are posted. So “truly anonymous” may be relative. A determined litigant with a court order could potentially obtain those logs, and an IP address, while not a name, can sometimes lead back to an individual via their ISP.

## The Broader Tension

There's a genuine unresolved tension in UK law here between:

The **right to anonymity** and free expression (Article 10, ECHR), and the **right to reputation** and an effective remedy for defamation (Article 8, ECHR).

UK courts have generally tried to balance these, but where a platform is structured in a way that makes a poster genuinely untraceable, the courts have shown increasing willingness to hold the platform itself more accountable — particularly if it failed to act on a complaint.

## Bottom Line

True anonymity doesn't just complicate things — it effectively transfers the practical burden of liability from the poster to the platform. NetNubby's best protection would be a robust and responsive takedown process, because that's likely its strongest remaining legal shield once poster identification is off the table. Again though, this is a genuinely unsettled and evolving area of law, and specialist UK legal advice would be essential for anyone concretely affected.

### MAC

What are the details of the moderation infrastructure that OSA demands be in place? Bear in mind the NetNubby platform is not a social media service, but an adjunct conversation overlay tool.

### CLAUDE

This is a rich and important question, and NetNubby's unusual architecture makes it genuinely interesting to analyse against the OSA. There are two separate issues to address: whether NetNubby falls within the OSA's scope at all, and if it does, what is actually required of it.

## Does the OSA even apply to NetNubby?

This is the threshold question, and it's not obvious. The OSA applies to any “user-to-user service,” defined as an internet service by means of which content generated, uploaded or shared by a user may be read, viewed, heard or otherwise experienced by another user. NetNubby Notes are stored on NetNubby's servers and can be seen by other opted-in users on the same URL — so on the face of it, this definition is met. The requirement is that user-generated content “may” be encountered by at least one other user — it does not have to be encountered in fact — and “encountered” is drafted broadly to include reading, viewing, hearing or otherwise experiencing the content.

However, NetNubby might argue for the “limited functionality” exemption. This covers services that permit only limited user interaction in relation to content published by the provider, such as posting comments or reviews or applying a “like” button or an emoji — intended to put services outside scope where the only user interaction consists of “below the line” content. The problem is that NetNubby Notes are posted *on third-party pages*, not on content published by NetNubby itself, so this exemption likely doesn't fit neatly. The exemptions are drafted very tightly and are not expected to be universally applicable; services should take care before assuming they can rely on them.

There is also a territorial element: for the OSA to apply, there needs to be a “UK link” — meaning the service has a significant number of UK users, UK users form a target market, or it is capable of being used by UK individuals and there is a material risk of significant harm.

## If NetNubby is in scope, what does it need?

The obligations are tiered. All in-scope services face a baseline set of duties, with heavier requirements for larger platforms. NetNubby, as a small service, would face the baseline tier. The key requirements are:

**Illegal Content Risk Assessment.** All in-scope services, regardless of size or type, must complete an illegal content risk assessment, identifying the types of illegal content that may be present on the service, including by reference to 17 types of “priority illegal content” identified by *Ofcom*, and then assessing the risk level.

(For reference, Ofcom (the Office of Communications) is the independent regulatory and competition authority for the UK's communications industries, covering TV, radio, on-demand services, telecoms (broadband/phones), and postal services. It protects consumers from harm, manages the radio spectrum for wireless devices, and enforces content standards, including new online safety duties.)

**Content moderation infrastructure.** Ofcom's codes recommend establishing a content moderation team to swiftly take down illegal content, appointing an accountable person for illegal content safety duties, enabling complaints via an easy-to-find and accessible complaints system, and ensuring clarity and accessibility of terms of service.

**Proactive measures and transparency.** Providers have a duty to include in their terms of service provisions specifying how individuals are to be protected from illegal content, to apply those terms consistently, and to give information about any proactive technology used for compliance — including the kind of technology, when it is used, and how it works.

**Children’s access assessment.** All user-to-user services in scope must carry out a children’s access assessment to establish whether their service is likely to be accessed by children, and services that fall into that category must then comply with children’s risk assessment duties and children’s safety duties.

### The NetNubby-specific wrinkle

Here the overlay architecture becomes relevant again. The OSA does not give Ofcom the power to require the removal of specific harmful content — instead, it imposes duties on services to put in place effective *processes and systems* to guard against that content. So NetNubby’s obligation would be to build systems capable of receiving complaints, assessing and removing Notes, and demonstrating that process to Ofcom — not necessarily to proactively scan every Note in real time.

