



ELECTRONIC FRONTIER FOUNDATION

Protecting Rights and Promoting Freedom on the Electronic Frontier

January 13, 2016

BY EMAIL — OCR@ed.gov

Secretary Arne Duncan
U.S. Department of Education
Lyndon Baines Johnson Department of Education Bldg.
400 Maryland Avenue, SW
Washington, DC 20202-1100

Assistant Secretary Catherine Lhamon
U.S. Department of Education
Office for Civil Rights
Lyndon Baines Johnson Department of Education Bldg.
400 Maryland Avenue, SW
Washington, DC 20202-1100

Re: Recent request for guidance on schools' obligations under Title IX and Title VI to address sex- and race-based harassment on anonymous online platforms

Dear Secretary Duncan and Assistant Secretary Lhamon:

The Electronic Frontier Foundation (EFF) writes in response to a request for guidance sent to the Department of Education (Department) on October 20, 2015 by a coalition of organizations seeking new rules surrounding the use of anonymous online platforms on college and university campuses.¹ EFF is a non-profit member-supported civil liberties organization founded in 1990 to protect rights in the digital world.

EFF agrees with the Coalition that gender and racial harassment and threats perpetrated on online platforms are a serious problem that can disproportionately affect communities of color and women.² EFF also agrees with the majority of the Coalition's recommendations regarding online harassment and threats occurring at universities and colleges, including ensuring prompt reporting and investigation of online harassment by universities, police, and online platforms where appropriate, disciplining and/or prosecuting perpetrators of threatening or harassing conduct, providing counseling and

¹ *72 Women's and Civil Rights Groups Urge Education Department to Issue New Federal Guidelines to Protect Students from Harassment and Cyber-threats Via Anonymous Social Media* (Oct. 21, 2015), available at <http://feminist.org/news/pressstory.asp?id=15714> (Coalition Letter).

² See Dia Kayyali & Danny O'Brien, *Facing the Challenge of Online Harassment* (Jan. 8, 2015), available at <https://www.eff.org/deeplinks/2015/01/facing-challenge-online-harassment> (outlining EFF's views on online threats and harassment).

815 Eddy Street • San Francisco, CA 94109 USA

voice +1 415 436 9333

fax +1 415 436 9993

web www.eff.org

email information@eff.org

accommodations for targets of online harassment and threats, and greater training of students, faculty, and staff about online threats and harassments.³

EFF, however, does not agree with the Coalition’s request to require colleges and universities to preemptively remove anonymous online speech platforms from campus or to otherwise restrain speech protected by the First Amendment.⁴ In addition to violating the U.S. Constitution, such rules would undermine the efforts of many people who rely on anonymous speech for any number of important purposes, including groups seeking to foster gender and racial equality on campuses across the country. Over the past few years, we have seen how policies that impede online anonymity, such as Facebook’s Real Names policy, present barriers to speech for marginalized communities and others who fear retaliation for their political or social commentary.⁵

EFF therefore respectfully requests that any future guidance issued by the Department uphold all of the civil and constitutional rights of those who attend colleges or universities, including both freedom from harassment and freedom of anonymous speech.

Colleges and universities must protect the civil and constitutional rights of everyone on campus, including the right to be free from harassment and threats.

EFF agrees with the Coalition that the First Amendment does not protect true threats and unlawful harassment. Online threats and harassment—anonymous or not—violate the civil and constitutional rights of their targets, often causing real and lasting harm. EFF believes in the fundamental power of the Internet and other emerging technologies to help individuals with less power or fewer resources to communicate more broadly and more effectively than ever before. But the Internet’s powerful communications tools, like any tool, can also be misused to harass individuals and particular groups, or to coordinate such attacks.

Educational institutions have an obligation to respond when true threats or unlawful harassment occur. These institutions have many ways to respond to true threats and unlawful harassment, including many of the recommendations provided by the Coalition, in addition to others suggested below.

³ Coalition Letter *at* 17.

