Online Abuse and Harassment

EMMA A. JANE
UNSW Sydney, Australia

Language Warning and Note on Terminology

This entry includes unexpurgated examples of real-life gendered cyberhate, including explicit imagery of sexual violence. Many readers are likely to find it confronting, offensive, and possibly triggering. While the intention is not to cause gratuitous upset, the use of euphemisms and generic descriptors such as "hostile," "graphic," and "in bad taste" simply do not capture the force and violence of the phenomenon in such a way that it can be properly understood and conceptualized. Additionally, for the most part, the term "target" rather than "victim" is used in this entry in recognition of research acknowledging the impact of language choice in terms of facilitating women's empowerment and resistance after surviving sexual assault. The expression "victim-blaming" is used for idiomatic reasons (that is, because "victim-blaming" has cultural and political connotations that "target-blaming" does not).

Introduction

Since the advent of the Web 2.0 era (for discussion, see the "Prevalence" section later), rape threats, cyberstalking, image-based abuse such as "revenge porn," and other forms of gendered violence online have become increasingly prevalent, toxic, and harmful. Contrary to claims—by a range of commentators in a range of contexts—that cyberhate is mostly innocuous (that is, "just words," "just the internet," and so on), a growing number of academic studies into the issue shows that the widespread suffering caused is real, tangible, and embodied. The coercive force of gendered cyberhate has been identified as causing many women significant social, psychological, reputational, economic, and political harms, and can be understood as constituting a new form of workplace harassment as well as an emerging, economic dimension of existing, gender-related digital divides.

The problem of gendered cyberhate has received extensive international media coverage, as well as being the subject of calls for urgent intervention from organizations such as the United Nations (UN), Amnesty International, and various international human rights associations. Yet there exists a wide range of insidious structural, institutional, and technological factors—as well as interactions between them—that continue to make gendered cyberhate into a problem that can be difficult to understand and appreciate in its damaging entirety, let alone to combat. In a nutshell, while the technology is new, the threats of sexual violence, victim-blaming, and institutional

The International Encyclopedia of Gender, Media, and Communication. Karen Ross (Editor-in-Chief), Ingrid Bachmann, Valentina Cardo, Sujata Moorti, and Marco Scarcelli (Associate Editors).

DOI: 10.1002/9781119429128.iegmc080

inaction associated with online abuse and harassment directed at women sit squarely in far older traditions. Among other things, this illustrates the tenacity of misogyny, the ongoing impacts of systemic gender inequity, the complexity of social problems flowing from machine–human interactions, and the continuing relevance of feminist activism.

Terms and Definitions

Despite many decades of discussion and debate in scholarly work, hostility, violence, and hate speech online have proved to be difficult to name and to define (for discussion, see Jane, 2015). In general, when vitriolic or disruptive discourse on the internet has not been coded as either racist hate speech or cyberbullying affecting children and young people, scholars have historically referred to it as either "flaming" or "trolling." Both are highly elastic and contested descriptors. The former is an antiquated expression used—mostly in the earliest decades of internet research—to refer to heated exchanges that are extremely tame and non-gendered compared to contemporary cyberhate. "Trolling," on the contrary, remains in common parlance and is used to refer to a very wide range of communications and phenomena including: relatively mild, "flame"-type discourse; extremely graphic, threatening, and violent cyberhate; the posting of deliberately inflammatory or off-topic material with the aim of provoking responses and emotional reactions in targets; and internet pranking in general. For these reasons, it is not a precise or particularly useful term.

Recent scholarly interest in misogyny on the internet has, however, led to the emergence of a range of other terms for gendered hostility, harassment, and abuse online. These include "technology violence" (Ostini & Hopkins, 2015), "technology-facilitated sexual violence" (Henry & Powell, 2015), "gendertrolling" (Mantilla, 2015), "rapeglish" (Jane, 2017a), and—from the UN Broadband Commission—"cyber violence against women and girls" or "cyber VAWG." In this entry, the term "gendered cyberhate" is used to refer to a range of phenomena occurring at the gender-technology-violence nexus. The use of grammatical variations on the word "phenomenon" instead of "action" or "speech" is deliberate and is to avoid begging the question in favor of either the claim that cyberhate is *action* or that it is *communication* (which is arguably a false dichotomy).

Gendered cyberhate includes sexually graphic invective, hyperbolic yet plausible rape and death threats, and/or persistent, unwanted sexual advances from senders who tend to become aggressive if they are ignored or rebuffed. Signal characteristics of the discourse include profanity, violent and sexualized rhetoric, explicit, *ad hominem* invective, and the framing of coerced sex as an all-purpose corrective. Aspersions are cast on women's intelligence, mental health, and sexual attractiveness, with targets frequently being appraised not only in terms of their "fuckability" but also their "rapeability." Incitements to suicide are common, especially if a target is known to suffer from mental health issues. Threats are also routinely made against women's online supporters, colleagues, intimate partners, children and other family members, friends, and pets.

Abuse and harassment are image- as well as text-based. Photo and video manipulation, for example, is often used to place an image of a target into a scene involving sex and/or violence—an example of a larger set of practices known as "deepfakes." It has also become common for men to send unsolicited and unwanted photos of their genitals—aka "dick pics," with 2018 research by YouGov United Kingdom showing that four in 10 female millennials have been sent such photos (Smith, 2018).

