PROTECTING AGAINST ONLINE ABUSE AND HARASSMENT, OFTEN BY THIRD PARTIES: RESOURCES AND INFORMATION FOR THE YALE COMMUNITY[1]

OVERVIEW

In recent years, the academic community has seen an increase in incidents of online harassment from outsiders. Students, faculty, staff, postdocs, and other academic appointees who publish articles, provide expert commentary, or are active on social media can become targets for online harassment.

Online harassment can take different forms:

- "Trolling" occurs when individuals deliberately follow and provoke others online, often with offensive content. While most trolling is merely a nuisance, occasionally trolling attacks can escalate to threats or to the point where numerous individuals are engaged in harassing the target and/or target's organization.
- "Doxing" (sometimes "doxxing") is when private identifying information that is not otherwise publicly available is published online. This information can include sharing an individual's private email, personal phone number, home address, etc. on various platforms to frighten the individual and encourage additional harassment.
- "Cyberbullying" is the willful and repeated harm inflicted through using computers, cell phones, and other electronic devices.

These situations can be very intense, alarming, and disruptive to an individual. Online targeting can also have real consequences for livelihoods and careers. Yale provides this document as a resource for community members who have been identified and targeted for online abuse, harassment, and intimidation.

Please note the following guidance contains resources and information on reporting incidents of cyber-bullying, doxing, or trolling. It is not the process for reporting conduct that violates or may violate the university's harassment/discrimination/bullying policy. You can find information about that policy here.

WHAT RECOURSE DO I HAVE AGAINST ONLINE ABUSE AND HARASSMENT?

Steps you can take to combat online abuse and harassment include (1) requesting takedowns of false statements that may have been made in error, (2) requesting that platforms and web domain registrars remove abusive content, (3) documenting the abuse (*i.e.*, preserving evidence), (4) reporting threats and other criminal misconduct to law enforcement, and (5) obtaining legal advice regarding consequences to you and possible civil actions against abusers. Legal action may be of limited utility in these matters.

[1] Adapted with permission from similar guidance provided by Harvard University.

Requests To Take Down False Statements

If an organization has posted false or misleading statements about you on its website, social media accounts, or elsewhere, and these statements are causing you to suffer harm, you may consider sending a written request to the organization to remove or correct the statements. In such a communication it is important that you (1) identify yourself, (2) identify the statements that are false or misleading, (3) explain why the statements are false or misleading, and (4) describe how the statements are harming you.

Not all such requests will be successful, but longstanding organizations with financial resources and credibility in the broader community may see that correcting false, harmful information is in their self-interest. Takedown requests directed to individual user accounts on social media platforms may not be as well received—especially if the accounts are anonymous or pseudonymous. An example of a request to take down false information is attached below ("Sample Request to Take Down False Statements"). If the recipient of your initial request ignores or declines it, you may consider engaging an attorney to write a follow-up letter on your behalf.

In cases where a user account has posted false or misleading statements about you on a social media or other publishing platform, you may have the additional option of reporting the content to the platform. *See* the next section below. Generally speaking, social media sites are reluctant to referee disputes over whether the content of a particular post is true or false. Indeed, you are likely to find that the applicable community standards or guidelines do not prohibit false statements (as opposed to, say, impersonations). Accordingly, while the platform may seem to be a more rational and objective actor than the user account, you may find that the platform does not act on the report.

Note: Before you submit a request to take down harmful content, you should save a copy of the content in order to preserve evidence of the abuse. *See* below ("Document What's Happening").

Requests To Take Down Abusive, Harassing, or Threatening Posts/Web Content

If a user account has posted abusive, harassing, or threatening statements about you or directed at you on a social media or other publishing platform, you may submit a takedown request to the platform, in accordance with the platform's rules and requirements, several of which we have linked here:

- Blogger/ Blogspot: Content Policy, Report a Community Violation.
- Facebook: Community Standards, Report Something.
- Instagram/ Threads: Community Guidelines, How to Report Things.
- Sidechat: Community Guidelines. Users may report a post for removal by emailing support@sidechat.lol.
- Substack: Content Guidelines ("If you encounter content that may be in breach of these guidelines or have any questions about them, you can email us at tos@substackinc.com.").
- TikTok: Community Guidelines, Report a Problem.

