Anonymous Online Comments: The Law and Best Media Practices from Around the World

October 2014

International Press Institute

Anonymous Online Comments:
The Law and Best Media Practices from Around the World

By Kyle A. Heatherly,[*] Anthony L. Fargo,[**] and Jason A. Martin[***]

Introduction

It may seem odd that news organizations, which generally embrace or demand transparency, also often champion a right to publish stories based on anonymous sources or sponsor websites that allow readers to comment on stories anonymously or through assumed names. But journalists know that some stories that the public should see could not be published if the sources had to give their real names because of the wreckage the sources could face in their careers or lives. Likewise, allowing people to comment anonymously or pseudonymously opens up forums for commentary and news tips to people who may fear negative consequences from peers, employers, or government officials.

Anonymous publication has been around since biblical times, in one form or another, for a variety or reasons. A literary historian enumerated several reasons why many writers of pre-19th century British literature chose not to identify themselves: mischief, modesty, to pose as members of the opposite sex, danger, reviewing, and mockery and devilry.[1] More recently, an American scholar attempted to identify motives for speaking or publishing anonymously that were either beneficial or harmful.[2] Beneficial motives included following convention, safety, engaging in spirited rhetoric, gamesmanship, disguising class or gender, and protecting privacy.[3] Harmful motives included intimidation, insulation, concealment, and crime or fraud.[4]

The reasons for remaining anonymous vary. Likewise, the methods of being anonymous have multiplied greatly in the Internet age, as have the venues for speech. Paradoxically, it is easier to be anonymous but also easier to be unmasked online than in the offline world. One no longer has to worry that she will be seen delivering a manuscript to a publisher or spray-painting on a wall. But legal scholar Daniel Solove has noted that online, true anonymity usually is unavailable.[5] Because every computer portal to the Web has a unique Internet Protocol (IP) address that is logged every time a user visits a website, one's anonymity is nearly always traceable. Anonymizing services can help obscure or erase Internet footprints, but most people do not take advantage of such services, which also are not fool-proof.[6]

---

[*] Ph.D. student, The Media School, Indiana University, Bloomington, USA.
[**] Associate Professor and Director, Center for International Media Law and Policy Studies, Department of Journalism, The Media School, Indiana University, Bloomington, USA.
[***] Assistant Professor, College of Communication, DePaul University, Chicago, Illinois, USA.
[1] JOHN MULLAN, ANONYMITY: A SECRET HISTORY OF ENGLISH LITERATURE (2007).
[2] Victoria Smith Ekstrand, *The Many Masks of Anon: Anonymity As Cultural Practice and Reflections in Case Law,* 18 J. TECH. L. & POL'Y 1 (2013).
[3] *Id.* at 7-21.
[4] *Id.* at 23-29.
[5] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 146-47 (2007).
[6] *Id.* at 147.

We are left with a situation in which people who may have good reasons for wishing to communicate anonymously can do so on a dizzying array of websites but with less safety than they suspect they have. At the same time, those who use their anonymity for nefarious reasons, including theft of copyrighted material or to falsely defame others, are often hard to unmask, at least initially, because they are not seen or heard outside of the Internet's realm. The challenge for legal and media institutions is to find some way to balance protection for speakers whose anonymous comments have social merit with the need to allow persons or governments to seek justice against those whose anonymity cloaks illegal or truly injurious behavior.

The purpose of this report is twofold: First, to provide an overview of the various legal and regulatory approaches that nations have taken to recognize communication anonymity as a right and how legislatures and courts have tried to balance the right with important opposing interests. Second, the report will examine how various news organizations around the world have developed policies to deal with anonymous comments on their websites. As noted above, news organizations often support the right of persons to comment or provide information directly to journalists anonymously, but they also recognize that such comments can be harmful or simply false in ways that conflict with their missions to provide truthful information.

Because there appears to be a consensus that people should not be allowed to use anonymity to mask criminal activity, the report will focus on the more contentious area of how to balance freedom of expression about governmental or social issues with the desire of governments or persons who believe they were defamed to bring the speakers to justice.[7]

Part I: The Law

It is not surprising that the nations with the most restrictive press freedom policies also are more likely to have restrictive policies toward communicating anonymously. What may be surprising is the wide variety of approaches and policies toward anonymity and unmasking online speakers in the countries generally identified as democratically governed.

International human rights agreements dealing with freedom of expression, protection of privacy, and freedom of association do not mention anonymity specifically as a right, although it could be argued that it is implied. The United Nations' Universal Declaration of Human Rights states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[8] The Declaration also states that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[9] The Declaration also states that "[e]veryone has the right to freedom of peaceful assembly and association" and "[n]o one may be compelled to

[7] The authors have used primary sources where possible, but in cases in which primary materials, such as statutes, court decisions, and official policies, were not available in English, secondary sources such as media accounts have been used.

[8] U.N. UNIV'L. DECLARATION HUM. RTS. ART. 12 (2013).

[9] U.N. UNIV'L. DECLARATION HUM. RTS. ART. 19 (2013).

belong to an association."[10] The U.N. Human Rights Committee's International Covenant on Civil and Political Rights,[11] the European Convention on Human Rights' Convention for the Protection of Human Rights and Fundamental Freedoms,[12] and the Inter-American Commission on Human Rights' American Convention on Human Rights[13] contain similar language. The African Union's African (Banjul) Charter on Human and Peoples' Rights guarantees rights to receive information, express opinions, associate freely, and assemble with others lawfully, but it does not mention a right to privacy.[14]

One legal scholar has suggested that the International Covenant on Civil and Political Rights already protects anonymous speech indirectly.[15] Article 19(2) states that "[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[16] Because anonymity "is critically important for ensuring freedom of expression," by allowing people to express themselves on controversial issues without fear, its protection is implied by Article 19(2).[17] So far, however, no international tribunal has followed that logic to the same conclusion.

