laws

MDPI

Article

Online Shaming and the Right to Privacy

Emily B. Laidlaw

Faculty of Law, University of Calgary, 2500 University Dr. NW, Calgary, AB T2N 1N4, Canada; emily.laidlaw@ucalgary.ca

Academic Editor: Carys J. Craig
Received: 1 November 2016; Accepted: 21 January 2017; Published: 8 February 2017

Abstract: This paper advances privacy theory through examination of online shaming, focusing in particular on persecution by internet mobs. While shaming is nothing new, the technology used for modern shaming is new and evolving, making it a revealing lens through which to analyze points of analytical friction within and between traditional conceptions of privacy. To that end, this paper first explores the narrative and structure of online shaming, identifying broad categories of shaming of vigilantism, bullying, bigotry and gossiping, which are then used throughout the paper to evaluate different angles to the privacy problems raised. Second, this paper examines shaming through three dominant debates concerning privacy—privacy's link with dignity, the right to privacy in public places and the social dimension of privacy. Certain themes emerged from this analysis. A common feature of online shaming is public humiliation. A challenge is to differentiate between a humbling (rightly knocking someone down a peg for a social transgression) and a humiliation that is an affront to dignity (wrongly knocking someone down a peg). In addition, the privacy concern of shamed individuals is not necessarily about intrusion on seclusion or revelation of embarrassing information, but rather about the disruption in their ability to continue to participate in online spaces free from attack. The privacy interest therefore becomes more about enabling participation in social spaces, enabling connections and relationships to form, and about enabling identity-making. Public humiliation through shaming can disrupt all of these inviting closer scrutiny concerning how law can be used as an enabling rather than secluding tool.

Keywords: internet; technology; shame; abuse; privacy

1. Introduction

This paper examines the privacy implications of online shaming, in particular the issues raised concerning persecution by internet mobs. In the situations explored in this paper "the shamed" are mocked, bullied or otherwise harassed by other internet users sharing thousands of messages, posting photos or otherwise commenting directly to or about the shamed. Sometimes the shamed have committed a social transgression and the internet mobs use shame sanctions to enforce the norms of the online community: to condemn offensive or hateful posts, rein in gossip, expose lies, and so on. At other times, the shamed have not necessarily committed a social transgression, but are targets nonetheless, being doxed,[1] swatted[2] or otherwise exposed ([1], p. 9)[3] (i.e., revenge pornography) or harassed (i.e., stalking, blackmail, threats, and fake profiles) in a way that shames them. In the messy world in which we live, often the scenario for the shamed is a mix of the above.

The goal with this paper is to use the modern phenomenon of online shaming to illuminate weaknesses in dominant debates concerning privacy. Shaming is nothing new. Various historical

[1] Doxing is when people search for private information about an individual and then reveal it online.
[2] Swatting is when emergency services are called to a person's house based on a false report.
[3] Jacquet discusses exposure as being "the essence of shaming" ([1], p. 9).

references have been used to describe an episode of public shaming: a lynching, the stocks and pillories, floggings and scarlet letters [2–5].[4] Indeed, there is much commonality between modern online shaming and the shaming of offenders in the stocks and pillories in public squares. However, technology is evolving such that shaming is deployed differently, making it a useful lens though which to stress-test traditional conceptions of privacy. Using three common debates about privacy—privacy's link with dignity, the right to privacy in public places and the social dimension of privacy—this paper dissects their conceptual underpinnings in light of modern technology and identifies common themes of disruption to participation and connections online, and identity-making as caused by the public humiliation of shaming.

This paper does not seek to interrogate the meaning of shame or the general merit of shame sanctions [6–14].[5] Rather, this paper uses the regulatory given of online shaming as a launching pad to analyze what this means for our understanding of the meaning of privacy. For the purposes of this paper, shame is best described as "a form of social control" [7]. Eric Posner asserts that, "[i]t occurs when a person violates the norms of the community, and other people respond by publicly criticizing, avoiding, or ostracizing him" [7]. It is this external element of a public transgression/behaviour and social enforcement that differentiates shame from the more self-imposed feelings of guilt [1].[6] Guilt is falling short of your expectations of yourself, while shame is violation of a group norm. It has an audience ([1], pp. 9, 11–12). This definitional focus on the normative role of shame is apposite given that internet law scholarship is rich with analysis of the role of norms in regulating the online environment [15–20]. In this paper, through recognizing that norms play a crucial regulatory role online, one tool being shaming, it dissects what happens when shaming goes awry.

In some ways, online shaming is what has allowed a more open internet to exist. At its best, shaming can enforce rules of civility in online communities.[7] It can be a facilitative force for positive change.[8] Indeed, shaming is entrenched in our culture, particularly to address social wrongs seen as outside the reach of the law. Naming and shaming is a core regulatory tool to address human rights abuses. Shame campaigns against corporations for violating a perceived social or moral wrong is common, such as campaigns against sweat shops or concerning environmental standards. It is a common strategy to address regulation of internet-based companies, such as the campaign against Facebook for its refusal to shut down a rape joke group [21,22],[9] or boycott of the internet registration authority GoDaddy for supporting the Stop Online Privacy Act (SOPA) and the PROTECT IP Act (PIPA) [23],[10] or creation of fake Facebook groups to publicly test the quality of Facebook's application of its community standards [24].[11] At its worst, shaming is a brutal form of abuse, causing, among other things, social withdrawal, depression and anxiety ([1], p. 10, chap. 6). The ramifications of shame