Gendered harassment and abuse online can be situated along a spectrum of violence and harm ranging from "mildly irritating" at one end to "unambiguously criminal" at the other. An example from the mildest end of the spectrum might involve a man on an online dating site continuing to send dozens of messages to a woman despite being ignored or explicitly informed she is not interested. A real-life case study that sits at the most extreme end of the spectrum is that of Jebidiah Stipe, a 28-year-old American man who in 2009 impersonated his former female partner on the internet site Craigslist and published a photo of her alongside text saying she was seeking "a real aggressive man with no concern for women." More than 160 people responded to the advert, including a man who—after Stipe divulged his ex-partner's address—arrived at the woman's home, bound and blindfolded her, and raped her at knifepoint (Citron, 2014a, pp. 5–6). Both Stipe and the rapist were subsequently jailed for 60 years to life in prison. This example shows the way gendered cyberhate can be contextualized within a broader "pandemic" of gendered violence—as per data provided by the UN indicating that there exist parts of the world in which 8 out of 10 women are reported to suffer some kind of violence including sexual, physical, and psychological violence (UN Broadband Commission for Digital Development, 2015, p. 13). In particular, cyber harassment and abuse is increasingly being observed as a dimension of domestic violence scenarios.

Manifestations

The following is a rough taxonomy of frequently observed manifestations of gendered cyberhate. Please note that this list is not exhaustive, contains items that have clear overlaps with other items (as well as with other phenomena not listed), and will likely date rapidly given the speed with which practices and technologies—and the interplay between them—are creating new modes of engagement online. Further, the listed practices are not exclusively directed against women and girls but may also be evident in attacks perpetrated against men and boys.

Cyberbullying: calculated and ongoing behavior used by individuals and groups wishing to inflict harm on and cause distress to their targets (a term used mostly in the context of school students and youth populations).

Doxing/doxxing: the publishing of personally identifying information to either explicitly or implicitly incite internet antagonists to hunt targets offline.

Cyberstalking: includes, making multiple and unwanted attempts to contact targets via mobile phone, e-mail, and social media; installing spyware on targets' computers; hacking into targets' e-mail or social media accounts; installing video cameras in and around targets' homes; and/or placing global positioning system (GPS) trackers on

targets' cars, thus enabling perpetrators to track targets' movements and potentially confront them in offline contexts.

Google bombing: the manipulation of the Google search engine so that web users searching for a specific term are directed to content determined by the bombers (usually material that is reputationally damaging, defamatory, and/or false).

Identity theft and impersonation: sometimes associated with criminal attempts at financial gain but, in the context of gendered cyberhate, usually deployed for the purpose of stalking, reputational attack, and/or inciting abuse against a target.

Rape video blackmail: the filming of sexual assaults and subsequent use of the footage to blackmail targets.

Revenge pornography: a colloquial term used to describe the public circulation of sexually explicit material, often of a former partner, without the consent of the pictured subject.

Sextortion: the use of techniques such as hacking targets' computers and webcams, installing malware on their devices, impersonating actual or potential romantic interests, and/or social media grooming to obtain intimate images of targets, which are then used for blackmail.

Swatting: the practice of tricking police dispatchers into sending Special Weapons and Tactics (SWAT) teams to raid targets' houses.

Wikipedia vandalism: malicious edits made to a target's Wikipedia page.

Mob attacks (aka "dog piles"): en masse attacks that may coalesce organically or be deliberately initiated and/or organized by groups or individuals.

Prevalence

While hostile interactions occurred from the earliest days of the internet, cyberhate was relatively rare and mild until around 2010 at which point it became far more prevalent, visible, harmful, gendered, and directly threatening (for discussion, see Jane, 2017b, pp. 16–42). These amplifications are likely a flow-on effect from the self-publishing and networking opportunities associated with the Web 2.0 era. ("Web 1.0" is generally used to describe those early decades of the internet when content was mostly static and delivered in a read-only format, while "Web 2.0" refers to the shift—most obvious from around 2006—toward user-generated material, interactivity, collaboration, and sharing.) In short, the Web 2.0 era has given online antagonists access to targets and appreciative audiences in a way that was not previously possible. Further, given that most offenders can attack with impunity, the number of girls and women subjected to cyberhate is rising rapidly.

In 2015, the UN Broadband Commission warned that cyber VAWG had become "a global problem with serious implications for societies and economies around the world." It noted that 73% of women and girls had encountered some form of online violence; that women were 27 times more likely to be abused online than men; that 61% of online harassers were male; and that women aged between 18 and 24 were at particular risk. The UN warned that, unchecked, cyber VAWG risked becoming "a 21st-century global pandemic with significant negative consequences for all societies

in general and irreparable damage for girls and women in particular" (UN Broadband Commission for Digital Development, 2015). In late 2017, Amnesty International UK condemned online abuse and harassment as an "emerging violation of women's human rights." It published research showing that of those women in the United Kingdom, the United States, New Zealand, Spain, Italy, Poland, Sweden, and Denmark who had experienced online abuse or harassment: more than a quarter (27%) received direct or indirect threats of physical or sexual violence; almost half (47%) had experienced sexist or misogynistic abuse; 59% said the perpetrator was a stranger, compared with 27% who personally knew the offender; and one-third (36%) felt their physical safety had been threatened (Amnesty International UK, 2017). Most recently, the Australian Human Rights Commission (AHRC) has found that 76% of women under 30 years of age had reported experiencing online harassment, and almost half (47%) of all women had been targets (AHRC, 2018, p. 20).

