

ACCOUNTABILITY FOR ONLINE HATE SPEECH: WHAT ARE THE LESSONS FROM “UNMASKING” LAWS?

CHRISTOPHER WOLF[†]

INTRODUCTION

I am delighted to be part of this Symposium and honored to be included among such distinguished fellow presenters.

This topic ties together so many of my curricular and extracurricular interests, so I am especially grateful for the opportunity to speak with you. In my “day job,” I am a partner at the law firm of Hogan & Hartson, focusing on privacy law. Almost thirty years ago, I started practicing law as a generalist litigator. For many of those thirty years, I thought that for sure my tombstone would read “He died with his options open,” because my practice alternately covered a wide array of commercial litigation issues, from antitrust to zoning. Fortunately for me, I had the opportunity to handle some of the earliest Internet law cases starting in the early 1990’s, and that led to my concentration on privacy law since around 1998. Related to that is my current role as co-chair of a think tank on contemporary privacy policy issues, the Future of Privacy Forum.¹

Outside the office, there are a number of non-profits I support. At the top of the list is the Anti-Defamation League, the civil rights agency better known by its initials “ADL.” I have been an ADL activist for more than two decades. In the mid-1990’s, my involvement as a volunteer lay leader for the ADL transformed from general support of the ADL’s mission “to fight anti-Semitism and promote justice and fair treatment for all” to a focus on Internet hate speech. I founded, and still chair, the ADL’s Internet Task Force. At the ADL, our monitoring of white supremacists, Holocaust deniers, homophobes, as well as racists and bigots of all kinds, showed that while in the pre-Internet era their messages of hate largely were delivered to a relative few in clandestine rallies and in plain brown envelopes delivered through the mail, the Internet empowered them, along with the rest of society, to reach millions of people (including vulnerable children).

I. ONLINE ANONYMITY AND PRIVACY ALLOW ONLINE HATE TO FLOURISH

The Internet, in large part because of the shield of online anonymity, has become the medium through which hate groups plot and promote

[†] Partner at Hogan & Hartson LLP and Chair, Anti-Defamation League Internet Task Force.
1. <http://www.futureofprivacy.org>.

real-world violence, recruit and indoctrinate like-minded haters, and mislead and distort information for those—like students—who innocently link to their content. There are, of course, notorious hate mongers who use their real identities and revel in the limelight. But the vast majority of hate spewed online is done so anonymously. The Internet content of hate mongers—words, videos, music, and social network postings—serve to offend the human dignity of the intended victims, minorities, and those who hate groups identify as “the other.” The Chief Commissioner of the Canadian Human Rights Commission, Jennifer Lynch, recently commented: “Freedom of expression is a fundamental right . . . [s]o is the right to be treated with equality, dignity and respect.”² The balance between free expression and the right to human dignity is way out of whack online. The Internet has become the launching pad for mean-spirited, hateful, and harmful attacks on people.

With that said, I should point out at the outset that neither the ADL nor I call for any restriction on the free speech rights of those who use the Internet for what most of society condemns as repugnant speech. The ADL and I are ardent First Amendment supporters. As this group knows, there are limits to First Amendment speech—the Nuremberg Files case³ where abortion providers were targeted on a web site for violence is a prime example—but the boundaries of the First Amendment are so wide that almost anything goes, as we know.

The Internet makes it more difficult than it used to be to follow the teachings of Justice Brandeis that “sunlight is the best disinfectant”⁴ and that counter-speech is the best antidote to hate speech. Still, a lot of what the ADL does is shine the light on hate so that the lies embedded in the prejudice can be revealed, and the ADL has a wide array of educational and other programs focusing on counter-speech. The ADL’s work to reduce and counter cyber-bullying is a great and current example.

An outgrowth of my ADL participation is my involvement with the International Network Against Cyber-Hate or “INACH,”⁵ a non-governmental organization based in Amsterdam. For several years I served as chair of INACH, which is an umbrella group of civil rights groups around the world concerned about Internet hate. Of course, in countries without the First Amendment—that is, everywhere else in the world—the restrictions on legislating speech are not nearly as robust as here in the United States. In many parts of Europe, for example, it is a

2. Jennifer Lynch, *Hate Speech: This Debate is Out of Balance*, THE GLOBE AND MAIL, available at <http://www.theglobeandmail.com/news/opinions/hate-speech-this-debate-is-out-of-balance/article1178149>.

3. *Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coalition of Life Activists*, 290 F.3d 1058 (9th Cir. 2002) (en banc), cert. denied, 123 S. Ct. 2637 (2003).