---

4 On online shaming see ([3], chap. 4). For a history see Goldman [4].

5 For further information see the series of scholarly articles from the 1990s, which debated the value of shaming, although the focus was on government-sponsored sanctions, such as such as the use of shaming by the judiciary as an alternative to imprisonment [9–11]. This is observed in the case of Shawn Gementera, who was sentenced to, among other things, carry a sign with the words "I stole mail; this is my punishment" outside a postal facility: [6] discussed by Goldman in ([4], pp. 424–26). More subtle forms of shaming can also be observed, such as maintenance of criminal records, the use of public trials and perp walks [7]. See detailed overview of this history Klonick ([8], part C). For more recent discussion, see Nussbaum [12], Flanders [13] and Cheung [14].

6 See also Klonick ([8], p. 1033) noting the difficulty in defining shame in general.

7 See the famous story of the LambdaMOO virtual community detailed by Lessig ([17], pp. 97–102). For the virtues of shaming see Solove ([3], pp. 92–94).

8 Some argue that the value we place on privacy makes shaming effective as a deterrent, because fear of losing that privacy convinces individuals not to behave a particular way: see discussion of Goldman [4].

9 Various efforts to shame Facebook for its initial decision to allow these groups remain led the company to reverse its decision and revisit its policies.

10 Several users transferred to (or threatened to) a different registrar. GoDaddy acquiesced and withdrew support for SOPA/PIPA.

11 For example, Shurat HaDin—Israel Law Center set up two fake Facebook groups "Stop Palestinians" and "Stop Israelis". Over the course of two days increasingly severe incitements of hatred and violence were posted on both pages and then the group complained to Facebook. The company initially only shut down the "Stop Palestinians" page until the organization publicized the test.

sanctions are magnified when executed online, because the punishment can be disproportionate to the social transgression, the perpetrators anonymous and diffuse, and the reach of the shaming immediate, worldwide and memorialized in Google search results ([1], chap. 10).[12]

This paper takes a broad, contextual approach to the analysis. It examines legal responses in the United Kingdom, Europe, Canada and the United States of America, although it does not seek to be a complete comparative analysis. Rather, the various judicial responses to the problems posed by shaming are useful in highlighting the underlying privacy rationale that is the focus of this paper. To that end, I first examine the narrative and structure of online shaming, identifying categories of shaming that are then used throughout the paper to evaluate different angles to the privacy problems posed by shaming. Second, I analyze what shaming reveals about points of analytical friction concerning the core meaning of privacy. To put it another way, by analyzing the privacy interests raised by shaming, the limits of the free speech model are tested. The privacy debates most strained by shaming concern dignity, privacy in public and social privacy.

2. The Narrative of Online Shaming

I frame the categories of online shaming broadly, including activities that might traditionally be analyzed as distinct, particularly as some of the individuals involved are more sympathetic than others. Scholars such as Kate Klonick, for example, employ a narrow conception of shaming, differentiating shame from harassment and bullying because of the enforcement via social norms ([8], p. 1034). However, I suggest that shame can be an element of a wide variety of forms of abuse. In some ways, shaming is not any category, simply a tactic employed, to varying scales, in inflicting the abuse. For the purposes of this paper, this broader approach is key, because by throwing open the door categorically-speaking, we can identify and untangle the appropriate differentiating factors between a shaming that might raise privacy concerns versus a shaming that merely causes offense or enforces the norms of a community. In this way, we can explore how the privacy interest might be different between a bullied child, a guy cracking sexual jokes about dongles[13] and revenge pornography. For analytical use in this paper, I use four broad and overlapping categories of shaming: vigilantism, bullying, bigotry and gossiping.

2.1. Vigilantism

One of the most striking phenomena of social media is vigilantes outing individuals that break social and legal rules. The cast of characters are not all sympathetic here. These "social villains" [25], include Lindsey Stone, who jokingly made an offensive gesture in a photograph of the Arlington War Memorial, to Alicia Lynch who dressed as a Boston Marathon bombing victim for Halloween, to Mary Bale who was caught on CCTV throwing a cat into a wheelie bin. All actions are offensive, or at minimum, ill-advised, but in some cases the sanction was total obliteration of these individuals lives. The common theme is a perceived social wrong punished by the mob through public humiliation.

One of the best examples of shaming is the experience of Justine Sacco. On a layover in London on her way to South Africa, American public relations executive Sacco posted the following tweet: "Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!" [5][14] At first blush this seems to be a racist comment, and indeed while she was en route to South Africa, Twitterverse deemed it just so. Later, Sacco explained that her tweet was intended to make fun of the bubble in which Americans live ([15], p. 73). She only had 170 followers on Twitter, but her tweet was noticed by a blogger with 15,000 followers. He tweeted: "And Now, a Funny Holiday Joke From IAC's P.R. Boss" [26]. Unknown to Sacco, while in flight, she was bombarded with tens of thousands of angry tweets, many

---

[12] Klonick asserts that shaming features three things: unclear social meaning, uncalibrated effects, and inaccuracy ([8], p. 1045).
[13] See discussion, infra, the Structure of Online Shaming.
[14] The tweet has since been deleted, but can be found through any Google search. It is also discussed in Ronson [5].

including the hashtag #HasJustineLandedYet. By the time she landed she had been fired from her job, an advertisement posted for her old job by her former employer and several parody accounts created, such as @loljustinesacco (with the tag "PR Disaster. Racist idiot. All-around awful") [27].