While some studies suggest that women and men are equally likely to report experiencing digital harassment and abuse (see, for example, Powell & Henry, 2015, p. 1), girls and women tend to be targeted for more severe abuse and tend to report more suffering as a result. For instance, a 2014 study by the Pew Research Center in the United States found that men are more likely to experience name-calling and embarrassment—harassment of the types categorized as less severe: "a layer of annoyance so common that those who see or experience it say they often ignore it" (Duggan, 2014, pp. 2–3). Young women, in contrast, are particularly vulnerable to severe types of abuse such as stalking, and sexual harassment. These findings comport with Australian research showing that women are more likely to be "very or extremely upset" by online abuse and are more likely to take actions such as changing their online details or profile settings, or leaving a site (Powell & Henry, 2015, p. 1).

Intersectional Nature of Abuse

Women from marginalized and/or vulnerable sectors of society—such as members of cultural and linguistic minority groups and of the LGBTQI+ community, as well as women with physical and mental disabilities—tend to experience more frequent and more noxious cyber abuse, not least because, in addition to being targeted by virtue of their identity as "female," they may additionally be targeted on account of being a person of color, a Muslim, a lesbian, and so on. For example, the Australian politician Dr. Mehreen Faruqi says she receives "relentless abuse and hate" whenever she speaks publicly—regardless of the topic she is discussing:

> Practically every day, I receive directly targeted messages on social media and through abusive phone calls, letters and emails that attempt to push me out of the political conversation simply for being who I am—a brown, migrant, Muslim woman from a Pakistani background … I'm not usually afraid to say what is right, but sometimes I've wanted to crawl into bed and not get up. I've thought of doing exactly what the haters want—shutting up. For the first time, I've seriously considered the question: Is it really worth it? (2019)

Another demonstration of the way cyberhate mirrors offline prejudices, biases, and oppression can be found in *The Guardian*'s 2016 quantitative analysis of its own comment threads. After examining 70 million remarks, its data analysts found that of the 10 regular writers who received the most abuse, eight were women (four White and four non-White) while two were men of color (Gardiner et al., 2016). The AHRC, meanwhile, notes that one in four lesbian, bisexual, and transgender women report targeted sexual orientation harassment online (2018, p. 20), while American statistics show that 45% of school-aged lesbian, gay, bisexual, or transgender cyber harassment targets feel depressed, and more than 25% wrestle with suicidal thoughts (Citron, 2014a, p. 11).

The Etiology of Gendered Cyberhate

Multiple explanations have been offered for the very high rates of gendered cyberhate currently circulating online. Some causal narratives emphasize the role of technology, while others point to enduring misogyny and systemic gender inequity. Certainly, many features of the cybersphere make it easy for people to abuse and harass others with impunity. Despite a move toward "real-name" policies on platforms such as Facebook, it remains simple and inexpensive to create an endless stream of anonymous, disposable accounts that can be used to engage in cyberhate and other forms of cyber abuse before being discarded—thus making it difficult for perpetrators to be identified and located. Similarly, various features of the internet such as proxy servers, virtual networks, and other technologies also make it effectively impossible to pin down either the physical location of the computer or device on which an offender's account was located, or the physical location from which they accessed it. These features of the cybersphere, however, are *general* features. While they explain the *mechanisms* that allow people to engage with each other in a hostile fashion (the medium), they are related to but do not fully explain the *content* of this speech (the message). The fact that so many men are using the affordances offered by the internet to abuse so many women using the rhetoric of gendered violence is both diagnostic and constitutive of the fact that men continue to hold a disproportionate share of political, economic, and social power, and use various forms of violence against women to maintain the inequitable status quo. To a certain extent, hateful cyber discourse can also operate as a litmus test for the sorts of community attitudes that exist below the surface but are no longer considered acceptable to express in "polite" company.

Gamergate

One of the most notorious instances of mob attacks on women online is the 2014 international assault on women in gaming that has been dubbed "Gamergate." Gamergate began in the aftermath of a relationship break-up between the feminist independent games designer Zoë Quinn and the software developer Eron Gjoni. After the couple separated, Gjoni published a lengthy blog accusing Quinn of exchanging sex for favorable reviews from a games journalist—a claim he later retracted. Shortly after the blog

was published, however, online antagonists began circulating Quinn's home address and personal photos online, and her Wikipedia entry was edited to read: "Died: soon." Anonymous strangers threatened Quinn's father, and the future employers of her new boyfriend (who subsequently had a pending job offer withdrawn). The 16 gigabytes of abuse Quinn received in the first year of Gamergate included threats such as, "Im not only a pedophile, ive raped countless teens, this zoe bitch is my next victim, im coming slut," and "kill yourself. We don't need cunts like you in this world." Quinn left her home in fear for her safety shortly after the assaults began.