National constitutions also rarely use the word "anonymous" or a synonym specifically. The Swedish constitution grants near-total anonymity for personal freedom of expression, with limited exceptions.[18] The constitution of Brazil guarantees freedom of expression but, in the same section, forbids anonymity.[19]

Courts in some nations have interpreted their constitutions as guaranteeing at least a limited right to speak and publish anonymously. In 2012, the South Korean Constitutional Court struck down a law passed in 2007 that required Internet users to verify their identities when they posted online comments.[20] The court said that the regulation violated free speech rights because anonymous comments allowed people to express unpopular views without fear, and the regulation could chill such speech.[21]

In Israel, the Supreme Court in 2010 found no established judicial process for determining whether and how Internet service providers (ISPs) should reveal identities in legal proceedings. The court stated that any motion seeking to reveal the identities of Internet users should be dismissed until the issue was addressed through legislation.[22] In

---

[10] U.N. UNIV'L. DECLARATION HUM. RTS. ART. 20 (2013).
[11] U.N. HUM. RTS. COMM. INT'L COVENANT CIV. & POL. RTS. ARTS. 17, 19, 21, & 22 (2013).
[12] EUR. CONVENTION HUM. RTS. ARTS. 8, 10, & 11 (2013).
[13] AMER. CONVENTION HUM. RTS. CH. II, ARTS. 11, 13, 15, & 16 (2013).
[14] AFR. (BANJUL) CHARTER ON HUM. AND PEOPLES' RTS., ARTS. 9-11 (2013).
[15] Molly Land, *Toward an International Law of the Internet,* 54 HARV. INT'L L. J. 393 (2013).
[16] INT. COVENANT CIV. & POL. RTS. ART. 19 (2) (2014).
[17] Land, *supra* note 15, at 433.
[18] REGERINGSFORMEN [RF] [CONSTITUTION] 2:1-12 (Swed.).
[19] "[M]anifestation of thought is free, but anonymity is forbidden." CONSTITUIÇÃO FEDERAL [C.F.] [CONSTITUTION] art. 5 § IV (Braz.).
[20] Choe Sang-Hun, *South Korean Court Rejects Online Name Verification Law,* N.Y. TIMES, Aug. 24, 2012, at A8.
[21] Constitutional Court [Const. Ct.], 2010Hun-Ma47&252 (consol.), Aug. 23, 2012 (S. Kor.).
[22] Civ. App. 4447/07 Rami Mor v. Barak E.T.C. 1(2) [Sup. Ct., March 25, 2010] (Isr.). (An Israeli health care practitioner sued an Israeli ISP to unmask an anonymous blogger who allegedly defamed him. The Supreme Court ruled that the blogger was entitled to anonymity and dismissed the petition.)

effect, the decision granted a constitutional right to unconditional anonymity to anyone on the Israeli Internet until statutorily prohibited.[23]

In the United States, the Supreme Court has interpreted the First Amendment[24] to the U.S. Constitution as providing protection from government interference with anonymous association with others and anonymous expression. Starting in the late 1950s, the court determined in a series of cases that the National Association for the Advancement of Colored People, a civil rights organization heavily involved in the then-nascent struggle to obtain equal protection for African-Americans' rights, did not have to reveal its membership lists to state and local authorities.[25] The concern was that the threat of exposure would force many members to abandon the controversial organization to avoid economic and possibly physical reprisals from white citizens.

Beginning in 1960, the court also stated in a series of cases that U.S. citizens had a right to be anonymous tied to protection of freedom of speech and the press.[26] The general idea expressed in the decisions was that speech on controversial issues could be chilled if people were forced to identify themselves as the speakers. But the Court also has upheld laws requiring that people or corporations disclose their identities in certain situations, such as when they have signed petitions to place referendum issues on election ballots or donated money to a candidate.[27]

In other parts of the world, the right to be anonymous is often connected to a right to privacy. This is especially true in Europe, where the European Union legislative and judicial bodies have been increasingly aggressive in protecting the privacy rights of Internet users, including the right to protect one's identity. In May 2014, the European Court of Justice ruled that Google would have to honor at least some requests from persons who wished to erase links to outdated information about them, even if the information was true.[28] Experts have raised some doubts about whether such a "right to be forgotten" can be enforced,[29] but the decision clearly reflects recent EU thinking on the subject. The European Parliament voted in 2013 to require companies to protect the

---

[23] *Israel Cannot Reveal Identity of an Anonymous Surfer*, LAW.CO.IL (March 26, 2010), http://law.co.il/news/free-speech/2010/03/26/first-john-doe-ruling-of-israeli-supreme-court/.

[24] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. AMEND I.

[25] *See* Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (1963); Louisiana ex. rel. Gremillion v. NAACP, 366 U.S. 293 (1961); Bates v. City of Little Rock, 361 U.S. 516 (1960); NAACP v. Alabama ex. rel. Patterson, 357 U.S. 449 (1958).

[26] Watchtower Bible and Tract Society v. Village of Stratton, 536 U.S. 150 (2002); McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960).