The category here is even broader, including recruiting the internet mob to track down offenders. Sometimes this is organized by the masses, something Anne Cheung discusses as the *human flesh search engine* common in Asian countries to hunt down individuals who have broken social rules ([14], p. 304). Daniel Solove discussed this phenomenon in the context of "dog poop girl", the Korean woman who failed to clean up her dog feces on a train. A passenger took a photograph of the incident and posted it online. It went viral with individuals identifying her name, address and place of work. She was let go from her job and forced into hiding ([3], chap. 1). More recently, a Swedish television show *Troll Hunters* is devoted to exposing perpetrators of online abuse and publicly shaming them [28]. These forms of "crowd-sourced surveillance" [29] have been encouraged by the police. Notably, the Vancouver police asked the public to share videos and photos after a riot to help them in their task tracking down the perpetrators.[15]

2.2. Bullying

Cyber-bullying in some ways is an all-encompassing term for the shaming described in this paper. It has been defined as, "any behavior performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others" ([30], Robert Tokunaga quoted, p. 3). Its notable characteristics are repeated aggression over a period of time in a situation of unequal power ([8], p. 1034). It is identified as a separate category to tease out its differences, as will be seen, concerning the privacy issues of a person like Justine Sacco or the Vancouver rioters and some of the more traditional cases of children being bullied online.

Rehtaeh Parsons and Amanda Todd are two examples of cyber-bullying. A teenage Parsons was allegedly sexually assaulted at a party and the incident photographed and shared online. She was bullied on Facebook and via text. The Royal Canadian Mounted Police (RCMP) initially declined to prosecute the young men involved on the basis that there was insufficient evidence. Parsons committed suicide the next month. Two of the young men involved were charged and plead guilty to distribution of child pornography [31,32]. In the case of Amanda Todd, at the age of twelve she was coerced by a stranger online to show her breasts. The individual relentlessly bullied her for several years, sharing the photo with her classmates, teachers and parents. Todd was then bullied online and off by her classmates. This forced her to move schools twice, and each time the individual re-circulated the photo and the taunting started afresh. Todd posted a YouTube video detailing her suffering[16] and then committed suicide. In each situation the bullying was linked to the teenager's community.

I would include within this category retribution oriented mob attacks such as revenge pornography. This is exemplified by the story of Holly Jacobs, detailed by Danielle Keats Citron in her book *Hate Crimes in Cyberspace* ([35], pp. 45–50). She shared intimate images and video with her then-boyfriend. After they broke up he posted these images and videos on hundreds of sites, including personal information such as her name, email address and work details. She was hounded by individuals re-posting the information, contacting her work, creating fake Facebook profiles and the like. Some websites are entirely devoted to bullying through shaming, what Citron terms "crowd leaders" ([36], p. 48), such as www.cheaterville.com and www.thedirty.com. However, cases such as *Jones v Dirty World Entertainment Recordings LLC* [37] confirm their immunity from liability as intermediaries in the United States of America under s. 230 of the *Communications Decency Act* [38].

---

[15] So many individuals submitted information that it crashed the Vancouver Police Department's website.
[16] Her video is available on YouTube [33]. On her story see [34].

This category also applies to what is best described as the hounded, to individuals like Monica Lewinsky relentlessly discussed by the masses, where gossiping translates to bullying. Her affair with former President Bill Clinton was revealed by the Drudge Report making it one of the first stories broken online [39].[17] She describes the experience as, "I was patient zero of losing a personal reputation on a global scale almost instantaneously" [40], describing internet users as "mobs of virtual stone throwers" [40]. In the situation of revenge pornography and general hounding, the bullying is sometimes directed at individuals, while at other times the bullied are simply the topic of discussion.

2.3. Bigotry

This category concerns an identifiable group attacked on the basis of their race, gender, sexual orientation, religion, colour or ethnic origin. These are more classic cases of hate speech, explored further below, except in situations of online shaming the attack is executed by the mob, further stigmatizing and excluding the victims.[18] In the case of women, for example, they are the targets of 90% of revenge pornography [41].[19] A study by the Pew Internet Center Found that 40% of women report having been harassed online. A recent survey of over 1000 women in Australia found that 76% of women under 30 surveyed had experienced online harassment [43].[20] The Guardian newspaper analyzed 70 million comments left by users on its site and found that they had blocked 2% for violating their community standards. Of the top 10 abused writers, eight were women (four white, four non-white) and the remaining two were black men [44].[21]

This kind of gender based hate is evident in the case of *gamergate* in 2014 where female games developers and critics were attacked online with threats of death and rape, and in the case of Zoe Quinn, the sharing of intimate information and photos. In many cases the women were driven from their homes out of fear of attack [46,47]. The campaign against them was attributed to 4chan, 8chan and Reddit. Such attacks can be seen against other women, with threats of death and rape on Twitter against campaigner Caroline Criado-Perez for suggesting a woman should be the face of at least one of the British bank notes [48]. Two tweeters were convicted in the United Kingdom of extreme threats for such tweets as "Ya not that gd looking to rape u be fine" and "f*** off and die you worthless piece of crap" [49]. One of the most well-known cases involved comments posted on a message board on AutoAdmit concerning two female law students, with threats of rape (such as "I'll force myself on her, most definitely" and "I would like to hate-fuck [last student's name] but since people say she has herpes that might be a bad idea.") ([35], pp. 39–40), other disparaging and defamatory remarks, and intrusive comments detailing their daily activities [35,50].[22]

2.4. Gossiping

Gossiping is a rather murky category for the unthinking masses that re-tweet and share content without a care as to its accuracy. They are not necessarily the trolls that hounded Holly Jacobs or Zoe Quinn, but they are key figures in the pile-on. It is identified on its own category in this paper, because the machine of mob persecution online is dependent on their participation to thrive.