Another high-profile target of Gamergate was the feminist games commentator Anita Sarkeesian whose ongoing "Tropes vs. Women" series about sexism in gaming meant she had already been subjected to years of abuse including receiving countless images depicting men ejaculating onto photos of her face. She was also the subject of an online game that allowed players to "punch this bitch in the face" until her image turned completely black and blue. In August 2014, Sarkeesian also had to leave her home after receiving a series of graphic death threats that demonstrated knowledge of her home address. She subsequently canceled a Utah State University address after an anonymous e-mailer threatened "the deadliest school shooting in American history" if her talk went ahead as planned. Another prominent target was the American games designer Brianna Wu. Within minutes of her personal details being posted online, Wu received a message from someone saying they were on their way to her house to rape her with a combat knife. Like Quinn and Sarkeesian, she also left her home because she feared for her safety.

As time passed, Gamergate supporters expanded their pool of targets, moving from women in the games industry, to female journalists writing about the games industry, to women regarded as "social justice warriors," and then to seemingly anyone who made any public comments that did not support or was critical of the movement. Tactics deployed included doxing, swatting, and coordinated reputational assaults—attacks that, in various forms, were ongoing at the time of publication.

Harms

Extensive quantitative and qualitative data exists showing that gendered cyberhate is causing women significant social, psychological, reputational, economic, and political harm—including limiting women's ability to engage in activism in response to the problem of gendered cyberhate itself. Abuse and harassment online are hampering their ability to freely enjoy key benefits of the Web 2.0 era in forms such as self-expression, self-representation, creativity, interactivity, collaborative enterprises, and participation in civic life and democratic governance. Indeed, new analysis demonstrates that gendered cyberhate infringes on at least 10 Articles from the Universal Declaration of Human Rights (UDHR) (Jane & Vincent, 2018). Research into the impact of gendered cyberhate shows that while women might *seem* to have full and unfettered access to the internet, in practice, the hate and harassment they experience might be severely constraining their ability to use it. Moreover, those women who most depend on unrestricted access to the internet and social media platforms to earn their livings

are particularly prone to receiving cyberhate (examples include freelance opinion writers and others engaged in similarly precarious labor). As such, the cumulative disadvantages of gendered cyberhate can be understood as constituting an emerging, economic dimension of existing, gender-related digital divides. ("Digital divide" is a term used to discuss online equity and refers to differences between population groups in terms of access and uses of information and communications technologies.) Further, this is a digital divide that is insidious in that it involves barriers to equity and full participation online that are not as easy to identify and measure as those barriers relating to access to computer hardware and network connections.

Hate and harassment online is affecting women's ability to find—and keep—jobs, to market their personal brands and their businesses, and to network socially and professionally. Much of the cyberhate women receive at work involves abuse and harassment that contravenes laws and policies in many nations, as well as various international labor treaties, conventions, and recommendations (Jane, 2018). For instance, it breaches many sections of the International Labour Organization (ILO) guidelines with regard to states' and employers' obligations vis-à-vis women worker's rights and gender equality (ILO, 2007). Far from being "just words" or harmless "jokes," online abuse has the power to destroy women's reputations in ways that have significant and ongoing repercussions for their future employment and career-building prospects. For example, the feminist legal scholar Danielle Keats Citron points out that schools have fired teachers whose naked photos have appeared on revenge porn sites, while a government agency terminated a woman's employment after a coworker circulated her nude photograph to colleagues (2014b). Cogent, too, is the fact that most employers rely on candidates' online reputation to filter applicants.

Harassment, threats, and abuse at the most extreme and sustained end of the spectrum are causing women debilitating fear and trauma, as well as profound life disruption. Gendered cyberhate targets describe emotional responses ranging from feelings of anxiety, sadness, shame, isolation, vulnerability, and unsafeness; to distress, pain, shock, terror, and violation. Some report developing serious mental health problems such as anxiety disorder, depression, panic attacks, agoraphobia, and conditions resulting in self-harm, and/or experiencing psychological breakdowns in the aftermath of being attacked online (Jane, 2017b, pp. 62–64; 2017c). Amnesty International UK research shows that of those women subjected to online abuse and harassment: more than half (55%) suffer stress, anxiety, or panic attacks; three out of five (61%) have trouble sleeping; two-thirds (67%) feel apprehensive when thinking about using social media; and one in five (20%) feel that the online abuse threatens their job prospects.

Institutional Inaction

Despite the violence and significant harms of gendered cyberhate, police, policy makers, and platform managers in most nations are failing to adequately acknowledge or address the problem. In 74% of Web Index countries (including many wealthy Western nations), law enforcement agencies and the courts are failing to take appropriate action in response to gender-based violence online, while at least one in five female internet

users live in countries where harassment and abuse online is extremely unlikely to be punished (Web Index, n.d., p. 15). A 2014 report by the Association for Progressive Communications (APC) identified multiple policy failures in that, despite increases in violence against women involving information and communications technology (ICT), there has been "very little corresponding recognition of ICT-related forms of violence against women by states, intergovernmental institutions and other actors responsible for ending violence against women" (APC, 2014, p. 4). This empirical data comports with multiple anecdotal accounts from women who report that the standard response from police in many jurisdictions is to suggest they simply "take a break" from the internet. Others report being chastised for some aspect of their mode of conduct online and are told to engage differently. The response of platform operators has been similarly problematic and inadequate. Another APC cyber VAWG report comparing the policies of Facebook, YouTube, and Twitter identifies a number of overarching issues including: a reluctance to engage directly with a problem unless it becomes a public relations issue; a lack of transparency around reporting and redress processes; a failure to engage with the perspectives of non-North American/European women; and no public commitment to human rights standards or to the promotion of rights, other than the encouragement of free speech (Nyst, 2014, pp. 3–4).