[27] *See, e.g.,* Citizens United v. Federal Election Commission, 558 U.S. 310, 366-71 (2010) (upholding disclaimer and disclosure requirements for corporations sponsoring advertising or other speech favoring or opposing a political candidate).

[28] Google Spain SL v. Agencia Española de Protección de Datos, ECJ, Case No. C-131/12 (May 13, 2014).

[29] Charles Arthur, *Explaining the "Right to be Forgotten" – the Newest Cultural Shibboleth,* GUARDIAN, May 14, 2014, available at http://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth.

anonymity of users' personal data,[30] and EU commissioners also agreed to support regulations that would require Internet companies to disclose with whom they shared users' personal information.[31]

In late 2013, the European Court of Human Rights determined that Estonia's courts had not violated the free-expression rights of a news website, Delfi, when they held it responsible for defamatory comments posted by anonymous users.[32] Delfi had argued that it used filtering software to catch offensive comments and had a policy of removing comments in response to complaints, but the court said those measures were not enough to protect the defamed man, whose reputation was among his privacy-related interests.[33] The court also said that it agreed with Estonian courts that forcing the defamed man to seek out and sue the people who posted the comments would be too burdensome.[34]

The position of ISPs and other interactive computer service providers in relation to litigation or prosecution over defamatory or privacy-invading material is perhaps the leading controversy in regard to online anonymity now. It is one thing to say that people have a right to communicate anonymously or protect their personal data. It is another to say that this right requires either that an ISP protects to the fullest extent its users' identities and data or that it gives up that information without a fight when asked by authorities.

In the United States, Congress decided in 1996 to protect the developing Internet by giving ISPs and other interactive computer service providers wide immunity from legal liability for users' actions.[35] This definition of ISPs as non-publishers relieves them of legal responsibility for their users' actions but does not necessarily free them from being subpoenaed to identify their users by IP address or registration information. Litigation concerning when and under what circumstances an ISP must comply with a subpoena to identify a user has been plentiful in the United States, but no clear consensus has developed about the proper way to balance the various competing interests. Courts in the fifty states and at the federal level have struggled with such issues as whether some speech is "high value" (about political and social issues) or "low value" (sharing copyrighted material without permission).[36]

In regard to high-value speech, U.S. courts have recognized that some attempts to unmask users are not designed to defend a falsely maligned reputation or protect a privacy interest, but to make it easier to improperly punish someone for stating an opinion that the potential plaintiff disagrees with. The most popular methods for

---

[30] Carol J. Williams, *Amid NSA Spying, European Lawmakers Vote to Tighten Data Protection*, L.A. TIMES, Oct. 21, 2013, http://articles.latimes.com/2013/oct/21/world/la-fg-wn-europe-data-protection-NSA-spying-20131021.

[31] Alan Travis, *European Commission Backs Merkel's Call for Tougher Data Protection Laws,* GUARDIAN, July 15, 2013, http://www.guardian.co.uk/world/2013/jul/15/european-commission-angela-merkel-data-protection.

[32] Delfi AS v. Estonia, [2013] ECHR 64569/09.

[33] *Id.,* ¶¶ 88-89.

[34] *Id.,* ¶ 91.

[35] Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C.S. § 230 (c) (LEXIS 2013).

[36] *See* Jason A. Martin, Mark R. Caramanica, & Anthony L. Fargo, *Anonymous Speakers and Confidential Sources: Using Shield Laws When They Overlap Online,* 16 COMM. L. & POL'Y 89 (2011).

determining whether an ISP must reveal a user's identity involve variations on a test developed by the New Jersey Superior Court Appellate Division in a 2001 case. In *Dendrite International v. Doe,*[37] the New Jersey court developed a four-part balancing test that weighs plaintiffs' interests and the rights of defendants to protect their identities from disclosure.[38] Part One requires that plaintiffs provide notice to potential defendants, through the same forums on which the disputed statements appeared, that their identities are being sought.[39] Part Two requires plaintiffs to identify exactly which statements they believe are defamatory.[40] Part Three requires the plaintiff to prove that its case could survive a motion to dismiss for lack of legal support or evidence.[41] Part Four shifts the burden to the court to balance the plaintiff's reputational interests and the defendant's First Amendment right to remain anonymous.[42]

News organizations that host forums that allow anonymous comments or allow readers to post comments on posted stories may also avail themselves of protection from subpoenas through shield laws in most U.S. states that create a presumption that information gathered by the organization is off-limits to authorities and private litigants absent an overriding need. News organizations in states with broadly written shield laws have had some success with this tactic by arguing that the identities of anonymous users are part of the "information gathered" by the news organization that is exempt from disclosure.[43]

Because of the unique constitutional protection that the United States affords to free expression through its First Amendment, as well as its highest court's decisions tying anonymity to that constitutional right, it is probably safe to say that it has the most developed law on the question of when ISPs must disclose users' identities. However, statutory and case law on the subject has been developing worldwide.

In the United Kingdom and Europe, as noted earlier, the right to anonymity is often tied to a more generalized privacy right. However, while the right to data privacy is strong, the right to publish anonymously is not as well defined, and the status of ISPs as non-parties is not as clearly defined as in the United States.