---

[17] See Rosen's discussion of privacy and Monica Lewinsky [39].

[18] As Nussbaum argues, the fallacy of shame justice is that "it is justice by the mob: the dominant group are asked to take delight in the discomfort of the excluded and stigmatized" ([12], p. 73).

[19] See discussion of a study by the Cyber Civil Rights Initiative in Citron and Franks [41]. In the case of domestic abuse, typically targeting women, victims service providers have reported that 97% of victims have been abused through misuse of technology, 95% through texting and 55% through posting online [42].

[20] Note that the term online harassment can be an umbrella for all sorts of unwanted behavior. The term was not defined in the study, at least in the material publicly available. The questions in the survey itself were not available to review [43].

[21] See more generally the excellent Guardian series "the web we want" [45].

[22] The situation was first discussed by Nakashima in a Washington Post article in 2007 [51]. The two students sued 39 posters and subpoenaed AutoAdmit and ISPs to identify the posters. Some were identified and the case later settled. Making a case in such situation will be more difficult in light of *Elonis v United States* [52].

The case of Lord McAlpine is particularly apposite here. In 2012 BBC Newsnight reported that a senior Conservative politician from the Thatcher era was involved in sexual abuse of children. Thousands took to Twitter to incorrectly link Lord McAlpine with this report, such as Sally Bercow, wife of the then Commons Speaker, who tweeted, "Why is Lord McAlpine trending. *innocent face*." Such tweets were retweeted by approximately 10,000 people. McAlpine sued several prominent individuals and offered to settle with any Twitter users with a following of less than 500 [53–56].[23]

Gossiping is not inherently bad. After all, two-thirds of all conversations are gossip ([1], p. 17). Rather, it can be a positive, pleasurable interaction. It is a way that individuals form social bonds, learn about cultural norms and establish their reputations ([3], chap. 3, in particular pp. 63–64). As Solove asserts, gossiping can be a way to enforce norms without direct confrontation thereby maintaining civil relations ([3], p. 64). However, gossip can be spread carelessly and can take on unwarranted authoritativeness given the questionable truth of the allegations. This is problematic when spread online, because of the ease of its circulation. It makes it easier to "judge out of context" ([3], p. 66) and reaches a greater audience than the more targeted nature of in-person gossip.

The ease with which online gossip destroys a person's reputation is exemplified in *Pritchard v Van Nes* [57], wherein the British Columbia Supreme Court awarded damages in defamation against the defendant not only for her Facebook post, but the comments of her friends.[24] She was, in effect, held liable for the pile-on. In her post, the defendant uploaded a photograph of the Plaintiff neighbour's backyard with comments falsely stating her neighbour spied on her and implying her neighbour was a pedophile. This prompted 48 comments by 36 of her friends, including nine further comments by the defendant ([57], para. 23). The comments referred to the plaintiff, a teacher, as "a 'pedo', 'creeper', 'nutter', freak', 'scumbag', 'peeper' and a 'douchebag'" ([57], para. 24), perpetuating the untrue pedophile accusation and implying the defendant was unfit to teach. The comments, which also identified the defendant by name, occupation and work ([57], para. 73), were viewable not only by the defendant's 2000+ friends and friends-of-friends, but the public, since the defendant did not use any privacy settings. The casualness with which these 36 individuals gossiped about the defendant, or what the plaintiff described as "venting" ([57], para. 41), is typical of an online take-down. For the targets, the damage can be wholesale. In this case, the plaintiff lost his enjoyment of teaching, withdrew from extra-curricular activities and experienced shunning in his community ([57], paras. 33–38).

3. The Structure of Online Shaming

A common thread in the categories above is that online shaming is a form of public humiliation. Privacy has struggled with how to handle humiliation and whether to handle it all. The point of interest concerning humiliation and privacy is the disconnect between the law, which tends to focus on individual offenses in the form of online comments, and the harm, which is often centred on the cumulative effect of the mob persecution. Caroline Criado-Perez describes her experience that way, stating, "I remember sitting in my flat, watching all these threats roll in, and it was horrifying, utterly shocking and scary. I didn't know who these people were and what they were capable of. It was relentless" [58].

If we dissect the comments made against Justine Sacco, for example, many are classically shaming comments, many angry and mean-spirited, rather than meeting the legal threshold of defamatory or threatening language. Comments made included, "Is that tweet real? You work in PR. You shld know better..." and "Justine Sacco should get fired...and get AIDS" and "I don't think America has watched a landing this closely since Apollo 13 re-entered the earth's atmosphere in 1970. #HasJustineLandedYet" [27]. What did her in was not the individual comments, but the sheer quantity

---

[23] In separate actions, Lord's McAlpine settled with the BBC, ITV, Sally Bercow and Alan Davies. Concerning the offer to Twitter users with less than 500 followers, see Branagh [56].