That said, the anonymity issue discussed earlier resurfaces here with added force: the OSA’s moderation infrastructure implicitly assumes a platform can identify and act against users. A platform that has designed away that ability faces a structural tension with the regime’s expectations that is, frankly, unresolved in the current legislation for novel architectures like NetNubby’s. This would be another area where specialist legal advice would be essential.

#### MAC

To clarify a few things:

1. “True anonymity” does not mean an account cannot be warned, banned or terminated. It means the accountholder is not required to divulge a name, home address, official email address, or other PII that may appear on official identification documents.
2. The platform gives accountholders the option to “flag” a Note they suspect contains content in violation of the platform’s TOS, AUP and Privacy policies.

#### CLAUDE

These are important clarifications that materially improve NetNubby’s legal position on several fronts.

### On “True Anonymity” Redefined

This reframing actually resolves one of the thorniest problems identified earlier. The concern wasn’t really about anonymity per se — it was about whether the platform had *any* lever to act against a wrongdoer. If accounts can be warned, suspended or terminated (even without knowing the real-world identity behind them), then:

**The Section 5 Defamation Act 2013 defence becomes considerably more viable.** The defence requires the operator to be able to respond to complaints and take action — it doesn’t strictly require the platform to unmask the poster to the claimant. An ability to terminate the offending account may be sufficient to demonstrate good faith responsiveness.

**The NPO problem is also softened.** A court order compelling disclosure of PII is less useful if there isn’t much PII to hand over — but the platform’s ability to *act* on a complaint is a separate matter from its ability to *identify* the poster to a third party. Courts are generally more interested in whether a platform is willing and able to remedy harm than in whether it can deliver a named individual.

From a reputational and regulatory standpoint, a platform that responds promptly to complaints by warning or banning the offending account looks very different to one that shrugs and pleads technical inability. The former has a credible moderation posture; the latter invites escalation.

## On the Flagging Mechanism

This is significant for OSA compliance purposes too. Ofcom's codes of practice specifically recommend enabling complaints via an easy-to-find, accessible complaints system and taking appropriate action upon receipt of complaints. A built-in flagging tool — visible to all users at the point of encountering a Note — arguably satisfies this requirement more elegantly than many larger platforms manage. The key follow-through requirement is that flags must actually be *acted upon* in a timely and consistent way, and that the process is documented.

Taken together, these two clarifications shift NetNubby's profile considerably — from a platform that looked structurally incapable of moderation, to one that has made a principled architectural choice about privacy while retaining meaningful enforcement tools. That's a much more defensible position, both legally and before a regulator like Ofcom. The remaining vulnerability is the paper trail: NetNubby would need to be able to demonstrate, if challenged, that flagged content was reviewed and acted upon, and within what timeframe — because legal defences ultimately rest upon that record of responsiveness.

### MAC

Since the NetNubby service is a U.S.-based service, the core of its operation is governed by Section 230 of The Communications Decency Act (CDA), a U.S. statute that establishes moderation guidance for online platforms. How does this square with U.K. law? If an accountholder were a British subject, does the platform apply U.S. law or U.K. law? Given the accountholder is permitted, encouraged even, to not divulge bona fide particulars, how would the NetNubby platform apply any law other than the law of the country in which the service was created?

### CLAUDE

This is one of the most fundamental tensions in international internet law, and it doesn't have a clean resolution. Let's take each question in turn.

## Section 230 and What It Actually Does

Section 230 is frequently misunderstood as a broad immunity shield. What it actually does is protect a platform from being treated as the *publisher or speaker* of third-party content — meaning NetNubby cannot be sued in a US court simply because a user posted something defamatory or harmful via its service. It also protects platforms from liability for good-faith moderation decisions (removing or leaving up content). This is the legal bedrock of most US-based user-generated content platforms.

## How Does This Square with UK Law?

Bluntly: it *doesn't*, and it wasn't *designed to*. Section 230 is a US statute and has no force in UK courts whatsoever. A UK claimant suing in a UK court over a defamatory NetNubby Note would proceed entirely under UK law — the Defamation Act 2013, the E-Commerce Regulations 2002, and the OSA framework discussed earlier. The fact that NetNubby enjoys Section 230 protection in the US is legally irrelevant in that UK proceeding.

This is not a novel problem. It is the same tension that has embroiled Meta, Google, and Twitter/X for years. The OSA's duty of care applies globally to services with a significant number of United Kingdom users, or which target UK users, or those which are capable of being used in the United Kingdom where there are reasonable grounds to believe that there is a material risk of significant harm. US incorporation provides no exemption. The OSA applies to more than 100,000 user-to-user and search services providers that target the UK market or have many UK users — including social media apps, messaging apps, online marketplaces and others — even if they're small or based overseas.