Real or Virtual?

In offline contexts, the types of threats, breaches of privacy, reputational attacks, incitements to violence, coordinated bullying, vilification campaigns, economic vandalism, and workplace harassment that occur in the context of gendered cyberhate would not be tolerated. Online, however, such behavior often passes unnoticed, or else is played down or dismissed out-of-hand as unimportant. For example, media and other commentators frequently argue that what happens online is virtual rather than "real" and that therefore any harms claimed to be suffered by targets of cyberhate are imagined, fabricated, and/or exaggerated. Contradicting such views is the argument advanced by the Australian academics Nicola Henry and Anastasia Powell who point out that harms in the supposedly "virtual" world can have real, bodily, and psychical effects, and "at least as much impact on a person as traditional harms occurring against the physical body" (2015, p. 765). This comports with the accounts given by gendered cyberhate targets who describe their experiences online in physical terms, reporting, for example, that being attacked feels like "being kicked in the guts," "slapped in the face," and "vomited on," as well as reporting physical manifestations such as increased heartbeat, sweating, nausea, feeling the hair on the back of their neck stand on end, experiencing cold chills, and so on (Jane, 2017b, p. 65). This illustrates the way seemingly disembodied discourse online can have a starkly embodied impact and supports the claim that online attacks should not be categorized as virtual and disembodied but instead constitute harms that can manifest in bodies.

Online phenomena spill into offline domains in other ways too. Consider, for instance, the increase in men publishing faux online advertisements claiming their ex-wives or former girlfriends are soliciting sex in order to incite strangers to assault

these women in offline contexts. One example involves a man who posted an advert titled "Rape Me and My Daughters," which included his ex-wife's home address, and which prompted more than 50 strangers to arrive at her home (Sandoval, 2013). This included one man who tried to break into the woman's home and another who attempted to undress her daughter. The above examples illustrate one of two distinct ways in which it is possible to account for why the virtual world matters (Vincent, Lindsay, & Potts, 2018, pp. 22–23). On the first account, what occurs online matters only derivatively, because things that happen in the virtual world impact what happens in the physical world—such as women suffering physical symptoms in response to cyber attacks or having assailants discover their home address online and turn up at their doorstep or workplace. On the second account, the virtual world can be understood as having significance in its own right (Vincent, Lindsay, & Potts, 2018, pp. 22–23). Human interactions increasingly take place online. We do not shop for groceries, pay our bills, and talk to our friends online—we simply do our shopping, pay our bills, and comment on our friends' Facebook posts. As such, feeling too fearful to engage in social media activity or being advised by police to stay away from online forums is significant even if it has no adverse spill-over effects in the physical world. It is important, therefore, that harms such as cyberbullying, cyberhate, and cyber abuse are recognized as significant not just because of the flow-on impacts in the physical domain, but because the virtual world is now an *inherently* significant part of contemporary life.

Women's Responses

Without wishing to downplay the harms of gendered cyberhate detailed earlier, many female recipients do report being able to laugh off or ignore attacks, and feel angry and spurred to action, rather than silenced. The rise of various forms of feminist action in response to misogyny online (see the "Feminist Issues" section later) demonstrates that many women are reclaiming a sense of power and agency by using a range of strategies to fight back against and sometimes enact revenge on their male attackers. Tactics used to navigate gendered abuse and harassment in online domains vary between individual women and individual episodes of cyberhate: that is, a woman might be able to brush off or disregard most attacks but reach one or more breaking points at which time she struggles to cope. This may come about because of: attacks that focus on a particularly sensitive subject or person (e.g., a recently deceased parent or sick child); attacks that are especially brutal and/or triggering (e.g., a survivor of sexual assault might find graphic rape threats re-traumatizing); and/or attacks that continue for long periods of time and involve large numbers of messages and/or assailants. The burn-out associated with the last one is linked not only to the content of messages, but also to the time, energy, and potential costs involved in blocking attackers, attempting to secure one's technology, reporting individual instances of abuse to platforms, dealing with police, attending court appearances, arranging either formal or informal security in offline contexts, explaining the situation to one's employers, and so on.

Generally speaking, women's responses to cyberhate involve one or more of the following, intersecting categories (Jane, 2017c):