[24] Note that the Plaintiff had obtained default judgment, and the Court's reasoning here related to the plaintiff's application for a permanent injunction, assessment of damages and special costs.

and ferocity of them, and the narrative force of these tweets in re-casting her identity as one of the raging, idiotic racist. Within one day of the original tweet, it was re-tweeted 30,000 times and the hashtag #HasJustineLandedYet retweeted 100,000 times [27]. However, as the examples concerning AutoAdmit and Caroline Criado-Perez above illustrate, the cause of action, when available, is against individual posters for their contribution to the pile-on, thus the legal action is removed, to an extent, from the cumulative context of the harm.

Some acts of shaming, particularly in some cases of cyber-bullying, are strongly associated with the shamed's real-world community. In such situations, legal solutions, whether criminal or private, as against the shamer might be desirable.[25] If an individual can be identified, there might be a claim, depending on the jurisdiction, of criminal hate speech, defamation, infringement of copyright, use of a telecommunications device to abuse, threaten or harass a person, behaviour or words causing alarm or distress, or communications that are grossly offensive or obscene, harassment, stalking, or infringement of privacy as a tort claim.[26] However, for those that have suffered because of a shaming gone viral, these legal options are of limited use, whether because they do not address what is so harmful in the shaming, or the individuals cannot be identified, or there are too many to be able to easily identify, or even if they are identifiable, as in the case of Lord McAlpine, there are just too many involved in the wrongdoing to realistically pursue. This invites assessment of the liability of intermediaries, moving the focus away from the law punishing those morally culpable, to efforts to use gatekeepers unique power to control the online pathways of communication to halt the shaming as much as possible.

Cass Sunstein discusses the pile-on as *informational cascades*, wherein group members express their disapproval of certain conduct not necessarily based on their own judgment or knowledge of the situation, but rather by following the lead of others in the group ([68], pp. 92–93). In this way, the shaming takes place in a cascade. This is evident in the cases of Lord McAlpine and *Pritchard*. As Sunstein describes the spread of rumours:

> When rumors spread, it is often through a process in which they are accepted by people with low thresholds for acceptance, and eventually through others as well, simply because most people think that so many people cannot be wrong. A tipping point can be reached in which large numbers of people accept a false rumor even though it is quite baseless ([67], p. 93).

These informational cascades raise questions about the responsibilities of the participants, and the privacy implications of their shaming. Cheung comments, "what we have to guard against is not only Big Brother of the Orwellian state, but all the little dictators around us" ([69], p. 209). The internet is a particularly effective place to deploy shaming. In one way, shame sanctions have an important role to play online where laws can be easily circumvented and social norms have a weaker hold.[27] Shaming here has normative force in regulating the rules of behaviour in participating in an online space. Solove notes, "[i]n a world of increasingly rude and uncivil behavior, shaming helps society maintain its norms of civility and etiquette" ([3], p. 92).

This is the irony. It is the very weakening of norms in reining in some behaviour of users on social media that makes shame sanctions more powerful. As an example, while social norms might

---

[25] See here settlement of two of the young men in the Rehtaeh Parsons case for distribution of child pornography [31,32].

[26] See Citron [35] discussing the American context. In the United Kingdom, for example, a host of Acts have been re-purposed to target offensive and otherwise hateful comments on social media such as s 127 of the *Communications Act* [59] (and here see *Chambers v DPP* [60], s. 4A of the *Public Order Act* [61], the *Malicious Communications Act* [62] and the *Protection from Harassment Act*, 1977 c 40 [63]. In Canada, one can rely on, to name a few, s. 8 of the *Canadian Charter of Rights and Freedoms* [64], provisions in the Criminal Code [65] on hate speech, harassment, stalking and child pornography, or the recent amendment to the Criminal Code to criminalize the sharing of intimate images (this is the controversial Bill C-13 [66], or extension of traditional tort claims in trespass, nuisance or defamation to privacy issues. For more on some aspects of the Canadian context see Scassa [67].

[27] This draws from Lessig's work wherein he argues that, in the Internet context, laws can be circumvented, markets weakened and social norms less effective because of the remoteness of Internet communications, but regulation through architecture, in contrast, is strengthened [17,70].

have less of a hold on lolcat123 who pseudonymously posts racist comments about an individual on Twitter, online mobs have significant power in sanctioning lolcat123 for this behaviour. However, the remoteness, anonymity and pseudonymity that breed the abusive behaviour in the first place, also means there are few normative limits to the shame sanctions once the cascade is underway. It is easy for them to get out of control. You see this process unravel in the case of Amanda Todd. After she committed suicide, Anonymous wrongly identified a man as the instigator of the abuse, providing the public with his name and number. This man received thousands of communications, including death threats [71].

A more borderline example involves a sexual joke Jack Jones[28] made to his friend about dongles during a technology developers conference. It was overheard by Adria Richards, another audience member, who took a picture of the men and posted it on Twitter along with a message shaming them for the joke: "Not cool. Jokes about forking repo's in a sexual way and "big" dongles. Right behind me #pycon" ([5], p. 114). The tweet went viral and Jones was fired from his job. A mob then turned on Richards for what they saw as putting a father of three out of a job, threatening her in a variety of ways, including death and rape, and cyberattacking her employer's computer systems. She too was then fired from her job. As Klonick describes this scenario, "sometimes certain norm enforcement actions will violate norms themselves, and in turn be shamed" ([8], p. 1057).