## Which Law Applies to a British Subject Using the Platform?

The honest answer is: *both could*, depending on the forum in which a dispute arises and the specific remedy being sought.

If a British user posts a defamatory Note about another British person, and the victim sues in a UK court, UK law governs. The court doesn't care where NetNubby's servers are. If that same user is sued in a US court (unlikely, but possible), Section 230 might protect the platform, though not the individual poster.

NetNubby's own Terms of Service will typically include a choice-of-law clause specifying US law — probably the law of whichever state it's incorporated in. However, UK courts have the power to disregard such clauses where applying foreign law would be contrary to UK public policy, or where mandatory UK statutory protections (like consumer rights or data protection law) cannot be contractually overridden. The OSA's duties in particular are statutory and cannot be waived by a choice-of-law clause.

## The Anonymity and Jurisdiction Problem

This is where your final question cuts deepest, and it identifies a genuine structural reality: in practical terms, a platform that collects minimal PII and is incorporated in the US is largely beyond the *practical* reach of UK enforcement, even if it is theoretically within the *legal* reach of UK law.

Ofcom's enforcement tools against a non-compliant overseas platform ultimately come down to a few mechanisms: fines (difficult to collect from a US entity with no UK assets), service restriction orders requiring UK ISPs to block the platform, and app store intervention orders. For a small platform like NetNubby, the nuclear option of blocking is disproportionate; the fine route requires UK court recognition of the order and some UK-jurisdictional hook to enforce it.

So the practical reality is this: NetNubby, by virtue of being a small US-based service collecting minimal PII, sits in a zone that UK law can theoretically reach but practically struggles to touch. This is not a unique or illicit position — it is the default condition of thousands of small US internet services that have UK users. The legal obligations nominally exist; the enforcement machinery is imperfect.

Where this calculus could change is if NetNubby ever sought to formally target the UK market, established a UK business presence, or grew to a scale where Ofcom considered it worth the effort of a formal enforcement action. Until then, the platform exists in a practical grey zone — legally subject to UK obligations in principle, but insulated from them in practice by geography, size, and the architecture of minimal data collection you’ve described.

#### MAC

Operationally, the NetNubby service is akin to other conversation overlay models such as the Hypothes.is service. Please examine that service and compare it to the NetNubby platform. Does anything you’ve stated so far materially change?

#### CLAUDE

### How Hypothes.is and NetNubby Compare Operationally

The architectural similarities are striking. Hypothes.is is an open-source project described as “a peer review layer for the entire internet” — a system which allows annotation of web pages using comments contributed by individuals, with normal use via a browser plug-in or bookmarklet. Like NetNubby, annotations are overlaid on third-party pages in the user’s browser; the underlying web server is not touched. Both platforms store user-generated notes on their own servers, and both require opted-in software to view annotations. While Hypothesis allows users to post content anchored to specific locations on any web page, NetNubby anchors content to a URL.

There are further similarities:

Hypothesis requires account creation with a username and email address, and annotations are associated with that account. NetNubby also requires a functioning email address as a condition of registration, while the moniker is self-styled.

Hypothesis also offers granular visibility controls — annotations can be made public, private, or shared within a specific group, with public annotations visible to anyone who visits the page with Hypothesis enabled. Likewise, NetNubby Notes can also be made public, private or reserved to a group.

Hypothesis differs in that it is heavily institutionally embedded — it is trusted by over 300 institutions and integrated into learning management systems like Canvas, Blackboard, Moodle and D2L — which gives it a predominantly academic use context that NetNubby’s more open social model does not share.

### Does Anything Previously Stated Materially Change?

On the core legal analysis, very little changes — but the Hypothes.is comparison does usefully *reinforce and nuance* several points.

First, it establishes that the overlay annotation model is not legally exotic or untested. Hypothes.is has operated for well over a decade at significant institutional scale without triggering any reported legal challenge to its fundamental architecture. This is useful precedent for NetNubby: it suggests that the browser-overlay model, as a category, has implicitly passed a long market stress-test without courts finding it inherently problematic.

Second, the comparison actually *strengthens* the case for NetNubby's privacy architecture being a deliberate and legitimate design choice rather than a suspicious evasion. Hypothes.is collects email addresses and is institutionally embedded; NetNubby opts for pseudonymous accounts. Both are valid design philosophies, and the existence of a well-regarded comparator in the same technical space makes NetNubby look less like an outlier.