In the UK, anonymity has a long history in literature and journalism, and it may even be a right, although precedent on that point is hard to find.[44] ISPs generally are not held responsible for user-generated content, but courts usually rely on a 1973 House of Lords precedent regarding when non-party witnesses may be compelled to provide evidence. That precedent often does little to keep ISPs from being forced to disclose user data. Under the test, the party seeking the information must show that the anonymous party likely committed a wrong against the plaintiff; that it is necessary to identify the

---

[37] 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001). The court found that the company did not prove that its reputation had been harmed, so it refused to force the ISP to reveal the identity of the anonymous speaker. *Id.* at 772.
[38] *Id*. at 760.
[39] *Id.*
[40] *Id.*
[41] *Id*.
[42] *Id.* at 760-61.
[43] *See* Martin et al., *supra* note 36.
[44] Paul Bernal, *Internet Anonymity: A Very British Dilemma,* U.K. CONST. L. GROUP, Nov. 6, 2012, http://ukconstitutionallaw.org/2012/11/06/paul-bernal-internet-anonymity-a-very-british-dilemma.

unknown party; and that the third party (the ISP) is able to identify the alleged wrongdoer.[45] Although the Norwich Pharmacal test, as it is called, was developed long before the World Wide Web became widely available, courts have used the same test in cases involving online publications.[46]

In Canada, anonymity is sometimes recognized as tied to privacy interests, although there is no generalized constitutional right to privacy.[47] In cases involving whether ISPs can be forced to identify their users, Canadian courts recognize a need to balance the right to be anonymous versus opposing interests before forcing ISPs to comply with subpoenas, but no single balancing test has emerged from decisions so far. For example, in a copyright case, a court required the plaintiff to demonstrate a bona fide claim and the lack of an alternative source for the identity, then engaged in a balancing of factors for and against disclosure.[48] Different tests have been developed in defamation cases. In *Warman v. Wilkins-Fournier*,[49] the Ontario Superior Court of Justice determined that the proper test for whether a website owner should have to identify users who allegedly defamed the plaintiff included whether the alleged tortfeasor had a reasonable expectation of anonymity; whether the plaintiff had established a prima facie case and was acting in good faith; whether reasonable efforts to identify the tortfeasor by other means had failed; and a balancing of the interests in reputation versus freedom of expression and privacy.[50] But a different Ontario judge had earlier advocated adopting the Norwich Pharmacal test from the UK.[51] It is not clear which test is the prevailing standard now in Ontario. The results were the same in both cases, however – the ISPs were ordered to comply with orders to identify users.

In the Netherlands, as in Canada, there is no general constitutional right of anonymity, but it might be implied by the right to free expression,[52] the right to personal and data privacy,[53] and the right to confidential communication.[54] In regard to ISPs, the Supreme Court of the Netherlands has established a balancing test for when an ISP can be required to identify a user that relies on a set of reasonableness questions: Is it reasonable to believe that the information in the communication in question was unjust

---

[45] Norwich Pharmacal Co. v. Comm'rs of Customs and Excise, [1973] 2 All E.R. 943 (H.L.); *see also* Ian Lloyd, "Anonymity and the Law in the United Kingdom," in LESSONS FROM THE IDENTITY TRAIL 465 (Ian Kerr, Valerie Steeves, & Carole Lucock, eds.) (2009).

[46] *See, e.g.,* Rugby Football Union v. Consol. Info. Servs. Ltd., [2013] 1 All E.R. 928; [2012] U.K.S.C. 55 (S.C.) (order to ISP to disclose identities of rugby match ticket resellers upheld); Smith v. ADVFN PLC, [2008] EWCA (Civ) 518 (A.C.) (ordering ISP disclosure of users in defamation case); Clift v. Clarke, [2011] EWHC 1164 (Q.B.) (denying Norwich Pharmacal order to ISP in defamation case); G. v. Wikimedia Found. Inc., [2009] EWHC 3148 (Q.B.) (ordering parent of Wikipedia to disclose identity of contributor(s) who amended Wikipedia entry about plaintiff); Sheffield Wednesday Football Club Ltd. v. Hargreaves, [2007] EWHC 2375 (Q.B.) (ordering ISP to disclose identities of users in defamation case).

[47] Carole Lucock & Katie Black, "Anonymity and the Law in Canada," in Kerr, et al., *supra* note 45.

[48] BMG Canada Inc. v. Doe, [2005] 4 F.C.R. 81, 99-102 (Can. Fed. Ct.).

[49] [2011] O.J. No. 2418 (Can. Ont. Super. Ct.).

[50] *Id.* at ¶ 12.

[51] *See supra* notes 45-46 and accompanying text.

[52] DUTCH CONST. (GRONDWET) ART. 7 (2008), available in English at http://www.government.nl/documents-and-publications/regulations/2012/10/198/the-constitution-of-the-kingdom-of-the-netherlands-2008.html.

[53] DUTCH CONST. (GRONDWET) ART. 10 (2008).

[54] DUTCH CONST. (GRONDWET) ART. 13 (2008).

and damaging to another; is it reasonable for the party seeking the information to desire it; have all reasonable alternative ways to find the information been exhausted; and do the interests of the party seeking the identity outweigh the interests of the ISP and the anonymous person?[55] Courts in later decisions also required persons seeking identities from ISPs to show beyond a reasonable doubt that the persons whose identities they sought were indeed those who damaged them and that it would be unreasonable for the ISP to withhold the information sought.[56]

Elsewhere in Europe, several decisions in France and Germany in recent years have highlighted the tension between anonymity as a privacy right and free expression, as well as lingering uncertainty about the extent to which ISPs are responsible for their users' actions. A French appellate court ruled in 2011 that the host of a blog was liable for damages under privacy laws after a blogger violated the privacy of another blogger.[57] After a man identified in court papers as Jean-Marc D. posted a comment anonymously, another blogger identified him and claimed he was a pedophile.[58] The blog host, JFG Networks, refused to take any responsibility for the privacy breach and claimed protection under a French law similar to Section 230 in the United States.[59] However, the appellate court ruled that JFG was not immune from legal responsibility in for the collection, processing, and storing of personal data.[60]