Was this shaming doing good work or shaming out of control? The shaming of Richards tipped into the territory of criminal harassment, but the interaction leading up to that point is more debatable. Jennifer Jacquet makes the case for shame sanctions, but only in a narrow set of circumstances she describes as "the sweet spot of shame" ([1], chap. 10), when it has the potential to change behavior ([1], p. 79). She identifies seven characteristics:

> The transgression should (1) concern the audience; (2) deviate widely from desired behavior; and (3) not be expected to be formally punished. The transgressor should (4) be sensitive to the group doing the shaming. And the shaming should (5) come from a respected source, (6) be directed where possible benefits are highest and (7) be implemented conscientiously ([1], p. 173).

The shaming of both Jones and Richards arguably failed these criteria, but much online shame would. The kind of shaming that Jacquet advocates is coordinated and targeted, such as the work of Greenpeace in advocating for changes in behaviour to protect the environment.[29] Effective online shaming can be observed, as detailed by Klonick, in the #manspreading campaign ([8], pp. 1055–57), a feminist campaign of unknown origins that advocated against men taking up too much room on public transportation seats. Part of its effectiveness is it targeted the act of manspreading rather than individuals ([8], p. 1057), executed using many of the criteria outlined by Jacquet above.[30] What is evident is that social norms when deployed in mobs can be powerful in social media, but because social norms are also weakened in cyberspace the line between abuse and enforcement of etiquette can be quite grey.

4. Privacy

In a typical shaming, the shamed has engaged in ill-advised public conduct that the vigilantes have deemed worthy of disapproval. In such a scenario, the privacy nugget engaged tends to be the sense of unfairness about the publicity the situation receives. In the typical case of bullying, the shamed never asked for the attention in the first place. Here the scenario is slightly different. Images might

---

[28] The identity of the men involved is not known. For further discussion see Ronson ([5], chap. 6) and Klonick ([8], in particular, pp. 1030–31).

[29] Greenpeace was used as a repeated example of an effective shamer in Jacquet ([1], chap. 6).

[30] This is observable in the latter days of the campaign when, for example, transport services began issuing advisories on manspreading as well ([8], p. 1056). Another example is #congratsyouhaveanallmalepanel drawing attention to all male conference panels [72].

have been shared privately between willing partners and then shared by without permission to the world, or individuals accosted and bullied without provoking. In the case of bigotry and gossiping, individuals might be hounded day and night with comments of hate, offense or simple curiosity. In such cases the complaint tends to be "I just want to be left alone" or "this isn't who I am". In many of these cases, "this isn't who I am" is tied up with "this isn't true". Once Google is involved, the shaming is petrified. Author Jon Ronson recounts from his interview with Justine Sacco: "[a]nd the worst thing, Justine said, the thing that made her feel most helpless, was her lack of control over the Google search results. They were just there, eternal, crushing" ([5], p. 204). For any of the above, once Google becomes involved, the privacy aspect engaged seems to be, "I just want this to all go away", or more specifically, "I want Google to forget".[31]

There are many aspects to privacy, and this paper interrogates three of the most common debates: dignity, privacy in public places and social privacy. The working hypothesis is that privacy, whether in law or otherwise, needs to better account for public humiliation. This concern is captured by Cheung's broad definition of privacy, which is as follows:

> At its core, privacy is about the 'right to be let alone', the right to remain anonymous, and freedom from being targeted. In a relational context, therefore, privacy is about how to achieve decent participation in the cyber world, and how to safeguard autonomy and dignity in one's life against the powerful social moral force of monitoring and enduring sanctions exercised through the internet ([69], pp. 194–95).

In this definition one can see the intertwining of dignity, identity and sociality as aspects of the claim to the right to privacy, particularly in public places.[32] These aspects of privacy will be teased out and explored in turn, with a particular focus on privacy and dignity.

4.1. Privacy and Dignity

Online shaming illuminates dignity as an aspect of what it means to claim a right to privacy. The concept of dignity is woven through international human rights instruments, such as the Universal Declaration of Human Rights [76], the Charter of Fundamental Rights of the European Union [77] and the Charter of the United Nations without any explanation of what it means to violate someone's dignity [78].[33] A compelling account of dignity is by David Luban in the context of legal ethics where he writes: "[c]ertain ways of treating people humiliates them; humiliating people denies them their dignity" ([78], pp. 71–72). He differentiates autonomy from dignity as follows:

> Autonomy focuses on just one human faculty, the will, and identifying dignity with autonomy likewise identifies human dignity with willing and choosing. This, I believe, is a truncated view of humanity and human experience. Honoring someone's human dignity means honoring their being, not merely their willing. Their being transcends the choices they make. It includes the way they experience the world—their perceptions, their passions and sufferings, their reflections, their relationships and commitments, what they care about ([78], p. 76).