- Truth Social: Terms of Use § 7 ("Prohibited Activities"). § 32 of the Terms of Use document states as follows: "In order to resolve a complaint regarding the Service or to receive further information regarding use of the Service, please contact us at support@truthsocial.com. "Users may report 'hateful conduct,' as defined by New York law, to legal@tmtgcorp.com."
- Wordpress: User Guidelines, Report a Site.
- X/ Twitter: The X Rules, Report Violations.
- YouTube: Community Guidelines. To report content on YouTube, you can click the "Report" button underneath the video frame on each video's webpage. To reveal the "Report" button, click the icon with three dots on it, just under the right-bottom corner of the video.

In cases where abusive content is posted on a website operated by the speakers themselves (rather than, say, Facebook or Substack), you may still be able to request that it be taken down. Many companies that provide web hosting services have their own community standards/acceptable use policies and allow visitors to websites to report abuse. There are some prominent web hosting vendors in the list below:

- DreamHost: Acceptable Use Policy, Report Abuse.
- GoDaddy: Universal Terms of Service § 5 ("General Rules of Conduct"), Report Abuse.
- Hostinger: Universal Terms of Service § 5 ("General Rules of Conduct"), Report Abuse.
- WP Engine: Acceptable Use Policy. Users may report violations of the Acceptable Use Policy to abuse@wpengine.com or (512) 273-3906.

Each social media platform or web hosting service applies its own standards and principles in reviewing and acting on requests to take down content. As noted above, platforms are reluctant to referee disputes over whether the content of a particular post is true or false.

They are far more likely to take action against communications that are abusive, harassing, or threatening or that impersonate you or seek to mislead or defraud the viewer. You can find more details on each site's rules and reporting pages.

We generally do not recommend that you engage directly with a social media account or website that is targeting you with abuse, harassment, or threats. If you see content on a social media platform or website that is directed at you and violates the site's community standards, you should report the content to the platform or web host.

An example of a request to take down abusive, harassing, or threatening posts is attached below ("Sample Request To Take Down Abusive, Harassing, or Threatening Posts/Web Content").

Note: Before you submit a request to take down harmful content, you should save a copy of the content in order to preserve evidence of the abuse. *See* below ("Document What's Happening").

Requests To De-Register Abusive Domain Names

We are aware of instances in which an online harasser has registered the names of individual persons as web domains and established websites at those domains to host online attacks on the named persons. It may be possible to have these domain names de-registered. The first step is to conduct a "whois" search to identify what domain registrar company (*e.g.*, Domain.com, GoDaddy) has registered the domain.

Requests To Domain Name Registrars. To perform a "whois" search, go to https://lookup.icann.org/en and enter the domain name into the search window. The search results will display, among other things, "Domain Information," "Contact Information," and "Registrar Information." The Registrar Information block identifies the domain registrar. The Contact Information block displays the contact information for the person who registered the domain, which may be a proxy company that has been paid to register the domain name on the actual user's behalf, so that you cannot tell who is really operating the website. In any case, several links will appear in the Contact Information block that, if clicked, will take you to the domain registrar's website.

The landing page on the domain registrar's website should display a phone number and email you can contact to report abuse to the registrar. In addition, the registrar's website will likely provide information about community standards for its registrants and how to report violations of its policies. Links to this information can usually be found in the footer of the website behind links that say "Legal," "Terms of Use," or "Terms of Service." We have collected below the community standards policies and reporting information posted by several popular domain registrars. The first link in each line is to information about the registrar's content standards: *i.e.*, what is allowed on their registered websites and what is not. The second link is to information about how to report abuse.

- Domain.com: Acceptable Use Policy, Report Member Violations.
- DreamHost: Acceptable Use Policy, Report Abuse.
- GoDaddy: Universal Terms of Service § 5 ("General Rules of Conduct"), Report Abuse.
- Hostinger: Universal Terms of Service § 5 ("General Rules of Conduct"), Report Abuse.
- Namecheap: Acceptable Use Policy, Report Abuse.
- Porkbun: Product Terms of Service ("Acceptable Use Policy" section), Report Abuse.

If you use the registrar's abuse reporting function and the registrar agrees that the website registered under your name has violated its content policies, the registrar may de-register the domain name. De-registration of a domain name is a big step for a registrar to take, and it will be more likely to take that step if the domain name contributes to violations of the registrar's rules. In cases where the site posts abusive content but the domain name itself is not objectionable, a takedown request to the web hosting company is more likely to be successful than a request to decommission the domain name. (In many cases the domain registrar also provides web hosting services for the site.)

An example of a request to de-register domain names is attached below ("Sample Request to De-Register Abusive Domain Names"). You can use the same template to submit a de-registration request to a domain name registry.