4. Louis Dembitz Brandeis, *What Publicity Can Do*, *Other People’s Money*, ch. 5, p. 92 (1932).

5. <http://www.inach.net>.

crime to deny the Holocaust or display Nazi symbols. So my fellow members of INACH often take issue with my American version of free speech. At a conference on Internet hate speech in Paris hosted by the Government of France, a former Minister of Justice shouted in my direction, “Stop hiding behind the First Amendment.”⁶ But, as I responded then, with a borderless Internet, and the ability of many from around the world to launch their hate speech from the U.S., the rest of the world has to deal with the First Amendment in crafting strategies to counter hate speech.

II. ACCOUNTABILITY FOR ONLINE HATE SPEECH: WHAT ARE THE LESSONS FROM “UNMASKING” LAWS?

There is no question that people take advantage of the privacy that online anonymity gives them to say and post and distribute hate-filled content that they most likely would not do if personal identity and accountability were required. The comments posted every day to news articles on mainstream newspaper sites demonstrate what I mean. In the wake of the Bernie Madoff scandal, the anti-Semitic rantings posted in comments to news articles got so bad that the *Palm Beach Post* shut down the comment function.⁷ And in the world of cyber-bullying, as bad as playground taunts might be, they pale in comparison to the online harassment launched anonymously from computers. The risks of being identified to a teacher or parent are far less online than in the schoolyard.

And that shield of anonymity is exponentially greater when we talk about general online interactions, from maintaining websites, to blogging, to posting comments to mainstream news sites. In that regard, just imagine if ICANN ever moves to an anonymous WHOIS registration scheme for domain names, as has been proposed. Domain hosts thus far have been identifiable and accountable because they can more easily be identified through published registration information required for registration of a domain name. Shielding from public view the names of registrants is a decidedly bad idea for a range of reasons too long to address here today. At the top of the list is a loss of accountability.

A. *Legal Tools to Identify Online Wrongdoers*

So, let me now turn to a couple of identification schemes familiar to some of us, to frame the discussion on whether there are legal tools to identify online hate-mongers.

6. See Christopher Wolf, *A Comment on Private Harms in the Cyber-World*, 62 WASH. & LEE L. REV. 355, 361 (2005).

7. John Lantigue, *Madoff Scandal Spurs Anti-Semitic Postings on Web*, PALM BEACH POST, December 28, 2008, available at http://www.palmbeachpost.com/search/content/nation/epaper/2008/12/18/a1b_madoffweb_1219.html.

In the world of online copyright infringement, the identification of anonymous online wrongdoers is not a revolutionary concept. Under the Digital Millennium Copyright Act or DMCA, even without filing a lawsuit, a copyright owner can obtain a subpoena directed to a service provider to identify alleged infringers of copyrighted material.⁸ The subpoena authorizes online service providers, like ISPs and colleges and universities, to expeditiously disclose to the copyright owner information sufficient to identify alleged infringers. That identification right only applies to users *hosting* content through an online service and not those who, as is far more common, use peer-to-peer networks to upload and download.

Recall the controversial case a few years back in which Verizon Wireless won its argument in the D.C. Circuit that the Recording Industry Association of America could not use the expeditious subpoena provisions of the DMCA with respect to peer-to-peer infringers but could only use it for materials actually hosted on Verizon's Internet service.⁹ As a result, the RIAA and other content owners are forced to file John Doe lawsuits and then seek discovery as to the identity of the John Does using peer-to-peer technology to illegally download copyrighted material. Fortunately for the content owners, we have witnessed some cooperation from ISPs and colleges and universities to send notices of infringement to infringers that the content owners would not be able to identify on their own. Around the world, and perhaps soon in the US, new schemes of graduated enforcement against online piracy are emerging whereby user privacy is preserved but the copyright laws are enforced.

Turning from copyright to defamation, Section 230 of the Communications Decency Act (CDA) is the federal statute that shields websites from lawsuits arising out of third-party content and communications online.¹⁰ The scope of Section 230's immunity for online services is extraordinarily broad. Still, dozens of lawsuits have been brought in state and federal courts concerning the CDA's immunity provisions, seeking to chip away at the breadth of the immunity and to hold online companies responsible for content posted by third parties. The reason there is so much litigation seeking to strip online services of immunity for the speech of others is that those *others*, cloaked in anonymity are so hard to find, and when found, likely do not have deep pockets to satisfy a hoped-for judgment.