- *Distancing* in forms such as ignoring, blocking, muting, and deleting objectionable content and users.
- *Rationalizing,* for example, by explaining away abuse in ways that render it less personal, such as focusing on the fact that it is a systemic, gender-related problem rather than a personal issue.
- Practicing *technological "hygiene"* by setting personal boundaries around technology in an effort to reduce the impact of cyberhate while still accessing and fielding such material (e.g., refraining from checking e-mail and social media accounts after hours or at home, outsourcing e-mail and social media account-checking to friends or colleagues during attacks or in the lead-up to anticipated attacks, and so on).
- *Restricting* internet use in forms such as attempting to avoid interactions with strangers and contentious debates and hashtags, restricting or refraining from circulating personal information and photos, seeking private spaces such as closed Facebook groups, "locking down" or privatizing accounts, disabling comment sections on blogs, and/or taking short, long, or permanent breaks from parts or all of the internet.
- *Reporting* to platforms, police, policy makers, and other institutions and institutional representatives via established protocols.
- *Confronting* attackers whether by similarly abusive tactics, reason, humor, good-natured appeals to assailants as fellow internet users, and so on.
- Engaging in "traditional" awareness-raising and advocacy *activism* such as writing/speaking about cyberhate, signing or launching petitions, lobbying platforms and policy makers, rallying support from online and/or offline communities, providing assistance to other female targets, forming or joining activist groups, archiving received cyberhate for activist purposes, and so on.
- Engaging in *performance-based* activism by creatively repurposing cyberhate (an example is the increasingly common practice of "performing" online hate speech by reading such material aloud in publicly circulated videos).
- Engaging in online vigilantism aka *digilantism*—that is, extrajudicial practices intended to punish attackers or otherwise bring them to account (see later for further discussion).

Feminist Issues

As with rape, domestic violence, and workplace sexual harassment prior to feminist campaigns in the 1970s, the abuse of girls and women online is frequently trivialized, mocked, dismissed as personal matters for individuals to solve, and presented as legally intractable (Jane, 2017d). Also paralleling more traditional forms of sexual assault and harassment is the fact that the onus is often put on gendered cyberhate targets to take safety precautions online, such as avoiding debates about loaded political topics, staying away from unknown terrain or interactions with unknown

people, and refraining from posting images of themselves that male users might find provocative (Jane, 2017b, pp. 88–92). The UK writer Laurie Penny draws parallels with the ubiquity of victim-blaming associated with offline sexual violence when she suggests that a woman's opinion has become the "short skirt of the internet" in that "having one and flaunting it is somehow asking an amorphous mass of almost-entirely male keyboard-bashers to tell you how they'd like to rape, kill and urinate on you" (Penny, 2011). Campaigning against gendered hate speech and harassment and other exclusionary practices online has become a key concern for contemporary cyber feminists, some of whom deploy the self-same technological artifacts and environments used against women to expose and push back against perpetrators.

The issue of gendered cyberhate poses many challenges for various sectors of contemporary feminist movements. For example, the sheer volume of gendered cyberhate can result in activist fatigue. Even dealing with cyberhate as an ally of targets can be extraordinarily time-consuming. When the morally conservative Australian activist Coralie Alison was targeted for a barrage of cyberhate incited by an American rapper in 2015, for instance, her supporters spent whole days filling out online forms reporting individual messages to Twitter on her behalf. One of Alison's allies joked that she had developed carpal tunnel syndrome from so many hours of reporting, because each individual report required 10 mouse clicks (Jane, 2017b, pp. 60–61). Also relevant are: the tensions between individual versus collectivist responses (as well as between older generations of feminists versus young, digital native feminists); the politics associated with intersectional feminism; and the fact that the domain in which these new versions of old misogyny are playing out—the cybersphere—is also a place of great social and political opportunity for feminists.

The situation is further complicated by the fact that women and girls are also known to attack each other, as well as to attack men and boys online—that is, women can be perpetrators as well as the targets of cyberhate. Ethical issues arise when feminists respond to gendered cyberhate in kind, for example, via public mockery, shaming, *ad hominin* invective, abusive rhetoric, and/or digilantism. Instances of the last-mentioned range from "calling out" or "naming and shaming" online attackers, and/or attempting to bring antagonists to account by contacting their employers or members of their families, and/or hunting down and confronting them offline (for examples and discussion, see Jane, 2017c). While digilantism can offer many benefits and is understandable given the dearth of institutional interventions, it can also: put individual activists at risk; contribute to an escalating cycle of amplifying aggression online; and involve large groups of digilantes engaging in excessive forms of retaliation.

The use of feminist humor to respond to gendered cyberhate is also becoming increasingly evident. An example involves the Australian stand-up comedian Hannah Gadsby who joked in a television appearance about having received a message saying: "You fat, ugly, bitch. You wouldn't be raped in a men's prison on a Saturday night." In her response, Gadsby agreed she was fat but questioned the man's assumption that days of the week are relevant in terms of prison recreational activities. She then mimicked a possible inmate of this penitentiary enthusing: "Oh I can't wait for Saturday night. It's craft and rape night!" (Gadsby, 2014). The comedian Amy Schumer, meanwhile, broadcast a sketch involving the introduction of a fictional "I'm Going to Rape and Kill

You" social media button in order to, "lessen the burden of typing those seven words out individually for the thousands of male internet users who express the sentiment on a daily basis." This, it was said, would free additional characters for men to make other comments about women such as "what ugly sluts they are" (cited in Provenzano, 2016).