The fact that one domain registrar company has taken steps to de-register a domain does not mean that the harasser cannot go to another registrar to re-register the name. Accordingly, you may need to visit the domain name periodically to see if it has been re-registered and is again posting the abusive content. If so, you will need to do another whois search and report abuse to the current registrar. Alternatively, you can register the domain name yourself, so that you can exclude others from using it.

Note: Before you submit a request to de-register a domain name, you should save a copy of all the content posted on the website in question in order to preserve evidence of the abuse. *See* below ("Document What's Happening").

Requests To Domain Name Registries. In addition to reporting abuse to a domain name *registrar*, you may also try reporting abuse to a domain name *registry*. A registry is an organization that controls the registration of all domain names within a top-level domain ("TLD") like ".com" or ".org." The registry for .com and .net domains is Verisign, and the registry for .org domains is the Public Interest Registry. We have gathered the following information about reporting abuse to these organizations:

- Verisign: "For any inquiries related to malicious conduct in the Verisign managed TLDs please contact Verisign at abuse@verisign.com."
- Public Interest Registry: Anti-Abuse Policy (generally disfavoring suspension of domain names, except in rare cases, such as "credible and specific incitements to violence" and "credible threats to human health or safety"), Report Abuse.

Our sense is that it may be more difficult to persuade a domain-name registry to de-register than to persuade a registrar to do so, so you should first try the applicable registrar.

Note: Before you submit a request to de-register a domain name, you should save a copy of all the content posted on the website in question in order to preserve evidence of the abuse. *See* below ("Document What's Happening").

Document What's Happening

If you are experiencing online abuse, harassment, or threats, you should take steps to preserve evidence of the communications.

- Save any emails, voicemails, or text messages you receive.
- Take screenshots or photos of comments on social media; because such comments can be deleted, screenshots are often useful to help document them.

While it may seem counterintuitive to hold onto messages or posts that are upsetting, it can be helpful down the line to have retained evidence of an attack, particularly one involving threats. Create a folder separate and apart from your live accounts and store copies or

screenshots of the abusive communications inside it. This way you can keep the evidence without having to see the communications again and again as you use these systems.

Reporting Criminal Conduct

States, including Connecticut, have written criminal laws to protect their residents against harassment and intimidation.

If you or those close to you are in imminent physical danger or there has been a direct threat of physical violence, you should immediately call the Yale University Police Department at (203) 432-4400 if you are on the Yale campus. If you are not on campus, call 911.

If there is no immediate physical threat, but you have received a credible threat to your personal safety or feel you have been criminally harassed, you may call contact Sergeant Kristina Reech (cell phone 203-464-4514) or Officer Gabrielle Cotto (cell phone 475- 267-9622) of the Yale Police Department.

Seeking Immigration Help

Some members of the community may have questions about how abusive or harassing online conduct may affect their immigration status or prospects. International students can reach out to their advisor in the Office of International Students and Scholars (https://oiss.yale.edu/) with concerns related to their immigration status.

Legal Consultations

You may wish to explore whether to pursue a legal complaint for online harassment. In doing so, be sure to explore with your lawyer the benefits and risks of pursuing a legal claim, the cost of doing so, and the barriers to a successful claim**.**

BASIC STEPS YOU CAN TAKE TO PROTECT YOUR ONLINE ACCOUNTS

1. Activate multifactor authentication everywhere you have a login. Your Yale netid is already protected, but you should activate MFA on all social media, external email, and financial accounts. If possible, don't use text message-based MFA. Phone apps like DUO or Google Authenticator are generally more secure. Multifactor authentication is the most important step you can take to protect your online security.
2. Change your passwords to something unique for each account.
3. A password manager can help. Your browser is a simple password manager. You can also use something like https://1password.com or https://keepass.info.
4. Consider whether to activate privacy features in social media accounts.
5. After you have secured your own accounts, consider whether you should encourage family members or significant others to take similar steps.

WHAT ELSE CAN I DO TO PROTECT MYSELF?

Managing Abuse and Harassment on Social Media

Online harassment of any kind can be extremely stressful. In addition to support that is available through the university or law enforcement, the following actions may help individuals respond to a difficult situation occurring online:

Consider temporarily disabling your social media profiles or switching them to private. This will ensure that only your close connections can post or comment in your feed.