That said, this cuts both ways: it also demonstrates that platforms in this space *can* operate responsibly with minimal data collection, and that regulatory and legal exposure hasn't materially hampered Hypothes.is despite its scale and institutional prominence.

In summary: nothing previously stated needs to be retracted or substantially revised. The Hypothes.is comparison confirms the legitimacy of the model, provides some comfort on the architectural questions, and introduces one marginal note — that NetNubby's anonymity posture is a policy choice that a regulator could scrutinise, precisely because a comparable service has shown the model can work with slightly more user identifiability.

#### **MAC**

If the NetNubby service wished to be not subject to U.K. laws of any kind, which would mean that British subjects were expressly forbidden to register as accountholders, how would the platform enact this policy on a technical level so as to insulate itself from liability?

#### **CLAUDE**

This is a well-defined legal and technical question, and it's worth separating the two layers: what technical mechanisms exist, and whether any of them would actually achieve the legal insulation sought.

### **The Technical Options**

*IP Geoblocking* is the most commonly deployed tool. NetNubby could block access to its registration and login pages from IP address ranges associated with the United Kingdom. This is the same mechanism used by streaming services to enforce regional content licences. It is straightforward to implement and would turn away most casual UK users at the door.

*Payment geofencing* is irrelevant here since NetNubby appears to be a free service (so far), but worth noting for completeness — many services combine IP blocking with payment card country-of-issue checks as a secondary filter.

*Registration field restrictions* could be employed at the account creation stage — requiring a non-UK mailing address, phone number, or selecting a country of residence, with UK excluded from the dropdown. This creates a contractual paper trail where the user affirms they are not a UK resident.

*Terms of Service exclusion* is the complementary legal instrument. The TOS would explicitly state that the service is not available to UK residents or British subjects, that any UK-resident user is in breach of the agreement by registering, and that the platform bears no liability arising from such unauthorised use.

*Browser locale and language signals* can supplement IP data — these are less reliable but can be used as secondary indicators.

## Why None of This Fully Works

Here is where the honest answer diverges from the theoretical one, and it is important to be direct.

IP geoblocking is trivially circumvented by any user with a VPN — a tool used by millions of ordinary UK internet users for entirely legitimate purposes. A determined British user could register from a US IP address in minutes. The platform would know this is possible, and so would a UK court or Ofcom.

The critical legal point is this: territorial exclusion through technical means does not eliminate legal exposure — it *shifts the moral responsibility* and may *reduce* liability, but it does not eliminate it. UK courts and Ofcom assess jurisdiction based on whether a service *is capable of being accessed* by UK users and whether there is a material risk of harm — not merely whether the platform has posted a no trespassing sign saying “UK residents not welcome.” A service can be caught if it is capable of being used in the UK and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK presented by the service’s content.

The Hypothes.is comparison is instructive here too. It is a US-based service with no apparent UK-specific compliance infrastructure, yet it operates freely in the UK academic market without having taken any of these exclusion steps — suggesting that, at NetNubby’s scale, the practical enforcement risk may be lower than the theoretical legal exposure in any case.

## What Would Actually Provide the Strongest Insulation

If the goal is genuine legal insulation rather than symbolic exclusion, the most defensible combination would be 1) robust IP geoblocking combined with an explicit TOS prohibition on UK registration; 2) a clearly worded declaration at the point of account creation requiring the user to confirm they are not a UK resident; and 3) documented evidence that the platform actively maintains and updates its geoblocking infrastructure.

This last point matters because it demonstrates *intent and effort* — a court is far more likely to accept a good-faith exclusion argument from a platform that can show a consistent and maintained technical policy than from one that added a clause to its TOS and did nothing else.

The declaration at registration is particularly valuable. If a UK user falsely declares they are not a UK resident in order to gain access, the responsibility for any consequences of that misrepresentation shifts substantially toward the user. This is the same principle used by age-restricted platforms — a user who lies about their age to access a service bears the primary moral and legal responsibility for doing so.

## The Residual Risk

Complete legal insulation is, in practice, unachievable. What the above measures yield is a *credible and documented good-faith effort* to exclude UK users, which would be relevant mitigation in any UK enforcement action or litigation. For a small US-based platform with no UK assets or business presence, that combination — technical barriers, clear TOS prohibition, and a false-declaration mechanism — likely represents the practical ceiling of what is achievable without withdrawing from the internet entirely.

## MAC

Should the NetNubby service wish to operate exclusively under U.S. jurisdiction protections, such as Section 230 of the CDA previously discussed, which countries would necessarily have to be GEO-blocked? Or is this level of online operation even feasible?