Potential Remedies

While gendered cyberhate is a complex and difficult problem, researchers, experts, and other commentators have proposed a number of potential avenues for interventions and remedies (for an overview and discussion, see Jane & Vincent, 2017, 2018; Vincent & Jane, 2017a, 2017b). One suggestion involves the formulation of new categories of criminal offences. Provisions could be made to levy fines for recognized offences—on a par with what already occurs in relation to parking and speeding violations, obscene or threatening conduct on public transport and in public spaces, and so on. Civil remedies could also be useful in forms such as protection orders and litigation against individual offenders, as well as class action law suits against software designers and platform operators who create and maintain unsafe environments. Platform operators and technology designers could also be encouraged (or "nudged" via carrot and stick legislative approaches) to implement measures such as a ban on instant/disposable and/or anonymous accounts. Software designers and platform managers who do not take responsibility for designing safer spaces—like the safety built into offline environments—could also face potential fines, liability, and even criminal sanctions if their users are harmed. To design the right technological solutions, ethics could also be taught to engineering and design students as a way of "baking in" ethical functionality into software and platforms. Learning to build ethical functionality into artifacts and environments—an approach known as "value-sensitive design"—could be an integral part of the training of designers and engineers and privileged as being just as important as learning to build and program any other functional requirement of a technological device or environment. Another option would be to expand existing cyber-safety programs in schools to include a greater focus on cyber ethics and cyber civility. Ultimately, however, it is difficult to imagine even the most comprehensive and multifaceted response to gendered cyberhate succeeding without a concomitant shift in the inequitable treatment of women and girls in the broader culture.

SEE ALSO: Doxing; Feminist/Activist Responses to Online Abuse; Gamergate; Gendered Hate Online; Sexism and Misogyny

References

Amnesty International UK. (2017). Press release, November 20. More than a quarter of UK women experiencing online abuse and harassment receive threats of physical or sexual assault—new research. Retrieved from https://www.amnesty.org.uk/press-releases/more-quarter-uk-women-experiencing-online-abuse-and-harassment-receive-threats

Association for Progressive Communications. (2014). Domestic legal remedies for technology-related violence against women: Review of related studies and literature.

Women's Legal and Human Rights Bureau for the "End violence: Women's rights and safety online project." Retrieved from http://www.genderit.org/sites/default/upload/domestic_legal_remedies_for_technology-related_violence_against_women_review_of_related_studies_and_literature.pdf

Australian Human Rights Commission (AHRC). (2018, July). Human rights and technology issues paper. Retrieved from https://www.humanrights.gov.au/sites/default/files/document/publication/AHRC-Human-Rights-Tech-IP.pdf

Citron, D. K. (2014a). *Hate crimes in cyberspace*. Cambridge, MA: Harvard University Press.

Citron, D. K. (2014b, January 16). "Revenge porn" should be a crime in U.S. CNN. Retrieved from http://edition.cnn.com/2013/08/29/opinion/citron-revenge-porn

Duggan, M. (2014, October 22). Online harassment. Pew Research Center. Retrieved from http://www.pewinternet.org/2014/10/22/online-harassment

Faruqi, M. (2019, February 8). The abuse and hate I get when I speak out hurts—but shutting up isn't an option. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2019/feb/08/the-abuse-and-hate-i-get-when-i-speak-out-hurts-but-shutting-up-isnt-an-option

Gadsby, H. (2014, June 23). The 2014 Opening Night Comedy Allstars Supershow—Hannah Gadsby. *YouTube*. Retrieved from https://www.youtube.com/watch?v=JHVuQjlNh-Y

Gardiner, B., Mansfield, M., Anderson, I., Holder, J., Louter, D., & Ulmanu, M. (2016, April 12). The dark side of Guardian comments. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments

Henry, N., & Powell, A. (2015). Embodied harms: Gender, shame, and technology-facilitated sexual violence. *Violence Against Women, 21*(6), 758–799. doi:10.1177/1077801215576581

International Labour Organization (ILO). (2007). *ABC of women workers' rights and gender equality* (2nd ed.). Retrieved from http://www.ilo.org/wcmsp5/groups/public/---dgreports/---gender/documents/publication/wcms_087314.pdf

Jane, E. A. (2015). Flaming? What flaming? The pitfalls and potentials of researching online hostility. *Ethics and Information Technology, 17*(1), 65–87.

Jane, E. A. (2017a). Systemic misogyny exposed: Translating rapeglish from the manosphere with a random rape threat generator. *International Journal of Cultural Studies, 21*(6), 661–680. doi:10.1177/1367877917734042

Jane, E. A. (2017b). *Misogyny online: A short (and brutish) history*. Los Angeles, CA: Sage.

Jane, E. A. (2017c). Feminist fight and flight responses to gendered cyberhate. In M. Segrave & L. Vitis (Eds.), *Gender, technology and violence* (pp. 45–61). London, UK: Routledge.

Jane, E. A. (2017d). Gendered cyberhate: A new digital divide? In M. Ragnedda & G. W. Muschert (Eds.), *Theorizing digital divides* (pp. 158–198). Oxford, UK: Routledge.

Jane, E. A. (2018). Gendered cyberhate as workplace harassment and economic vandalism. *Feminist Media Studies, 18*(4), 575–591. doi:10.1080/14680777.2018.1447344

Jane, E. A., & Vincent, N. A. (2017, July 18). Women online are getting used to cyber hate: They need to get used to reporting it. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/lifestyle/news-and-views/opinion/women-online-are-getting-used-to-cyber-hate-they-need-to-get-used-to-reporting-it-20170717-gxctr8.html

Jane, E. A., & Vincent, N. A. (2018). Cyberhate and human rights. Submission in response to the Australian Human Rights Commission's Human Rights and Technology Issues Paper. Retrieved from https://tech.humanrights.gov.au/sites/default/files/inline-files/112%20-%20Nicole%20Vincent%20and%20Emma%20Jane.pdf

Mantilla, K. (2015). *Gendertrolling: How misogyny went viral*. Santa Barbara, CA: Praeger.