Ignore the communications. Although your first instinct may be to respond and defend yourself online, responding to harassing messages can tend to prolong and inflame incidents. Often the objective of social media agitators is to elicit a response, which they can use to raise their profile still further. In addition, your response may provide more opportunity for harassment: *i.e.*, the online abuser will find a way to mischaracterize, take out of context, and cast what you say in the worst possible light. Trolls may—but do not always—move on to other targets if you ignore them long enough.

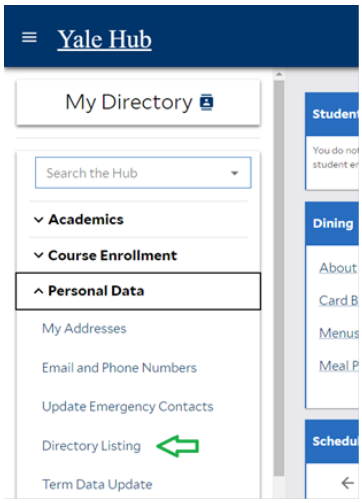
Stick to the facts. If you do feel that a response is necessary, try to adhere to the following guidelines: (1) stick to facts that are not open to interpretation; (2) keep your response short, concise, and above all factual; (3) correct inaccuracies and move on; (4) avoid adopting an aggressive or defensive tone and resist the temptation to "fight fire with fire."

Mute the attacker. Most social media platforms allow users to "mute" particular accounts. Muting another user means that user's communications are not viewable to you. The muted party ordinarily is not notified that you have muted them and may still comment on your social media posts, but you will not need to see those comments. If you are worried a muted user's comments may become threatening, ask a friend or colleague to check your feed on your behalf.

Block the attacker. Several social media platforms allow you to "block" other accounts, meaning that they can longer follow you, see your posts, or comment on your content. Unless you have also muted the account, you will still be able to see a blocked user's posts. Social media platforms ordinarily notify users when another account blocks them. Accordingly, they may choose to attack you elsewhere on the platform.

Delisting from University Directories

If you are concerned that online harassers can find you on campus or use your Yale email or phone number to direct harmful communications to you, you may manage your information in the university directory through Yale Hub. Once logged in, see "Directory Listing" under "Personal Data" on the far right. Faculty and staff can update their directory information in WorkDay.



Note: Members of the community should be aware that these instructions may not result in the delisting of all Yale-related programs and activities. Reach out to your Yale affiliations (academic department, extracurricular activities, etc.) if you wish to make a similar request.

Requesting a Non-Disclosure

Students may also direct the university not to disclose information designated as "directory information" under FERPA, the Federal Educational Rights and Privacy Act. Under FERPA, a university may disclose a student's directory information to any person, unless the student opts out of such disclosures. Click here for more information about what qualifies as "directory information" and how to request an opt-out from the Registrar's Office.

Email Filtering

Email filters can be an effective way to automatically block, filter, or delete incoming messages. Instructions below detail how to set up filters for both Microsoft and Google accounts.

Microsoft Outlook:

Step 1: Log into Outlook on the web (outlook.office.com).
Step 2: Once you are in the mailbox, click on the ellipsis (…), click on "Rules," then "Manage Rules." This will open a new window.
Step 3: Click on "+ Add New Rule." Name your new rule.
Step 4: Click on "Add a Condition." "Subject or body includes" can be an effective condition, if there are common keywords in the subject line or body of their messages. Enter those keywords.
Step 5: Click on "Add an Action." Select "Move to," click on "Select a Folder," click on "Move to a Different Folder," and select "Junk Mail."
Step 6: **This is essential in order to implement the new rule.** Confirm that the "Stop Processing New Rules" checkbox is checked. Confirm that the "Run Rule Now" checkbox is checked. Then click "Save."

Click here for additional support from Microsoft.

Gmail:

Step 1: Click the gear symbol in the top right corner of your Gmail window.
Step 2: Click on "See All Settings." Then Click on the "Filters and Blocked Addresses" tab.
Step 3: Click "Create a New Filter." If there are common words in the subject line or body of the message, enter those words into the "Subject" or "Has the words" field. You can also filter out messages from a particular sender by entering that email address into "From." When you have defined the filter, click "Create filter."
Step 4: A new window will open, asking you what to do with filter email. Check the "Skip the Inbox (Archive it)" checkbox.
Step 5: Check the "Apply the Label" checkbox and click on "Choose label," then "New label." Another window will open. Type "Junk Email" into the new label name field and click "Create."
Step 6: **This is essential in order to implement the new filter.** Click "Create filter." You can search for filtered spam emails by clicking "Labels," then "Junk E-Mail" in the left toolbar.

