NEWS / MEDIA ALLIANCE

MYTHS & FACTS

The Stealth Bot Prohibition Act (SBPA)

A quick-reference guide for responding to common misconceptions about the Stealth Bot Prohibition Act — for use with press, congressional offices, and other stakeholders.

QUICK REFERENCE

Jump to any myth below — each is linked to its full response.

1. **Investigative journalism**
2. **Technical burden of ID**
3. **"Just block bots yourself"**
4. **First Amendment rights**
5. **Unprecedented regulation**
6. **Unrestrained access to information**

MYTH 1

The Stealth Bot Prohibition Act (SBPA) would stop journalists, researchers, and cybersecurity professionals from performing key portions of their jobs.

FACT

The bill only affects bots that impose a burden on web hosts (section 2(a)(1)), which does not encompass the limited use of anonymous bots for investigative, research, or cybersecurity purposes. It only holds bad bots, not all bots, accountable when they don't identify themselves.

That said, the Senate version of the bill has additional language included to further clarify that these and other legitimate uses are deliberately excluded from the bill's definition of stealth bots, protecting human users, journalists, researchers, and other good actors whose legitimate activities should not be unintentionally swept into the legislation. While the existing language will not interfere with good actors, these safeguards will help protect reporting, research, and access to information while addressing the deceptive conduct the bill is intended to stop.

MYTH 2

Asking companies to identify their bots creates a significant and unfair technical burden.

FACT

A rebuttal directly from Tollbit in their post supporting the SBPA:

> *"The objection tech and scraping companies will raise is that this is a burden. It isn't. Identifying yourself is one of the easiest things a bot can do. It is far less complicated and expensive than the extensive efforts these bots use today to hide themselves.*
>
> *We know what lengths scraping companies go to remain hidden, because we've cataloged it for nearly 40 vendors. The evasion techniques these scraping vendors use today include residential proxy networks that route requests through real homes (the same technique foreign hackers use), rotating IP addresses, user agent spoofing, and they charge up to $22.50 per thousand pages.*
>
> *All this effort and cost is deployed to avoid detection. Instead of investing in that, this bill would simply require identification. It's a basic ask that the well-behaved bots, like Googlebot, already abide by."*

MYTH 3

Publishers can just block bots using existing technical means, there's no need for legislation on this issue.

FACT

Publishers have tried to stop these bots on their own, but it's impossible to stop them all when malicious bots are able to disguise themselves and act with impunity. Small publishers simply don't have the resources to filter out bad bots, and even larger, more sophisticated publishers can't keep up. Twenty-five percent of Politico's hosting costs now go toward bot management, for example, but bots still get through. This problem is virtually universal - one study by Tollbit found that 95% of top sites are unable to completely block scrapers.

MYTH 4

The bill threatens First Amendment rights by forcing citizens to state who they are and how they will use public information just to access websites.

FACT

Individual users are not inherently subject to the SBPA, unless they're deploying stealth bots on a massive scale for a nefarious purpose. The Senate bill includes exceptions that specifically exclude human users from the bill's requirements.

MYTH 5

This kind of regulation of the internet is unprecedented.

FACT

Congress has repeatedly responded when technology makes the origin of communications difficult to determine. There is a lengthy, strong precedent for the disclosure measures in our bill. Across multiple channels, automated or electronic communications have been required to disclose what they are and/or who is behind them, and Congress can prohibit concealing or falsifying identifying information, for the purpose of protecting consumers and businesses.

A number of laws require automated or electronic communications to disclose what they are, who is behind them, and/or prohibit concealing or falsifying identifying information.

- Artificial/prerecorded calls must state the identity of the business, individual, or entity initiating the call and provide a phone number/address. (Telephone Consumer Protection Act (TCPA)).
- It is illegal to knowingly transmit misleading/inaccurate caller ID with intent to defraud, harm, or obtain value. (Truth in Caller ID Act).
- Phone companies are required to use congressionally-mandated identity-authentication architecture to verify that the caller ID information transmitted with a call matches the caller's real phone number. Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)
- Commercial email headers and routing information must be accurate and identify the person/business initiating the message. (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)).
- The falsification/concealment of email headers, domains, accounts and IP registration information is criminalized in certain circumstances. (CAN-SPAM Act).

State legislatures in California (Bot Disclosure Law), Utah (AI consumer protection law) and Colorado (chatbot law) have also enacted disclosure requirements for bot activity.

MYTH 6

Unrestrained access to information is a good thing, and legislation that blocks anyone (or anything) from gathering information is inherently bad.

FACT

News publishers recognize the importance of access to information. They work tirelessly every day to ensure that their readers have access to high-quality, timely information about the world around them. But while we want to create and spread quality information widely, the current onslaught of bad bots is counterproductive to those goals. Allowing bad bots to overload websites and steal information isn't expanding access to information, it's actually doing the opposite. Unrestricted access to information means less overall access to information in the long run.

Reporting the news is expensive, and in order for publishers to continue producing high-quality journalism, they need to have sustainable revenue sources. But when bad bots steal journalistic work, they undermine subscription and advertising revenue streams, and block the growth of a nascent content licensing marketplace. If this continues, news publishers will be forced to limit coverage, lay off reporters, reduce frequency of publication, or shut their doors entirely, shrinking the public's overall access to information.