⁴ The Coalition Letter specifically requests that the Department recommend that institutions “bar[] the use of campus wi-fi to view or post to these applications” and “geofenc[e] anonymous social media applications that are used to threaten, intimidate, or harass students.” *Id.*

⁵ Dia Kayyali, *Global Coalition to Facebook: ‘Authentic Names’ Are Authentically Dangerous for Your Users*, Electronic Frontier Foundation (Oct. 5, 2015), available at <https://www.eff.org/deeplinks/2015/10/global-coalition-facebook-authentic-names-are-authentically-dangerous-your-users>.

However, as institutions protect the civil rights of students to be free from unlawful harassment and true threats, they must also protect students' right to free speech, including, in the words of the U.S. Supreme Court, "insulting, and even outrageous, speech."⁶

Categorical and prophylactic rules restraining all anonymous speech, on the grounds that a subset of such future speech may be harassment or threats depending on a particular context, would be unconstitutional. But institutions can and should apply the law of harassment to particular facts on a case-by-case basis.

Empowering campus officials to strip digital anonymity tools from students could jeopardize current political movements seeking racial and gender equality.

The Coalition Letter's request for the Department to promulgate new rules that require university and college officials to block or restrict access to certain digital tools that provide users with anonymity would be counterproductive to protecting civil rights on campus. It would disempower the very groups the policies are designed to protect by limiting their ability to speak anonymously. Anonymous speech has particular value on college campuses when students seek to advance controversial or unpopular views or otherwise avoid being the targets of threats or harassment.

Allowing educational institutions to unilaterally block certain online platforms would deprive marginalized communities of essential digital tools to organize politically and advocate for change. Time and again, in the face of outright censorship or efforts to crack down on free expression, online platforms have proven invaluable for helping groups around the world meet, exchange ideas, and demand political change in ways that are sometimes impossible to do offline. For example, after the elections in Iran in 2009, online platforms were essential to activists and journalists seeking to document state-sponsored violence and censorship.⁷ The ability to protect the identity of participants has been one of the key benefits of such technology that has allowed such conversations and activism to take place.⁸

At the University of Southern California, an anonymous group of students who identify themselves as the USC Girl Mafia use Twitter to map locations of assaults on campus

⁶ *Boos v. Barry*, 485 U.S. 312, 322 (1988).

⁷ Hiawatha Bray, *Finding a way around Iranian censorship*, The Boston Globe (June 19, 2009), available at https://www.boston.com/business/technology/articles/2009/06/19/activists_utilizing_twitter_web_proxies_to_sidestep_iranian_censorship/.

⁸ Jillian York, *The Case for Pseudonyms*, Electronic Frontier Foundation (Jul. 29, 2011), available at <https://www.eff.org/deeplinks/2011/07/case-pseudonyms> (last visited Jan 8, 2016).

and to distribute sketches of a man suspected in several sexual assaults.⁹ Relatedly, anonymity was essential for student activists at Columbia University seeking to bring attention to what they believe was an inadequate response to a series of sexual assault allegations.¹⁰ The activists relied on anonymity out of fear of being disciplined or sued for speaking out to identify individuals who allegedly assaulted female students. Further, because some universities have punished victims of sexual violence who publicly identified themselves,¹¹ anonymity provides an important way for students to discuss their experiences and find support without exposing themselves to further contact by their attacker or campus discipline. At Guilford College, students used an online form to collect anonymous testimonials and reports of racial violence from those who felt unsafe revealing their identities through official channels.¹²

Additionally, anonymous online platforms allow groups unfairly targeted by law enforcement to engage in protected political activity without disclosing their identities to police.¹³ Most recently, law enforcement and private security have targeted the Black Lives Matter and other police reform movements, including surveilling their online activity and personal information, as well as monitoring peaceful demonstrations, vigils, and other real-world activities.¹⁴

⁹ Angie Crouch & Nancy Oy, *Anonymous College Group Fights Against Sexual Assault on Campus*, NBC4 News (April 10, 2015), available at <http://www.nbclosangeles.com/news/local/USC-Girl-Mafia-Group-Raise-Sexual-Assault-Awareness-299423751.html>.