Click here for additional support from Google.

Note: If you block or filter abusive messages, you may not be made aware of threats sent to your account.

ADDITIONAL ONLINE SERVICES

Removing harmful personal information from the Internet can be a time-consuming task. There are services that can manage this effort on your behalf. This *Consumer Reports* article identifies individual steps you can take, along with several *CR*-vetted companies who do this work.

COUNSELING SERVICES

Students can contact Mental Health and Counseling at Yale Health at (203) 432-0290 during business hours and for urgent concerns after hours.

Faculty, staff, and post-docs can find information about Yale's Employee Assistance Program at Yale Signature Benefits | It's Your Yale.

The Chaplain's Office (Old Campus, Bingham Hall, Entryway D; 203-432-1128), Yale Religious Ministries; the Joseph Slifka Center for Jewish Life at Yale (203-432-9419); and Muslim Life at Yale (203-432-8753) are among the resources available to all members of our community.

ADDENDUM:
TEMPLATES OF TAKEDOWN REQUESTS

SAMPLE REQUEST TO TAKE DOWN FALSE STATEMENTS

Dear _____:

My name is [insert], and I am a [student, former student, faculty member, employee, postdoc, etc.] at Yale [College, Law School, etc.] I am writing to ask you to take down the post appearing at [URL address] stating that I joined in a statement issued by [person/organization] on or about [date] concerning [subject matter]. I also request that my name and photograph be removed from [additional publication] that falsely associates me with the statement. The information your organization has published about me is false. I had no knowledge of nor did I approve of the statement before or after publication. [If applicable: At the time of publication, (a) I had no affiliation with the [name of organization] and/or (b) I no longer was an officer of the organization.]

Falsely associating me with the statement has subjected me to online attacks and harassment as well as threatening personal confrontations that have caused me to fear for my physical safety. The false information you have published about me also threatens [my future employment prospects, etc.].

Now that you know the information about me published on [URL address] and [additional publication] is false and causing me harm, I request that the information be taken down immediately.

Thank you for your prompt attention to this matter.

Sincerely,

[Name]

SAMPLE REQUEST TO TAKE DOWN ABUSIVE, HARASSING, OR THREATENING POSTS/WEB CONTENT

Dear _____:

My name is [insert], and I am a [student, former student, faculty member, employee, postdoc, etc.] at Yale [College, Law School, etc.] I am writing to ask you to take down the post appearing at [URL address] stating that I joined in a statement issued by [person/organization] on or about [date] concerning [subject matter]. I also request that my name and photograph be removed from [additional publication] that falsely associates me with the statement. The information your organization has published about me is false. I had no knowledge of nor did I approve of the statement before or after publication. [If applicable: At the time of publication, (a) I had no affiliation with the [name of organization] and/or (b) I no longer was an officer of the organization.]

Falsely associating me with the statement has subjected me to online attacks and harassment as well as threatening personal confrontations that have caused me to fear for my physical safety. The false information you have published about me also threatens [my future employment prospects, etc.].

Now that you know the information about me published on [URL address] and [additional publication] is false and causing me harm, I request that the information be taken down immediately.

Thank you for your prompt attention to this matter.

Sincerely,

[Name]

SAMPLE REQUEST TO DE-REGISTER ABUSIVE DOMAIN NAMES

To Whom it May Concern:

My name is [insert]. I am writing because [registrar name] is the registrar for the domain name [website URL]. This domain name is being used for a website containing false information. It is making unauthorized use of my name and contains false information about me. [Add details, e.g., The website falsely claims that I ….]

The owner of the domain name for the website is in direct violation of [registrar's] Terms of Service, which prohibit using the site in a way that infringes on intellectual property rights or involves any false, abusive, or fraudulent activity. [Cite or quote Terms of Service.] The website is fraudulent and a violation of trademark and copyright laws as detailed above. As a result, [registrar] has the right to terminate its services and potentially take necessary legal action. [Cite or quote Terms of Service.]

Given the misleading nature of this site I request that [registrar] immediately cease providing domain name registrar services to the infringing website and take all actions available to [registrar] to prevent the party responsible for the site from transferring the domain name, changing website hosting providers, or taking other actions that will allow for further infringement of my rights.

Failure to expeditiously disable access to the fraudulent and infringing website may expose [registrar] to liability.

Thank you for your prompt attention to this matter.

Sincerely,

[Name]