Nyst, C. (2014, August). End violence: Internet intermediaries and violence against women (Report by the Association for Progressive Communications for the "End violence: Women's rights and safety online project,"). Retrieved from https://www.apc.org/en/pubs/end-violence-internet-intermediaries-and-violence

Ostini, J., & Hopkins, S. (2015, April 8). Online harassment is a form of violence. *The Conversation*. Retrieved from https://theconversation.com/online-harassment-is-a-form-of-violence-38846

Penny, L. (2011, November 4). Laurie Penny: A woman's opinion is the mini-skirt of the internet. *Independent*. Retrieved from http://www.independent.co.uk/voices/commentators/laurie-penny-a-womans-opinion-is-the-mini-skirt-of-the-internet-6256946.html

Powell, A., & Henry, N. (2015). Digital harassment and abuse of adult Australians: A summary report. Tech & Me Project. Melbourne, Australia: RMIT University.

Provenzano, B. (2016, May 1). Amy Schumer's latest sketch takes on Twitter cyberbullying. *Mic*. Retrieved from https://mic.com/articles/142298/amy-schumer-s-latest-sketch-takes-on-twittercyberbullying#J7vhtRrDP

Sandoval, G. (2013, September 12). The end of kindness: Weev and the cult of the angry young man. *The Verge*. Retrieved from http://www.theverge.com/2013/9/12/4693710/the-end-of-kindness-weev-and-the-cult-of-the-angry-young-man

Smith, M. (2018, September 8). Four in ten female millennials have been sent an unsolicited penis photo. *YouGov UK*. Retrieved from https://yougov.co.uk/news/2018/02/16/four-ten-female-millennials-been-sent-dick-pic

UN Broadband Commission for Digital Development. (2015). Cyber violence against women and girls: A world-wide wake-up call (Report of the Working Group on Broadband and Gender). Retrieved from http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf

Vincent, N. A., & Jane, E. A. (2017a). Beyond law: Protecting victims through engineering and design. In E. Martellozzo & E. A. Jane (Eds.), *Cybercrime and its victims* (pp. 209–223). Oxford, UK: Routledge.

Vincent, N. A., & Jane, E. A. (2017b, July 18). A crime is a crime, even if it's online—here are six ways to stop cyberhate. *ABC News*. Retrieved from http://www.abc.net.au/news/2017-07-18/six-ways-to-stop-cyberhate/8721184

Vincent, N. A., Lindsay, D., & Potts, M. (2018). Human rights and technology issues paper: UTS submission. Submission by University of Technology Sydney in response to the Australian Human Rights Commission's *Human Rights and Technology Issues Paper*. Retrieved from https://tech.humanrights.gov.au/submissions?mc_cid=3526cb82bd&mc_eid=8328e29bcc

Web Index. (n.d.). *Web Index: Report 2014–15*. Retrieved from http://thewebindex.org/wp-content/uploads/2014/12/Web_Index_24pp_November2014.pdf

Further Reading

Jane, E. A. (2016). Online misogyny and feminist digilantism. *Continuum, 30*(3), 284–297. doi:10.1080/10304312.2016.1166560

Jouvenal, J. (2013, July 14). Stalkers use online ads as weapon against victims. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/i-live-in-fear-of-anyone-coming-to-my-door/2013/07/14/26c11442-e359-11e2-aef3-339619eab080_story.html

Martellozzo, E., & Jane, E. A. (Eds.). *Cybercrime and its victims*. Oxford, UK: Routledge.

Neary, B. (2010, June 29). 2nd man gets 60 years in Wyo. Internet rape case. *Ventura County Star*. Retrieved from http://www.vcstar.com/news/2nd-man-gets-60-years-in-wyo-internet-rape-case-ep-368408277-348997991.html

Phillips, W. (2015). *This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture*. Cambridge, MA: MIT Press.

Sarkeesian, A. (2012, July 1). Image based harassment and visual misogyny. *Feminist Frequency*. Retrieved from http://feministfrequency.com/2012/07/01/image-based-harassment-and-visual-misogyny

Segrave, M., & Vitis, L. (Eds.). (2014). *Gender, technology and violence*. London, UK: Routledge.
Smith, L. (2014, March 1). Domestic violence and online abuse: Half UK survivors experience trolling in "tidal wave of hate." *International Business Times*. Retrieved from http://www.ibtimes.co.uk/domestic-violence-online-abuse-half-uk-survivors-experience-trolling-tidal-wave-hate-1438420

Emma A. Jane, PhD, is an associate professor at UNSW, Sydney. She researches the social implications of emerging technologies using transdisciplinary methods to interrogate the issues and consider proposed interventions. Having previously led a major study on gendered cyberhate, her current projects include a study on radicalized misogyny and research into the future of sex and gender. Prior to her career in academia, she spent nearly 25 years working in the print, broadcast, and electronic media during which time she won multiple awards for her writing and investigative reporting. Her tenth book—*Misogyny Online: A Short (and Brutish) History*—was published by Sage in 2017.