Plaintiffs seeking redress for online defamation, for the most part, have to identify and track down the person responsible for posting the

8. 17 U.S.C. § 512(h) (2007).

9. Recording Indus. Assoc. of Am. v. Verizon Internet Servs., 351 F.3d 1229, Case No. 03-7015 (D.C. Cir. 2003) *cert denied* 125 S. Ct. 309 (2004).

10. 47 U.S.C. § 230 (2007).

content, and there has been significant litigation over the standards to be used in evaluating a request to unmask someone accused of online defamation or other tortuous wrongdoing.

I remember the day not so long ago when a lawyer using a pre-litigation discovery tool such as that available in New York¹¹ could simply ask for a subpoena with little in the way of a showing of need, and get the requested subpoena. But then online liberty groups such as the Electronic Frontier Foundation and others monitored the dockets, got involved, and pushed for a high threshold standard for disclosure.

A trend is emerging whereby the standards articulated in *Dendrite Int'l, Inc. v. John Doe No. 3*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001) are becoming the common requirements. Under *Dendrite*, a trial court confronted with a defamation action in which anonymous speakers or pseudonyms are involved and a subpoena is sought to unmask the alleged wrongdoer, should (1) make a reasonable attempt to notify the person, (2) give that person a reasonable time to respond, (3) identify the allegedly defamatory statements, (4) make a substantial showing of proof on each element of the claim, and if the plaintiff satisfies these four requirements, a judge must (5) balance First Amendment interests.

This balancing test with respect to issuing and enforcing a subpoena to unmask someone accused of online defamation is generally viewed as more protective of privacy – of shielding the identity of those online accused of wrongdoing. Yet, the application of the standard has resulted in orders going both ways, with a recent uptick in orders requiring the disclosure of the alleged wrongdoers. In his presentation today, Professor Grimmelman provides a compelling analysis of the competing interests in disclosure where an actual legal right has been invaded.

An opinion piece recently appeared in the *Cleveland Plain Dealer* on the heels of a New York state court order requiring Google to turn over the identity of a blogger accused of defamation. The opinion piece was authored by the founder of a social networking company, J.R. Johnson. In the piece,¹² Mr. Johnson concluded we are witnessing what he saw as a powerful shift away from anonymity online and toward accountability. To support his conclusion that online people are supporting accountability, he cited the New York state court case where the judge ordered Google, which owned the blogging software at issue, to turn over the e-mail address of an anonymous blogger because the judge determined that content on the blog may be defamatory. The blogger turned

11. N.Y. C.P.L.R. 3102(c) 2008.

12. J.R. Johnson, *Accountability's Hot and Anonymity's Not*, CLEVELAND PLAIN DEALER, September 14, 2009, available at http://www.cleveland.com/opinion/index.ssf/2009/09/accountabilitys_hot_anonymitys.html.

around and sued Google for millions of dollars for not protecting anonymity.¹³

Johnson observed: "In the past, most online comments posted in response to a case like this typically defend anonymity. Often, the commenters themselves are anonymous and obviously sympathize with anyone being forcibly unmasked."

The comments with respect to the Google blogger case highlighted what Johnson believed to represent a shift in overall tone and opinion regarding anonymity. One comment said, "OK, let's get this straight. A blogger using a free media service defames someone while hiding behind anonymity and then when she is charged with having to take responsibility for making such defaming statements sues the media service for her having to do so. Anyone else feel sick?" Another boiled it down simply, "I'm glad this Blogger's identity was revealed. Trashing someone else and hiding behind anonymity is cowardly."

Johnson added his own views:

For too long, we have accepted the idea that the Internet is the supposed "Wild West" communication medium where people say whatever they want without consequence. Granted, there are valid and important reasons for having some degree of anonymous contribution, such as whistle-blowing and political expression. However, with the propensity for anonymous contribution to be so negative and hateful, we have also suffered an untold loss as a result.

Most online contribution is from a very small minority of people. Studies report anywhere from 1 percent to 20 percent of the online population is actually contributing; I'll just use 10 percent. If we are getting contributions from such a small but vocal minority, we are losing out on what 90 percent of the online population has to say.

One of the roadblocks to getting the other 90 percent to contribute has been the negative culture that has been acceptable online. But, with this recent shift toward accountability, we finally stand to benefit from the ocean of untapped potential that lies in those who may now feel more welcome to participate in a more evolved online community.

. . . More people will contribute, increasing not only the quality of what's written online but, in turn, our mutual understanding of one another. More understanding begets more tolerance and a more thoughtful society as a whole.