The strong protection for the privacy of web users in France is not absolute and can be trumped by other interests, as was evidenced by a 2013 Paris Court of Appeal decision. The court ordered the U.S.-based social networking site Twitter to identity users who sent anti-Semitic tweets,[61] even though Twitter had promptly removed the tweets when it got a request to do so.[62]

In the German state of Schleswig-Holstein in January 2013, a data protection agency announced that it was fining Mark Zuckerberg, the founder and CEO of Facebook, €20,000 because the social media site required users to provide their identities in order to open and maintain accounts. German law requires that online media services provide users with the option of using pseudonyms in their online communications.[63] In February 2013, however, a German court ruled in favor of Facebook and voided the fine.[64]

---

[55] Simone Van Der Hof, Bert-Jaap Koops, & Ronald Leenes, "Anonymity and the Law in the Netherlands," in Kerr, et al., *supra* note 45, at 509-10 (citing HR 25 November 2005, LJN 2005, 4019 m.nt. AU (Lycos/Pessers) (Neth.)).

[56] Van Der Hof et al., *id.,* at 510.

[57] Cour d'appel [CA] [regional court of appeal] Montpellier, 5e ch. Dec. 15, 2011, No. 11.5A-4310, Legalis (Fr.).

[58] *Court Rules E-Commerce Law Does Not Trump Web Privacy Rights,* WORLD DATA PROT. REP. (BNA), Jan. 2012, at 31.

[59] *Id.*

[60] *Id.*

[61] Katia Moskvitch, *Twitter Told to Reveal Details of Racist Users*, BBC NEWS, June 13, 2013, http://www.bbc.co.uk/news/technology-22887988

[62] *Id.*

[63] Louise Osborne, *German State Fights Facebook Over Alleged Privacy Violations,* GUARDIAN, Jan. 4, 2013, http://www.guardian.co.uk/world/2013/jan/04/facebook-germany-data-protection.

[64] Hayley Tsukayama, *Facebook Wins Germany Lawsuit on Naming Policy,* WASH. POST, Feb. 15, 2013, http://www.washingtonpost.com/blogs/post-tech/post/facebook-wins-germany-lawsuit-on-naming-policy-thecircuit/2013/02/15/5c6d19ee-778c-11e2-aa12-e6cf1d31106b_blog.html.

In Australia, the law of online anonymity is still developing. Courts seem to recognize some right to anonymity but so far have generally ruled against ISPs seeking to shield users' identities from disclosure, according to a recent research paper by a University of Sydney law professor.[65] In one case, a court ordered HotCopper, the operator of an Internet forum about business, to identify the user who posted allegedly defamatory information about a company.[66] Also, in 2013 a court in South Australia ordered Google to identify the people responsible for websites criticizing a former soccer player turned businessman.[67]

While many Western nations at least indirectly recognize a right to communicate anonymously tied to either free-expression or privacy rights, the picture is somewhat different in nations that have more repressive histories.

For example, the Supreme Court of the Philippines has attempted to find a middle ground between unfettered online communication and a repressive Internet law that critics fear will stifle anonymous dissent, but its final decision left the law largely intact. The cybercrime prevention act[68] that passed in 2012 would have allowed the government to shut down websites hosting allegedly libelous material.[69] The sections of the law that attracted the most criticism would have made it a crime to commit libel "through a computer system or any other similar means which may be devised in the future"[70] and would have allowed the Philippines Department of Justice to block or restrict access to data based on a prima facie showing that it violated the act.[71] Another section would have required persons or service providers to turn over subscriber information within seventy-two hours in response to a court warrant.[72]

Initially, the Supreme Court issued a restraining order to prevent enforcement of the law.[73] However, in February 2014, the court upheld most of the provisions of the original act.[74] The court struck down Section 19, which would have allowed the Department of Justice to block access to data upon a prima facie showing that it violated

---

[65] David Rolph, *Defamation by Social Media* (Sydney Law School Legal Studies Research Paper, Paper No. 13/81, 2013), *available at* http://ssrn.com/abstract-id=2356028.
[66] *Id.*
[67] *Id.*
[68] An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes, Rep. Act No. 10175 (Oct. 10, 2012) (Phil.), http://www.gov.ph/2012/09/12/republic-act-no-10175.
[69] Jillian C. York, *A Dark Day for the Philippines as Government Passes Cybercrime Act,* ABOUT, Oct. 3, 2012, https://www.eff.org/deeplinks/2012/10/dark-day-philippines-government-passes-cybercrime-act .
[70] An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes, Rep. Act No. 10175, § 4(a)(4) (Oct. 10, 2012), available at http://www.gov.ph/2012/09/12/republic-act-no-10175.
[71] An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes, Rep. Act No. 10175, § 19 (Oct. 10, 2012), available at http://www.gov.ph/2012/09/12/republic-act-no-10175.
[72] An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes, Rep. Act No. 10175, § 14 (Oct. 10, 2012), available at http://www.gov.ph/2012/09/12/republic-act-no-10175.
[73] Ellyne Phneah, *Philippines Extends Suspension of Cybercrime Law,* ZD NET, Feb. 5, 2013, http://www.zdnet.com/ph/philippines-extends-suspension-of-cybercrime-law-7000010820/.
[74] Disini v. Secretary of Justice, G.R. No. 203335 (S.C. Feb. 18, 2014) (Phil.).

the law, on free-expression and unreasonable-search grounds.[75] The court upheld penalties in the law for online libel but limited responsibility to the author of a defamatory post, not persons who commented on it,[76] which would seem to favor anonymous commenters. However, the court also upheld Section 14, which requires service providers to divulge subscriber information in response to a valid court warrant,[77] which leaves anonymous online speakers vulnerable to being identified by their ISPs.