¹⁰ George Joseph and Jon Swaine, *Behind Columbia's 'rape lists': 'When existing systems fail, what then?'*, The Guardian (June 26, 2014), available at <http://www.theguardian.com/education/2014/jun/26/columbia-university-students-rape-list-mishandle-sexual-assault>.

¹¹ Evette Dion, *A UNC Rape Victim Faces Expulsion*, Clutch Magazine (Feb. 2013), available at <http://www.clutchmagonline.com/2013/02/a-unc-rape-victim-faces-expulsion/>.

¹² Nicole Zelniker, *Student leaders create anonymous reporting form*, The Guilfordian (November 20, 2015), available at <http://www.guilfordian.com/news/2015/11/20/student-leaders-create-anonymous-reporting-form/> (last visited Jan 8, 2016).

¹³ George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, The Intercept (July 24, 2015), available at <https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/>.

¹⁴ Mick Dumke, *Chicago cops conducted unauthorized spying on protesters*, Chicago Sun-Times (Nov. 14, 2015), available at <http://chicago.suntimes.com/news/7/71/1096951/chicago-cops-conducted-unauthorized-spying-protesters>; Lee Fang, *Mall of America Security Catfished Black Lives Matter Activists*, Documents Show, The Intercept (Mar. 18, 2015), available at

There are constitutional alternatives for addressing online harassment and threats short of banning access to anonymous platforms.

There are many alternatives for responding to threats and harassment, including several suggested by the Coalition. These solutions do not require any new rules or guidance from the Department or risk violating students' First Amendment rights. They include:

- **Educating the campus community—including administrators, educators, students, and law enforcement—about what constitute true threats and unlawful harassment and appropriate methods of addressing it.**
- **Enforcing existing laws and policies surrounding true threats and unlawful harassment:** Institutions and local police already have policies and laws in place that allow them to investigate reports of true threats or harassment and to take action where appropriate. These laws and policies should be enforced to protect victims of harassment. The First Amendment is no bar to punishing particular acts of unlawful misconduct.¹⁵
- **Improving tools for targets to flag or filter unwanted content:** Targets of online threats or harassment should have the ability to flag or filter out unwanted users or particular content.¹⁶ It is the responsibility of online platforms, and not the government, to provide these tools to their users.
- **Using tools to protect online personal information:** Many forms of online harassment involve the perpetrator collecting and abusing the victim's online personal information. That is, in addition to victims being threatened or harassed directly, they are also the targets of efforts to reveal personal information or to use such information to harass individuals offline. Students and other Internet users can use tools such as

<https://theintercept.com/2015/03/18/mall-americas-intelligence-analyst-catfished-black-lives-matter-activists-collect-information/>.

¹⁵ In distinguishing between protected speech and unprotected harassment, the Department has stated:

the offensiveness of a particular expression, standing alone, is not a legally sufficient basis to establish a hostile environment under the statutes enforced by OCR. In order to establish a hostile environment, harassment must be sufficiently serious (i.e., severe, persistent or pervasive) as to limit or deny a student's ability to participate in or benefit from an educational program.

First Amendment: Dear Colleague, Department of Education (July 28, 2003), available at <http://www2.ed.gov/about/offices/list/ocr/firstamend.html> (*DOE First Amendment Guidance*).

¹⁶ *Facing the Challenge of Online Harassment*, *supra* n.2.

encryption to protect or obscure their communications and personal information so as to prevent perpetrators from outing them or using personal information found online to further harass or threaten individuals. EFF has developed a guide to help individuals understand the various threats of online surveillance and to provide tools for how they can protect themselves.¹⁷ Digital tools are part of the solution to online harassment, as they allow victims to preserve their voices when abusers try to silence them. For example, individuals operating websites can use proxy registry services to protect their personal information or remain anonymous.¹⁸ Thus, individuals can express themselves without having to disclose personal information that may be used to target them online or offline.