13. See Chris Matyszczyk, Outed "Skanks in NYC" Blogger to Sue Google, CNET NEWS, Aug. 24, 2009, available at http://news.cnet.com/8301-17852_3-10315998-71.html.

The columnist, Mr. Johnson, was talking about online defamation and unmasking the perpetrator, but he could just as easily have been talking about online hate speech.

But, obviously, the dispositive difference between identifying online infringers and online defamers, and identifying those engaged in online hate speech is that the former category involves “speech” which is not protected by the First Amendment. There is no legal vehicle to seek the identity of an online proponent of hate and intolerance except in a distinct minority of cases where hate speech crosses the line into unprotected territory, such as direct threats addressed to identify individuals, or someone identifies the host of a web site through the WHOIS registry. The First Amendment gives license to remaining anonymous. No court will issue a subpoena to unmask people “merely” engaged in hate speech.

But what about a law that provides that while there are no legal consequences for most hate speech, people should be required to be identified, to be held accountable in society, just as they might be in the offline world?

B. KKK Unmasking Laws

More than 18 states and localities have over the years passed “anti-masking” laws that make it a crime to wear a mask in public. Most of the laws were passed in response to activities of the Ku Klux Klan.

New York City Corporation Counsel and my former law partner Michael Cardozo argued in 2004 to the Second Circuit with respect to a New York City anti-masking ordinance that “New York’s anti-mask law was . . . indisputably aimed at deterring violence and facilitating the apprehension of wrongdoers . . . [and that] the statute was not enacted to suppress any particular viewpoint.”¹⁴ The Second Circuit agreed with Mr. Cardozo in that case and found that the mask “does not communicate any message that the robe and hood do not” and its expressive force was therefore “redundant.”¹⁵

It was believed at the time of the Second Circuit ruling that the interest of police in maintaining the law included new concerns over the role that masks might play in a post-9/11 New York City, where security concerns in public gatherings and demonstrations expanded.

Even with that recent outcome in the Second Circuit, there are First Amendment issues at stake with anti-masking statutes beyond the expressive speech issues. In a series of cases, the Supreme Court has made it clear citizens have the right to communicate and associate any-

14. <http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005541417>

15. *Ku Klux Klan v. Kerik*, 356 F.3d 197 (2d Cir. 2004).

mously, without fear of harassment or reprisals by others who oppose their views.

For example, the 1958 Supreme Court case *NAACP v. Alabama*¹⁶ made it clear the government cannot require groups to reveal members' names and addresses unless public officials have a compelling need for the information and no alternative means of obtaining it.

And, as the Supreme Court pointed out in *McIntyre v. Ohio Elections Commission*,¹⁷ a 1995 case striking down an ordinance prohibiting the anonymous distribution of political leaflets: "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society."

Notwithstanding this Supreme Court precedent, the Second Circuit upheld the New York City anti-masking ordinance, and Georgia's highest court ruled in 1990 however the state's anti-masking law was enacted to protect the public from intimidation and violence and to aid law enforcement officials in apprehending criminals, and these purposes far outweighed the Klan's right to associate anonymously.

Unlike the laws on disclosing member lists struck down by the U.S. Supreme Court, the Georgia court concluded the anti-masking laws do not require the Klan to reveal the names and addresses of its members, nor do they stop Klan members from meeting secretly or wearing their hoods on private property. The anti-masking law, in the words of the court, "only prevents masked appearance in public under circumstances that give rise to a reasonable apprehension of intimidation, threats or impending violence."¹⁸

C. *Unmasking Laws as a Model for Fighting Online Hate?*

Some have suggested the KKK anti-masking laws might serve as models for a law requiring online identification of those who engage in hate speech. For example, last year a Kentucky legislator proposed a ban on the posting of anonymous messages online.¹⁹ The proposed law would have required users to register their true name and address before contributing to any discussion forum. The stated goal was the eliminator of "online bullying."

16. 357 U.S. 449 (1958).

17. 514 U.S. 334 (1995).

18. *State v. Miller*, 260 Ga. 669 (1990).

19. Posting of purefopperty to Harvard Law's The Web Difference Blog, <http://blogs.law.harvard.edu/webdifference/2008/03/17/kentucky-to-ban-online-anonymity/> (Mar. 17, 2008 12:33 PM).

The apparent impetus of the Kentucky bill was the growing popularity of the now defunct JuicyCampus.com, a “Web 2.0 website focusing on gossip” where college students post lurid—and often fabricated—tales of fellow students’ sexual encounters. The website billed itself as a home for “anonymous free speech on college campuses,” and used anonymous IP cloaking techniques to shield users’ identities.