## CLAUDE

This is an excellent question that cuts to the heart of how internet jurisdiction actually works — and the short answer is that operating exclusively under US jurisdiction is theoretically conceivable but practically unachievable at any meaningful scale. Here is why.

### The Scope of the Problem

Section 230 protects NetNubby only in US courts. Every other country with active internet regulation has its own liability framework for user-generated content, and most of them either explicitly assert extraterritorial reach over foreign platforms serving their citizens, or have courts willing to do so. To rely solely on Section 230, NetNubby would need to ensure that no user from any country with a conflicting legal regime could access the service — which means geoblocking not just the UK, but most of the world.

The countries that would *necessarily* need to be blocked, because they have active and enforceable platform liability regimes that conflict with or go beyond Section 230, include at minimum:

**Australia**, which passed the Online Safety Act 2021 imposing removal obligations on platforms for harmful content, and which has pursued enforcement actions against US-based platforms.

**Brazil**, whose Marco Civil da Internet creates platform liability once a platform has been notified of court orders to remove content and fails to comply.

**Canada**, which has proposed and is advancing platform liability legislation, and whose courts have historically been more willing than US courts to hold platforms liable for user content — as the EFF noted in the Section 230 discussion earlier.

The entire **European Union**, which operates under the Digital Services Act (DSA). The DSA imposes content moderation, transparency, and risk assessment obligations on platforms accessible to EU users, regardless of where the platform is based. With 27 member states, this alone accounts for roughly 450 million potential users who would need to be excluded.

**Germany**, which even within the EU framework maintains its own Network Enforcement Act (NetzDG), requiring large platforms to remove illegal content rapidly or face substantial fines.

**India**, which through its Information Technology Rules 2021 imposes due diligence, grievance redressal, and content removal obligations on “significant social media intermediaries.”

**Japan, South Korea**, and a growing number of other jurisdictions in the Asia-Pacific region are each developing or have developed platform accountability frameworks.

**Singapore**, whose Online Safety Act 2022 gives authorities broad powers to direct platforms to disable access to harmful content.

The **United Kingdom**, as already discussed in detail.

In aggregate, blocking all these jurisdictions would mean excluding the entirety of the EU, the UK, Canada, Australia, much of Asia, and significant parts of Latin America. What remains would be essentially the United States, plus a collection of smaller nations that have not yet enacted platform liability legislation — a list that shrinks every year as the international regulatory tide continues to move in just one direction.

### Is This Level of Operation Feasible?

Technically, yes — geoblocking all of the above is achievable with the same infrastructure discussed in the previous answer, scaled up. IP ranges for most countries are well-documented, and commercial geoblocking services can implement and maintain this automatically.

Commercially and practically, the answer is almost certainly no, for several reasons.

1. The addressable user base would be reduced to the United States population plus a diminishing rump of unregulated jurisdictions. For a social annotation platform whose value proposition depends on network effects — the more users annotating the web, the more valuable each annotation becomes — this would be a crippling constraint.

2. The VPN circumvention problem discussed in the previous answer scales with the number of blocked countries. The larger and more diverse the blocked list, the more users have routine, non-malicious reasons to be using a VPN, and the more porous the geoblocking becomes in practice.

3. The regulatory landscape is also not static. The United States itself is not a permanently safe harbour. Section 230 has faced sustained legislative pressure for years, individual US states have passed or attempted to pass their own platform liability laws, and the legal environment in even the one jurisdiction NetNubby would be relying on is in flux.

4. Perhaps most fundamentally, there is a philosophical tension at the core of this strategy: the web itself is borderless by design. **A service whose core function is to overlay annotations on any web page — including pages hosted in, and accessed by users in, every country on earth — is structurally ill-suited to a jurisdiction-exclusion model.** Unlike a streaming service that can license content territory by territory, NetNubby's product is the internet itself as its canvas. Restricting participation to US users would not prevent a US-registered user from posting a Note on a page primarily read by people in Germany, Australia, or the UK — and those downstream readers, encountering the Note, may themselves be subject to laws that consider the platform's content their concern.

### The Realistic Alternative

Rather than attempting pure jurisdictional insulation, most US-based platforms of NetNubby's type and scale reach an accommodation: they maintain Section 230 as their primary domestic shield, implement a baseline of good-faith moderation sufficient to invoke the equivalent protections available in other jurisdictions (such as the E-Commerce Regulations safe harbour in the UK), and rely on the practical enforcement gap — the difficulty regulators face in pursuing small foreign platforms — as their actual insulation from liability. This is less elegant than a clean legal answer, but it is how the overwhelming majority of small US platforms with international user bases actually operate in practice.