- **Engaging in counter-speech:** Both students and university officials can exercise their own free speech rights to condemn racist and sexist speech and acts. As the Department has previously recognized in the context of sexual harassment, “while the First Amendment may prohibit a school from restricting the right of students to express opinions about one sex that may be considered derogatory, the school can take steps to denounce those opinions and ensure that competing views are heard.”¹⁹ Students and other members of the campus community can also take steps to denounce derogatory speech. For example, in response to a racial threat on campus, high school students in Berkeley, California, recently organized a daylong assembly and curriculum to discuss racism and black culture.²⁰
- **Providing assistance to the targets of harassment or threats:** EFF agrees with the Coalition Letter that academic institutions should provide counseling and other appropriate assistance to the targets of online harassment and threats and others who are likewise affected by them.

¹⁷ See *Surveillance Self-Defense: Tips, Tools, and How-tos for Safer Online Communications*, Electronic Frontier Foundation, available at <https://ssd.eff.org/>.

¹⁸ Jeremy Malcolm and Mitch Stoltz, *Changes to Domain Name Rules Place User Privacy In Jeopardy*, Electronic Frontier Foundation (June 23, 2015), available at <https://www.eff.org/deeplinks/2015/06/changes-domain-name-rules-place-user-privacy-jeopardy>.

¹⁹ *Revised Sexual Harassment Guidance: Harassment by School Employees, Other Students, or Third Parties*, Department of Education (Jan. 19, 2001), available at <http://www2.ed.gov/about/offices/list/ocr/docs/shguide.html#XI>

²⁰ Jill Tucker, *Berkeley High’s extraordinary response to ‘lynching’ threat*, San Francisco Chronicle (Dec. 9, 2015), available at <http://www.sfchronicle.com/bayarea/article/Berkeley-High-s-extraordinary-response-to-6687648.php>.

Proposals to prevent access to online anonymous speech platforms are unconstitutional.

If required or encouraged by the Department, the proposed censoring of communications platforms would violate students' First Amendment rights²¹ in several respects, including:

- **Curtailing anonymous speech online:** A school cannot place blanket restrictions on students that substantially burden their right to speak anonymously. Anonymous online communication is critical, given our nation's history of government entities trying to silence unpopular organizations by exposing the identities of their members and supporters.²² "Anonymity is a shield from the tyranny of the majority," according to the U.S. Supreme Court.²³ Indeed, our founders relied on anonymity when creating the Constitution.²⁴ Moreover, as courts have explained: "Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas. The ability to speak one's mind on the Internet without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate."²⁵

²¹ Decades of well-settled law and the Department's own guidance demonstrate that institutions can police harassment and threats without violating the First Amendment. *See, e.g., Davis v. Monroe Bd. of Educ.*, 526 U.S. 629 (1999); *Saxe v. State Coll. Area Sch. Dist.*, 240 F.3d 200 (3rd Cir. 2001) (harassment must be "so severe, pervasive, and objectively offensive, that it can be said to deprive victims of access to the educational opportunities or benefits provided by the school"). The Department has stated that harassment (1) "must include something beyond the mere expression of views, words, symbols or thoughts that some person finds offensive," (2) must be "sufficiently serious to deny or limit a student's ability to participate in or benefit from the educational program," and (3) is evaluated "from the perspective of a reasonable person in the alleged victim's position, considering all the circumstances." *DOE First Amendment Guidance*. In some cases, words alone can comprise harassment that is unprotected by the First Amendment. *See, e.g., Jackson v. Quanex Corp.*, 191 F.3d 647, 662 (6th Cir. 1999).

²² The First Amendment protects the rights of individuals to anonymously associate with political organizations. *NAACP v. Alabama*, 357 U.S. 449 (1958). Striking down a state's efforts to seize the NAACP's membership list, the Supreme Court explained: "revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *Id.* at 462. The First Amendment also protects anonymous pamphleteering. *Talley v. California*, 362 U.S. 60, 64-65 (1960).