There are a host of problems with the proposed Kentucky law, which presumably is why it made little progress in the legislature. Similar proposals requiring online identification would face similar hurdles.

First, a broad prohibition on anonymous speech (which is essentially what the law would create) surely would run afoul of the Supreme Court’s views on the right to remain anonymous set forth in *McIntyre*. Second, the requirement that real names be used implicates *NAACP v. Alabama* as it would effectively be state law-ordered identification of a person’s views and affiliations. Third, any attempt to define a more limited category of speech for which accountability is required would face First Amendment problems. Most hate speech, no matter how objectionable, is permitted under the First Amendment and defining what is in or out of bounds is nearly impossible in the abstract. Third, enforcement in this technological work-around age likely would be futile. Finally, the same laws designed to deter online defamation and harassment can also be used to target political dissent or silence whistleblowers for whom the option of remaining anonymous is critical. China requires real-name registration for a range on online activity precisely because of its chilling effects. Thus the KKK anti-masking laws must be viewed as *sui generis*, not easily imported online.

III. PRIVACY AND ACCOUNTABILITY: THE LIMITED ROLE OF LAW AND THE ROLE OF THE ONLINE COMMUNITY

In a recent speech, FTC Consumer Protection Head David Vladeck quoted science-fiction writer David Brin who said, “when it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else.”²⁰ Professor Anita Allen wrote in her book *Why Privacy Isn’t Everything* “although privacy is important, accountability is important too. Both in their own way render us more fit for valued forms of social participation.” Professor Allen and David Vladeck both advocate for privacy and accountability. Which virtue wins their advocacy depends on the circumstances.

I also advocate for both privacy and accountability. And that is why at conferences on hate speech around the world in which I have participated, I have said it is frustrating as a lawyer not to be able to come up

20. David C. Vladeck, Director, FTC Bureau of Consumer Protection, Promoting Consumer Privacy: Accountability and Transparency in the Modern World at New York University (Oct. 2, 2009) available at <http://www.ftc.gov/speeches/vladeck/091002nyu.pdf>.

with a legal solution to the problem of hate speech that often prompts people to exclaim: "There oughta be a law." The laws protecting privacy, including principally the First Amendment, overwhelm our ability to craft laws on accountability.

The law is a tool that can be held in reserve for the clearly-egregious cases, but we have seen the untoward consequences of stretching the law to cover hate speech—such as contorting the Computer Fraud and Abuse Act to prosecute Lori Drew, the woman who pretended to be a 13 year old boy on MySpace and whose taunts caused a young girl, Megan Meier, to commit suicide. You will recall a federal court ultimately rejected the use of the computer law to fight online hate in that case.

And so I often end, as I do today, by turning to the online community rather than lawyers to address the problem of hate speech, and especially accountability for online hate speech.

I hope Mr. Johnson, the opinion columnist, is right—that there is a trend online towards accountability. Certainly, the use of real names on the wildly popular social networking site Facebook is perhaps changing the culture online. There is an opportunity for other online companies—who are not constrained by the First Amendment in setting rules of use for their private services—to require real names for people seeking to post content, so people know they will be held accountable for what they say or do. There will still be plenty of places online where people can hide behind the shield of anonymity, but the big players can start to change the culture.

Regardless of a requirement of real-name identification, online companies should have and enforce Terms of Use that prohibit hate speech. And users of such services should be provided with a simple procedure for communicating with providers to ensure complaints can be given and companies act on them (or reject them) in a timely fashion.

I also am curious about the effects on online discourse with the adoption of identity management tools—the tools being proposed by Microsoft and other to protect privacy and prove identity. Their global use would have users understand while they can control their privacy, the tool have obligations as well as benefits, such as accountability.

One obvious tool to promote privacy and accountability is the early and regular online education of the next generation of "digital natives," teaching them online etiquette and that even with assumed anonymity, they can be held to answer for what they do online. The "permanent record" of the Internet can hinder educational, job and social opportunities and kids need to better understand that. And when they do, maybe they will constrain the base instinct to engage in bullying and, later in life, hate speech.

CONCLUSION

There are many extra-legal opportunities for the online community to take action that will serve to diminish online hate. My remarks here are intended to start the discussion of what might be done by private actors online to create a culture of online accountability, and I hope that I have stimulated some thinking and new ideas. I look forward to continuing the discussion. Again, many thanks to the University of Denver for hosting me at this Symposium.