In 2014, Russia, which has stepped back somewhat in recent years from earlier attempts to democratize, adopted regulations to make it harder for Internet users to communicate anonymously. A regulation approved in August of that year would require bloggers with 3,000 or more daily readers to comply with the same rules as mass media, including a provision that would require bloggers to identify themselves.[78] Bloggers also are responsible for all content on their blogs, including reader comments.[79]

China and Vietnam have among the most stringent policies against anonymous speech. Chinese constitutional guarantees of free speech and association are subject to limitations if they conflict with the ruling party and cannot be used as legal defenses.[80] The Chinese government uses filtering, blocking, and investigations of ISPs and other interactive computer service providers to stop anonymous public participation in discussions of issues.[81]

The Chinese government approved a policy in 2012 that would require Internet users to register with their real names with service providers. The government said the policy would help service providers better protect customers' information, while critics suggested the policy was meant to silence dissent.[82]

In Vietnam, the ruling Communist Party adopted a decree that it that would force Internet users to provide their real names online and require ISPs to remove content the government found objectionable.[83] Decree 72 took effect in September 2013 and also stated that it was government policy that blogs and social networks were for the sharing of personal information, not news.[84]

In South Africa, registration and monitoring are legally required online, effectively banning anonymity. The government requires ISPs to keep customer data so it

---

[75] *Id.* at 45.
[76] *Id.* at 24-25.
[77] *Id.* at 42.
[78] Michael Birnbaum, *Russian Blogger Law Puts New Restrictions on Internet Freedoms,* WASH. POST, July 31, 2014, http://www.washingtonpost.com/world/russian-blogger-law-puts-new-restrictions-on-internet-freedoms/2014/07/31/42a05924-a931-459f-acd2-6d08598c375b_story.html. *See also* Olga Razumovskaya, *Russian Parliament Approves New Law Restricting the Internet,* WALL ST. J., Apr. 29, 2014, http://online.wsj.com/news/articles/sb10001424052702304163604579531460215555456.
[79] Birnbaum, *supra* note 78.
[80] XIANFA art. 35, § 1 (1982) (China).
[81] *China: Freedom on the Net 2012*, FREEDOM HOUSE, http://www.freedomhouse.org/report/freedom-net/2012/china
[82] Philippa Warr, *China Cracks Down on Internet Anonymity,* WIRED, Dec. 28, 2012, http://www.wired.com/news/archive/2012-12/28/china-internet-registration.
[83] Simon Roughneen, *In Vietnam, Draconian Decree Would Clamp Down on Blogs, Online Speech,* MEDIASHIFT, Feb. 11, 2013, http://www.pbs.org/mediashift/2013/02/in-vietnam-draconian-decree-would-clamp-down-on-blogs-online-speech042.html.
[84] *Vietnam Internet Restrictions Come Into Effect,* BBC NEWS, Sept. 1, 2013, http://www.bbc.co.uk/news/world-asia-23920541.

can be examined, and any Internet system that cannot be monitored is banned.[85] Mobile telephone service providers require subscribers to provide considerable personal information, which can be used by the government. Subscribers also receive a government registered identification number. Enforcing the provisions of South African law are trained inspectors who monitor online communications.[86]

As the above discussion shows, the law regarding online anonymity is largely unsettled around the world. Because the Internet is by nature a global medium, such a lack of consensus causes some concern, but anonymity also joins a long list of legal issues that are unresolved regarding the Internet and its global reach.

Among nations that have long histories of respecting rights to free expression, association, and privacy, there is some consensus that there is a limited right to communicate anonymously. There is also some consensus that Internet service providers are not legally responsible for the acts of their users, anonymous or not, but the recent Delfi decision casts doubt on that proposition in Europe. ISPs may be required to identify their users to private litigants or government officials in some cases. In more authoritarian governmental systems, or systems that are transitioning to democracy but still have vestiges of repressive regulation, there appears to be little support for allowing people to communicate anonymously on any subject, particularly in regard to governmental policies or social reforms.

Part II: Media "Best Practices"

Because the law regarding online anonymity is in flux, and also because allowing readers and viewers to comment anonymously on stories raises certain ethical issues, many news organizations have proactively developed self-regulatory policies regarding whether to accept and how to manage anonymous comments on their sites.

Even within the United States, a wide range of moderation regimes exists. Many online news websites, including NYTimes.com, allow readers to post comments after registering with a valid email address and entering a customizable display name.[87] This provides readers with a degree of anonymity, which is thought to stimulate robust and unhindered conversations on important economic, political, and social issues.