This account of dignity and autonomy resonates concerning online shaming. A common complaint of the shamed is the utter humiliation they feel, and in the case of some individuals this shame goes

---

[31] This opens the debate concerning a right to be delisted from search results (more broadly debated as the right to be forgotten) addressed in a data protection context in *Google Spain SL, Google Inc.v Agencia Espanola de Proteccion de Datos, Marios Costeja Gonzalez* [73]. The risks of such an environment of perfect remembering were earlier examined by Viktor Mayer-Shonberger, *Delete: The Virtue of Forgetting in the Digital Age* [74].

[32] Indeed Lisa Austin frames the process as "social" ([75], pp. 15–16).

[33] David Luban asserts that this was done on purpose for fear of going down the philosophical rabbit-hole and never emerging to reach consensus when drafting the UDHR. He commented, "the invocation of human dignity in human rights documents does no conceptual work in explaining what rights everyone ought to have" ([78], p. 68).

to the core of their sense of a life worth living. The response of some has been that some of these individuals should not have taken the intimate photo in the first place, or posted the stupid comment, or been caught doing something they should not have been doing. This is rooted in a focus on autonomy, that the individual was somehow in a position of control to negotiate the boundaries of what was revealed or not revealed about them.[34] Indeed, this also assumes that the privacy harm was revelation of information rather than rooted in being the target of bullying, which is the case for many shamed, and it further stigmatizes and harms the victim to suggest that social withdrawal or isolation is the preferred solution. For many, the privacy interest is to go about their lives free from being the target of attacks. This aspect of privacy in public will be discussed below. For now, it is suggested that autonomy, while of appeal in some situations, is of limited service to address online shaming.

This does not mean there is no place for autonomy in privacy discussions. Indeed, many countries, such as Canada, analyze privacy in terms of both [79,80]. It is recognized that historically autonomy has had a stronger pull on the American judicial and social consciousness. James Whitman provides a compelling comparative account of the privacy histories of continental Europe and America. He shows that continental Europe roots privacy in the protection of dignity, in protection from public exposure and humiliation. In this way European rights are focused on the right to control information disclosure, and the right to control one's image or reputation. In contrast, America's core privacy protection is rooted in liberty ([81], p. 1161). As Whitman describes it, America's primary privacy anxiety relates to "maintaining a kind of private sovereignty within our walls" ([81], p. 1162) and this translates in law to the right to be free from state intrusions ([81], pp. 1161–62). There is no need to resolve these differing approaches here. It is more modestly argued here that online shaming illuminates that dignity reflects some part of what it means to have one's privacy invaded.

Luban's concept of dignity is more narrowly linked with status rather than worth. On this point I disagree with him. Rather, I favour approaching dignity as a core aspect of one's self-worth. As Ari Waldman explains, "[i]f privacy is essential to who we are as free selves, then a right to privacy need not wait for a physical intrusion into a private space or a revelation of a stigmatizing private fact" ([82], p. 583). Luban's narrower focus, however, has analytical merit when attempting to differentiate the nature of the privacy rights of a Justine Sacco versus a case of cyber-bullying against an Amanda Todd. In linking dignity with status, Luban asks the question whether the humiliation *rightly* or *wrongly* knocks a person down a peg. He differentiates it in terms of being humbled (*rightly* knocked down a peg) and humiliated (*wrongly* knocked down a peg) ([78], pp. 88–89). Under this formulation of dignity, Justine Sacco or Lindsey Stone would have simply been humbled, at least in the eyes of some, rightly taken down a peg for a stupid, offensive post. To be consistent with Luban's conception invites the question: at what point, if at all, did the humbling of Justine Sacco or Lindsey Stone become a humiliation and therefore an affront to their dignity?

In contrast, in the case of traditional cyber-bullying, such as against Amanda Todd, or revenge pornography as in the case of Holly Jacobs, the attack was always a humiliation, it was always an affront to her dignity. In the case of Lord McAlpine, the humiliation was wrong from the beginning and is captured, unlike many cases of shaming, under the umbrella of defamation law. Analytically, Luban's approach is better at creating space for different treatments of online shaming, leaving more room for public discourse and free speech, and arguably the issue of dignity is only triggered when the discourse becomes out of control. This is the catch: how can we identify the tipping point on slippery slope of when such speech goes from being *right* to *wrong*?

Luban concludes, "[t]o violate someone's human dignity means to treat them as if they were a being of lower rank—as an animal, as a handy but disposable tool, as property, as an object, as a subhuman, as an overgrown child, as nothing at all" ([78], p. 89). One of the problems with shaming online is that with the remoteness of computer communications everyone is more readily seen as a

---

[34] See related discussion by Austin ([75], pp. 24–25).

caricature, an object and subhuman. The social norms we might normally rely on to regulate this kind of behaviour are weakened in cyberspace and yet the ease with which shaming is executed online is strengthened. In this way, Luban perhaps overstates the argument that dignity is better linked with status rather than self-worth. Rather, it can be see as two tiers. Avishai Margalit approaches it in this way, differentiating between "privacy as a constitutive element of human status, and privacy as a constitutive element of human flourishing. One is concerned with human life, the other with a good human life" ([83], p. 256).

