## Cloudflare (used by 6million websites to improve speed) bans Switter.at (Twitter for workers)

<https://motherboard.vice.com/en_us/article/9kgvga/cloudflare-switter-down-fosta-sesta>

On Wednesday 18 April, [Cloudflare terminated its content delivery network services](https://motherboard.vice.com/en_us/article/8xk78x/switter-down-cloudflare-banned-sex-workers-sesta-fosta) for an alternative, decentralized social media platform called Switter. Developed by the Australia-based organization Assembly Four, the weeks-old Switter served as a home for thousands of sex workers and their fans and clients after they were kicked off or preemptively removed themselves from mainstream internet platforms because of FOSTA.

See also <https://motherboard.vice.com/en_us/article/8xk78x/switter-down-cloudflare-banned-sex-workers-sesta-fosta>

Cloudflare provides DNS services to 6 million websites,[[43]](https://en.wikipedia.org/wiki/Cloudflare#cite_note-cloudflareblog1-43) including [Uber](https://en.wikipedia.org/wiki/Uber_%28company%29), [OKCupid](https://en.wikipedia.org/wiki/OKCupid), and [Fitbit](https://en.wikipedia.org/wiki/Fitbit), adding approximately 20,000 new customers every day.

This is not an ‘establishment’ operation:

Cloudflare has been vocal of their values, with CEO Matthew Prince stating:

"One of the greatest strengths of the United States is a belief that speech, particularly political speech, is sacred. A website, of course, is nothing but speech...A website is speech. It is not a bomb. There is no imminent danger it creates and no provider has an affirmative obligation to monitor and make determinations about the theoretically harmful nature of speech a site may contain."

Switter.at seems to have moved to masking their IP via a large Australian host, but their site appears now to be hosted by a subsidiary of Orange in Egypt. Hence very slow connection times to the USA.

##

## [‘Domains by Proxy’ Hands Over Personal Details of “Pirate” Site Owner](https://torrentfreak.com/domains-proxy-hands-personal-details-pirate-site-owner-140307/)

In 2014 Domains by Proxy, the domain privacy service offered by GoDaddy, which is owned by GoDaddy founder Bob Parsons, handed over his personal details without a subpoena, or any form of due process.

“We have received a possible legal complaint regarding your domain name xxx.com,” Domains By Proxy informed the site owner.

“Since we were provided with proof the complainant owns a potentially applicable copyright, we have disclosed your identity for the limited purpose of this complaint so that the complainant can communicate directly with you to seek resolution.”

Their ToS state:

Cancel the privacy service (which means that Your information will be available in the "Whois" directory) and/or reveal Your name and personal information that You provided to DBP:

A. When required by law, in the good faith belief that such action is necessary in order to conform to the edicts of the law or in the interest of public safety;

B. To comply with legal process served upon DBP or in response to a reasonable threat of litigation against DBP (as determined by DBP in its sole and absolute discretion);

https://torrentfreak.com/domains-proxy-hands-personal-details-pirate-site-owner-140307/

# **Serving Subpoenas to Unmask the Identities of Website Owners, Domain Registrants**

### This is not in the area of sex workers but outlines how website owners and operators can be unmasked.

When unidentified individuals defame businesses or professionals online, the harmed parties can potentially serve subpoenas on relevant entities for documents containing identifying information about the authors of the online defamation.

The way this process often plays out is as follows (noting this is extremely generalized):

* Party A publishes false and defamatory statements about Party B in a review on a third-party website;
* Party B, which/who has adequate legal grounds for doing so, files a lawsuit against the unknown Party A for defamation and related causes of action;
* Party B serves a subpoena—seeking documents containing identifying information pertaining to Party A—on the parent company of the website on which Party A published his or her defamatory statements
* The subpoenaed entity produces the requested documents, from which Party B will either learn Party A’s identity, or Party B will need to consider issuing additional subpoenas based on new information produced in response to the first subpoena (such as IP addresses and/or email addresses owned by other entities).

While we most often see internet defamation take place on third-party websites—and we have published several blog posts about using subpoenas to [identify anonymous defamers](http://www.defamationremovalattorneysblog.com/category/identify-anonymous-defamers/) on various websites—some people actually register new domains and publish false and defamatory content on their own websites.

In this latter scenario, the website owner/author of the damaging statements is unlikely to leave identifying information on his or her website. Further, he or she might even use a privacy service to hide his or her contact information, which is legitimate so long as he or she has not provided [fake or inaccurate contact information](http://www.defamationremovalattorneysblog.com/2016/01/3169icann-whois-inaccuracy-domain-cancellations/).

Nonetheless, parties who are victims of anonymous defamation on specially-created websites are not out of luck.

If they can meet the necessary standards and comply with the relevant statutes, defamed businesses and professionals can potentially subpoena domain registrars, privacy services used to mask domain contact information (if relevant) or even the web hosts. You can determine domain registrars and contact information from a [WHOIS search](https://who.is/), while there are various host lookup websites on which people can enter domains to determine their hosts.

One of the most popular registrar and web hosting companies in the United States is GoDaddy.com, LLC, better known simply as GoDaddy. In fact, the company has “more than 14 million customers worldwide and more than 63 million domain names under [its] management,” according to its website.

Thus, say that a harmed business determines that the website on which someone published defamatory content about it is registered with GoDaddy, the business can prepare a subpoena to the Scottsdale, Arizona-based GoDaddy. *See* GoDaddy’s [subpoena compliance policy](https://www.godaddy.com/agreements/showdoc.aspx?pageid=CIVIL_SUBPOENA).

A subpoena to GoDaddy might include, among other things, requests for the GoDaddy customer’s billing records or other documents containing the customer’s contact information. Of course, subpoenaing GoDaddy in Arizona requires that the requesting party be familiar with relevant laws and procedures, especially if the party is not from/the case is not based in Arizona.

Many people who register their domains with GoDaddy also use GoDaddy’s privacy service, Domains by Proxy, LLC, to mask the registrant, administrative, and technical contact information. Thus, it can be beneficial to separately subpoena Domains by Proxy, LLC for identifying information pertaining to a Domains by Proxy customer’s domain. *See* Domains by Proxy’s [subpoena compliance policy](https://www.godaddy.com/agreements/showdoc.aspx?pageid=CIVIL_SUBPOENA), noting GoDaddy’s compliance department also manages Domains by Proxy subpoenas.

GoDaddy and Domains by Proxy take about 30 days to respond to subpoenas. If, upon notification to the relevant customers, there are no objections to valid subpoenas, GoDaddy and Domains by Proxy will produce the requested documents/information.

As an alternative to subpoenaing registrars (including, but certainly not limited to, GoDaddy) or privacy services like Domains by Proxy, defamed businesses and professionals might also consider serving subpoenas on the hosts of the websites on which they have been disparaged. Hosts essentially provide space on their servers to make customers’ websites accessible online.