Other news outlets, such as the Wall Street Journal Online, require the use of real names when online readers post comments to news articles.[88] Similarly, some news websites require readers to log in via a social networking platform, such as Facebook, Twitter, or Google+, in order to post a comment to a story. USA Today Online, for instance, requires commenters to be logged in to a Facebook account that contains a profile photo and has at least four friends.[89] The real name and social networking login

---

[85] Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2003 § 1 (S. Afr.).
[86] Electronic Communications and Transactions Act of 2002 § 1 (S. Afr.).
[87] N.Y. Times, *Comments.* http://www.nytimes.com/content/help/site/usercontent/usercontent.html.
[88] Wall St. J., *WSJDN Commenting Rules & FAQS.* http://online.wsj.com/public/page/commenting-rules.html.
[89] USA Today, *Conversation Guidelines.* http://static.usatoday.com/conversation-guidelines/.

requirements arguably bring more responsibility, ownership, and accountability to readers' online commenting activities.[90]

In light of the diversity of approaches taken to address online news commenting, the effect of anonymity on the quality and tone of discussions is a subject of ongoing debate.[91] This section of the report aims to highlight the concerns and experiences of online editors, community managers, comment moderators, and journalists from around the globe in developing and implementing commenting policies, and reports on the emerging "best practices" from media organizations around the world.

The following subsections focus on the advantages and drawbacks of various aspects of a comment moderation policy that may affect comment quality.

Login and Identification

One of the first questions news organizations must consider with respect to publishing online comments is the login and user identification process. Identification procedures can be classified into three broad categories, depending on whether they: (1) allow readers to create a customizable username or pseudonym unique to the website; (2) require readers to log in via a social networking account; or (3) require readers to use their real names when posting comments.

Does the degree of user identification affect the quality of comments posted to news websites? Several editors, journalists, and other commentators have suggested that requirements to attach one's name to an opinion elicits more thoughtful comments.[92] However, one recent study pointed out that there is "no published empirical research into whether must-sign policies actually do result in higher-quality submissions."[93] Overall, a clear picture has not yet emerged about the relationship between commenter identification and the quality of discussions.

Moderation

A second question concerns whether staff should pre-screen comments prior to their public visibility on the website (pre-moderation), selectively delete comments only after they become viewable (post-moderation), or both. Under post-moderation, specific comments are brought to the attention of staff through a community reporting system, where individual users have the ability to flag comments they deem to violate the commenting rules or discussion guidelines. The following chart provides a picture of the moderation and user identification policies of a selection of online news websites:

---

[90] Leonard Pitts, *Pseudonymity Can Battle the Scourge of Comment Anonymity*, CHICAGO TRIBUNE, April 1, 2010. http://blogs.chicagotribune.com/news_columnists_ezorn/2010/04/pseudonymity-can-battle-the-scourge-of-comment-anonymity.html.

[91] Tyler Wells Lynch, *Online Commenting: A Right to Remain Anonymous?*, USA TODAY, March 6, 2014. http://www.usatoday.com/story/tech/2014/03/05/online-anonymity-debate-reviewed/6072431/.

[92] Dean Wright, *What Did You Say Your Name Was?* REUTERS, July 9, 2010, http://blogs.reuters.com/fulldisclosure/2010/07/09/what-did-you-say-your-name-was/; Julie Zhuo, *Where Anonymity Breeds Contempt*, N.Y. TIMES, Nov. 29, 2010, http://www.nytimes.com/2010/11/30/opinion/30zhuo.html.

[93] Bill Reader, *Free Press v. Free Speech: The Rhetoric of 'Civility' in Regard to Anonymous Online Comments*, 89 JOURNALISM & MASS COMMUN. Q. 495 (2012).

Table 1. Login Type and Moderation Procedures of Select Online News Websites

	Pre-Moderation	*Post-Moderation*
Real name or SNS login		Wall Street Journal USA Today Miami Herald Chicago Tribune
Pseudonym	New York Times Washington Post LA Times (blogs) Reuters	NPR LA Times (news) The Guardian (UK) Globe and Mail (Canada)

According to a study published in 2011, the existence of moderation strategies greatly reduces the number of insults posted in online comments, but the various methods used did not seem to affect the quality of the debates.[94] For example, Repubblica.it and NYTimes.com both used pre-moderation done by journalists, but the quality of comments was radically different in the two forums. Meanwhile, Guardian.co.uk, which was the only website studied that adopted a system of post-moderation by members of the public rather than journalists, had the least derogatory language.[95]

Best practices for managing online news commentary

A study published in 2013 by the World Association of Newspapers and News Publishers (WAN-IFRA) and sponsored by the Open Society Foundations (OSF) provides a set of best practices for online news comment moderation. The survey includes online editors and community managers at 104 news organizations from sixty-three countries.

The WAN-IFRA/OSF study outlines the following best practices for journalists, editors, and news organization staff with respect to online news comment management:

1. Publish and update discussion guidelines, comment policies, or community rules.
2. Hire an online community manager to monitor the discussions.
3. Encourage journalists to interact with commenters.
4. Increase the visibility of valuable comments.
5. Give feedback intended to educate readers.
6. Seek legal advice and train staff in the laws around online commenting.
7. Openly discuss management policies with the comment community.