²³ *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995).

²⁴ *Talley*, 362 U.S. at 64-65 (discussing publication of the Federalist Papers by founders using fictitious names).

²⁵ *Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001).

- **Interfering with students' speech, assembly, and petition rights:** Banning access to online platforms would greatly limit the tools students can use to speak, organize, and demonstrate in support of or against any number of political and social causes. Online platforms play an integral role in modern social justice and political movements, allowing people to communicate and organize in ways that are faster and more powerful than offline alternatives. That is why authoritarian regimes that lack strong free speech protections often seek to shut down Internet access or block such platforms.²⁶ Those efforts are less common in the United States, because governmental efforts to shut down or block communication systems, such as the Bay Area Regional Transit's (BART's) shuttering of its cellular network in to hinder protests, are roundly regarded as an unconstitutional interference with people's ability to communicate and organize.²⁷
- **Inhibiting the right to gather and receive information:** Commensurate with students' right to speak anonymously, students also have the First Amendment right to gather and to receive information via online platforms.²⁸ By excluding anonymous speech in such platforms, schools would unconstitutionally prevent some students from obtaining information from other students who will only express certain criticisms of the status quo using anonymous online platforms.
- **Prior restraints on speech:** Preventing users on campus networks from accessing or using particular online platforms would also be an unconstitutional prior restraint. A prior restraint occurs when a censor bars a party's First Amendment rights in anticipation that the speech will result in some future harm.²⁹ A prior restraint is "the most serious and the least tolerable infringement on First Amendment rights" and thus bears a heavy presumption that it is unconstitutional.³⁰ Preventing or interfering

²⁶ Christopher Rhoads & Geoffrey A. Fowler, *Egypt Shuts Down Internet, Cellphone Services*, *The Wall Street Journal* (Jan. 29, 2011), available at <http://www.wsj.com/articles/SB10001424052748703956604576110453371369740>.

²⁷ Eva Galperin, *BART Pulls a Mubarak in San Francisco*, *Electronic Frontier Foundation* (Aug. 12, 2011), available at <https://www.eff.org/deeplinks/2011/08/bart-pulls-mubarak-san-francisco>.

²⁸ See *Bd. of Educ. v. Pico*, 457 U.S. 853, 867 (1982) (plurality) (noting that the "right to receive ideas is a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press, and political freedom") (emphasis in original); *Richmond Newspapers v. Virginia*, 448 U.S. 555, 576 (1980) (plurality) (observing that without the right to gather information, the First Amendment's guarantees "would be eviscerated"); *Virginia v. American Booksellers Ass'n, Inc.*, 484 U.S. 383, 389 (1988) (challenging law that restricted adult's abilities to access books).

²⁹ *Alexander v. U.S.*, 509 U.S. 544, 550 (1993).

³⁰ *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976); *New York Times Co. v. United States*, 403 U.S. 713, 714, 730 (1971) (Stewart, J. joined by White, J., concurring).

with the use of anonymous online platforms based solely on future potential harassment or threats would not satisfy the exacting scrutiny required to impose a prior restraint. Moreover, for a prior restraint to survive First Amendment scrutiny, it must actually be effective in preventing the harm at which it is targeted.³¹ As described below, the proposed blocking of certain platforms will not work.

- **Facial overbreadth:** The First Amendment prevents regulations that proscribe unprotected speech from sweeping up broad amounts of protected speech.³² Thus, for example, if a college restricted anonymous online communications about controversial issues like race and gender, that policy would be overbroad, as well as an unlawful content-based restriction.³³

Even if such measures were constitutional, they are neither technologically feasible nor sound policy.