[94] Carlos Ruiz, David Domingo, Josep Lluís Micó, Javier Díaz-Noci, Koldo Meso, & Pere Masip, *Public Sphere 2.0? The Democratic Qualities of Citizen Debates in Online Newspapers*, 16 INT'L J. PRESS/POLITICS 463 (2011).
[95] *Id.*

Publish and update discussion guidelines, comment policies, or community rules

According to the WAN/IFRA study, discussion guidelines should consist of "clear, thorough, transparent suggestions that enable the news organization to host an intelligent discussion and defend [its] moderation decisions."[96] Comment policies should explicitly forbid any and all forms of hate speech and illegal content. At the same time, rules should not overwhelm commenters with a long list of 'don'ts,' but provide proactive guidance, including:

- Details about the discussion environment that is sought;
- Clear definitions of hate speech, defamation, libel, etc.;
- Promotion of dialogue and opportunities for response;
- Encouraging commenters to back up their opinions with data and facts;
- Keeping the commenters focused on the issue at hand, rather than on attacking individuals;[97]

Hire an online community manager to monitor the discussions

"Hiring staff to working solely on comment threads and user-generated content can be a hard sell in tough financial times," the WAN/IFRA study said. Outside of editors and journalists, dedicated staff must be allocated to the task of cultivating constructive discussions, protecting readers from abuse, and gathering community input. If resources permit, hiring a community manager to guide discussions and support the work of moderators is an ideal solution.[98]

Encourage journalists to interact with commenters

Staff participation is thought to improve the quality of discussion, lessen the need for moderation, motivate people who have never commented before to take the "leap of faith," and encourage readers to come back and comment more on a site.[99]

Journalists may pose or provide answers to questions, reply to criticism, and/or highlight the most interesting comments made by readers. It should be kept in mind that some journalists may hold a disdain for comment threads and be reluctant to engage in a dialogue with readers (who may have some degree of anonymity). One respondent from the *Dallas Morning News* said most people in its newsroom "are not interested in comments or feel they're a necessary evil."[100]

---

[96] Emma Goodman and Federica Cherubini, Online Comment Moderation: Emerging Best Practices, Oct. 4, 2013, World Association of Newspapers and News Publishers (WAN-IFRA), http://www.wan-ifra.org/reports/2013/10/04/online-comment-moderation-emerging-best-practices.

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

Increase the visibility of valuable comments

Enhancing the visibility of the most valuable comments is one way to add value to the experience of all readers. At the same time, it serves to reward and reinforce commenters who make substantive contributions and may encourage others to make more valuable comments if they want their contributions to be seen by others. Allowing readers to like or dislike comments is a common mechanism for accomplishing this (with the most liked comments appearing at the top of the discussion). Comment voting also gives readers who may not wish to comment a way to participate in or influence the shape of the conversation. *Helsingin Sanomat* (Finland) employs a unique comment system by allowing readers not only to indicate whether they agree or disagree with an individual comment but also if they think a comment is well-argued.[101]

In addition to allowing users to rate comments, staff can be a source of comment recognition. Staff may pick comments to deliberately showcase the diversity of opinions readers hold about an issue. At the same time, staff picks demonstrate to readers that news staff read and place value on their comment submissions.[102]

Give feedback intended to educate readers

Rather than simply deleting comments that seem unsuitable without providing any information for why it was deemed offensive, news staff should try to give feedback to readers about why their comments were deleted. Oftentimes, readers can make offensive comments without intending to insult others. News organizations that have sought to educate readers have reported positive responses and improved comments (BBC, UK: *The Guardian*, UK; Gulf News, UAE). Simply asking the reader to think about why the comment was deemed offensive, or asking her to reword or rewrite it, has also been met with success (*Winnipeg Free Press*, Canada).[103]

Seek legal advice and train staff in the laws around online commenting

Moderators, community managers, and online editors should have up-to-date knowledge of the legal situation, as "foggy" as it is, regarding third-party content hosted on news sites.[104]

Openly discuss management policies with the comment community

Der Standard (Austria) has created a special section of the website where community management issues can be debated.[105]

---

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*

Other ideas

- *Libération* (France) encourages readers who voice complaints, such as politicians who are criticized in the comments section, to create a profile and engage in dialogue with other readers directly.
- Some outlets seek to ensure that majority voices do not drown out individuals in the minority who may already be reluctant to contribute to the conversation.
- Project Syndicate allows readers to pin comments to specific paragraphs in a news article so that they can comment on a specific point, argument, or idea.[106] This creates a pin that other readers can click to read the comment.
- *Winnipeg Free Press* (Canada) has utilized a "bozo filter" for trolls who violate its rules: it allows the poster to see the comments, but no one else.[107]

Conclusions

Just as the law regarding anonymous commenting remains unsettled, media policies are still in an experimental stage. Media companies, eager to tap into the possibilities for engagement with audiences that the Internet provides but unhappy with the tone of some comments, are trying a variety of methods to monitor comments. There is little research on the effects of the various methods, but what research there is indicates that some form of moderation helps to improve the civility of comments.

The recommendations from the WAN/IFRA study are worth noting because they deal with both the goals of allowing comments and the best practices adopted to date for moderating the comments. The study indicates that a comments section works best when it is incorporated into the operation of the news organization, rather than treated as a side business, and when the organization rewards some comments to encourage writers to post similar material. It also helps if journalists interact with those who post comments and if the organization provides feedback to commenters instead of just deleting their comments without explanation.

While some news organizations have discouraged or banned comments by anonymous or pseudonymous persons, either by requiring registration or limiting comments to social media sites, not all have done so. The potential cost of such policies in terms of discouraging comments from persons who, legitimately or not, fear reprisals for their views may deter many organizations from banning anonymity. There is no strong research indicating that banning anonymity will, in and of itself, elevate the level of discourse on media websites.

Governments that claim to value democratic discourse among their citizens should be cautious about adopting policies that ban or discourage anonymous publication either directly or indirectly. Likewise, they should be cautious about discouraging news

---

[106] *Id.*
[107] *Id.*

organizations and other ISPs from accepting such comments by making them liable for what their users say or making it too easy to force them to identify their users to authorities or private litigants. Sometimes the truth is uttered from behind a mask; banning the mask may also ban the truth.