Even if they were constitutionally permissible and not detrimental to valuable political speech, the Coalition's proposal to block access to certain communications platforms by restricting campus Wi-Fi or requiring geo-fencing of particular platforms has another fundamental flaw: they would not actually prevent online harassment and threats. As explained below, technical restrictions on accessing online platforms will not prevent individuals from accessing anonymous platforms on campus. Thus the proposed technical solutions may do more harm than good by leading some campus administrators to believe that they have addressed concerns about online harassment with a technical quick fix when the problems require more complex responses.

With respect to Wi-Fi blocking, although a university has the technical ability to block particular websites or applications from being accessed on the university's own network, students can easily work around such measures. First, students could simply switch their smartphones or other devices to cellular networks, bypassing the campus network entirely to access the blocked content. Additionally, students could still use the campus Wi-Fi to access restricted websites or applications through services that hide or anonymize their web browsing, including a Virtual Private Network (VPN) or the online anonymity service Tor.³⁴

³¹ *Nebraska Press Ass'n*, 427 U.S. at 565-67.

³² *R.A.V. v. City of St. Paul*, 505 U.S. 377 (1992).

³³ *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000). For all of the reasons described in this section, it would also be a bad idea for campus officials to actively monitor anonymous online communication platforms, as proposed by the Coalition Letter. This raises First Amendment concerns, and as such monitoring by university officials – who often will be the targets of online criticism – would chill and deter free expression on the platforms.

³⁴ EFF has written extensively about both VPNs and Tor as part of its Surveillance Self Defense Guide. See *Choosing the VPN That's Right for You*, available at <https://ssd.eff.org/en/module/choosing-vpn-thats-right-you> (last visited Dec. 11, 2015);

Regarding geo-fencing, campus officials lack the technical ability to unilaterally geo-fence particular online platforms, as only a provider of a particular service or platform can implement a geo-fence. Yik Yak, for example, provides geo-fencing around primary and secondary schools and also allows users to request a geo-fence.³⁵ Nonetheless, even if administrators were able to geo-fence particular platforms from being accessed on campus, students could still evade those technical barriers. For example, students could change their smartphone settings so it appears as though they are off campus when they are actually on campus – a practice known as location spoofing.³⁶

Moreover, to actually block anonymous online platforms, universities would have to adopt much more intrusive technical solutions, such as banning the use of VPNs or Tor on campus. That, in turn, would mean interfering with additional legitimate and constitutionally protected activity.

* * *

EFF appreciates the opportunity to address the issues raised by the Coalition Letter and to provide the Department with important context as it considers how to guide educational institutions in responding to anonymous online threats and harassment. EFF believes in the fundamental power of the Internet to provide valuable communication and organization platforms for groups with less resources or political power. At the same time, EFF recognizes that the same capabilities that make the Internet a force for positive social change can also be misused to target particular groups and individuals. EFF wants to help find solutions to the problem of online harassment and threats, though we believe the solutions should not include blocking access to anonymous Internet platforms.

Sincerely,

Corynne McSherry
EFF Legal Director

cc: Feminist Majority Foundation (first signatory of the Coalition Letter)

*See also How To: Use Tor for Windows, available at <https://ssd.eff.org/en/module/how-use-tor-windows> (last visited Dec. 11, 2015); see also Thorin Klosowski, *What Is Tor and Should I Use It?*, Liferhacker (Feb. 21, 2014), available at <http://liferhacker.com/what-is-tor-and-should-i-use-it-1527891029>.*

³⁵ Yik Yak Support: Geofence Request, available at <http://support.yikyakapp.com/>.

³⁶ Zack Whittaker, *How to spoof your geolocation on Facebook Places or Twitter*, ZDNet (Nov. 16, 2010), available at <http://www.zdnet.com/article/how-to-spoof-your-geolocation-on-facebook-places-or-twitter/?tag=content;search-results-rivers>; *Here's how to easily fake your GPS location on Android*, phoneArena (Nov. 12, 2014), available at http://www.phonearena.com/news/Heres-how-to-easily-fake-your-GPS-location-on-Android_id62775.