We can flesh out this idea of privacy and dignity in another way. An online shaming often involves taking information out of its proper context, raising the "but that isn't who I am" claim of the shamed. Jeffrey Rosen captures this idea, although he does not frame it in terms of identity, when he states, "privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge" ([84], p. 8). However, Rosen gears the significance of this statement to situations where private information is revealed in public without the subject's permission ([85], p. 211). This only captures some of the shamed situations explored above. Rosen's reasoning is that if information is already public you have an opportunity to correct the narrative. However, mob persecutions on social media carry their own narrative force and it is difficult for the shamed to intervene to recast the story in a different, truer, light. He does note, however, that the ability to correct a misjudgement depends on one's ability to keep people's attention. His argument is more subtle, focusing on control over sharing of information in other contexts in a way that might lead to misjudgements: "it is the involuntary wrenching out of context of personal information that itself constitutes an offense against privacy and causes the related injuries I have described –against understanding, dignity, and autonomy" ([85], p. 216).

Privacy as dignity, it is suggested, can be seen as an enabling force in leading the good life, an authentic life ([86], pp. 146–47).[35] Lisa Austin harnesses this when she argues privacy insulates us from the social pressure of shame. The shame is not about what should or should not be exposed about a person from the viewpoint of society, but rather about that person's core sense of what his or her identity is [75].[36] Austin talks about it in terms of self-presentation—that we experience shame when how we want to present ourselves to the world is different than how we are being presented and we form a negative judgment from that ([75], pp. 10–11). She states, "instead of linking privacy to the protection of things that one "ought" to be ashamed of if exposed, the view defended here links privacy to protection from being seen in ways that one does not wish to be seen" ([75], p. 12).

This can be seen in Sacco's comment to Ronson: "[a]ll of a sudden you don't know what you're supposed to do," she said. "If I don't start making steps to reclaim my identity and remind myself of who I am on a daily basis, then I might lose myself" [87]. Identity, here, can be seen as a narrative, "an individual story that each person needs to build, develop and rewrite over time in order to define the meaning of their lives" ([88], p. 432).[37] Shaming can be seen to disrupt the narrative of our identity-making. People behave differently in different context ([39], p. 170), yet much of the shaming we see online does not allow for this.[38]

Privacy is compelling described as a "safe zone" as argued by Justice Karakatsanis in dissent in *R v Fearon* ([80], para. 109), and in this space one can explore who you are or want to be, your likes and dislikes, ideas, humour and self. What is social media to this space? We cannot describe it as freedom "to ponder outside the human gaze" ([80], para. 114), which focuses on privacy as seclusion. Rather, the desire is the freedom to participate *within* the public gaze. Even in cases of

---

[35] This was also quoted in *Fearon* ([80], para. 114).

[36] She also notes we can overcome many of the cultural difference that have been identified by scholars between the European notion of dignity as the root of privacy and the American notion of autonomy as the root of privacy ([86], pp. 34–35).

[37] See also discussion in Bernal ([89], chap. 9).

[38] Nissenbaum argues that privacy should be thought of in terms of contextual integrity, meaning that "a privacy violation has occurred when either contextual norms of appropriateness or norms of flow have been breached" ([90], p. 125).

traditional cyber-bullying, the victims want freedom to participate in the space with a safe zone of dignity surrounding them. This shifts the focus outward, to arguments that privacy protection can be deployed through civility rules.[39] The question is how can you manufacture it or impose it? Enforced etiquette? Moderation?[40] The problem with persecution by the mob is that the offenders are at once individuals, and the group as a whole.

A related approach is the argument of Whitman that shaming (in the context of state sanctioned shaming) infringe what he calls "transactional dignity" ([11], p. 1090). It is related to this outward focus above in the sense that he distinguishes bodily and status dignity from this "marketplace dignity" ([11], p. 1090):

> It is the dignity involved in having the right to know what kind of a deal one has struck, and on what terms. It is the dignity of the one-shot transaction-the dignity that arises from our marketplace right to complete one deal and move on to the next one, the dignity that comes from our right to pay off a debt once and for all and be done with our creditor ([11], p. 1090).

The offence, he argues, is the unpredictability of shame sanctions. Online sanctions lack the government approval that Whitman was arguing against. Rather, the mob persecutions online often develop organically. However, the platforms that offer the spaces to interact, such as Twitter, arguably are robbing[41] their users of transactional dignity without having in place policies to attempt to address the problem of online shaming.

A natural point of reflection is hate speech as some of the shaming that is perpetrated on social media is hate speech. Additionally, the harm of a social media shaming mimics the harm of hate speech even when it does not entirely align with it. In countries like Canada, with stronger hate speech laws, dignity has long been accepted as the heart of such laws. In *R v Keegstra* [92], the Supreme Court of Canada commented

> The derision, hostility and abuse encouraged by hate propaganda...have a severely negative impact on the individual's sense of self-worth and acceptance. This impact may cause target group members to take drastic measures in reaction, perhaps avoiding activities which bring them in contact with non-group members or adopting attitudes and postures directed towards blending in with the majority. Such consequences bear heavily in a nation that prides itself on tolerance and the fostering of human dignity through, among other things, respect for the many racial, religious, and cultural groups in our society [92].[42]

Jeremy Waldron pushes this argument further stating that when it comes to hate speech, dignity requires public assurance you will be treated justly or decently. It is this element of degradation, experienced as humiliation, that is common to hate speech and online shaming.[43]

A further issue to be teased out is exactly what is different between attacking one's dignity and causing offense. Here I suggest there is analytical similarity with humbling (*rightly* knocked down a peg) versus humiliating individuals (*wrongly* knocked down a peg) ([78], pp. 88–89). Waldron states that, in the context of hate speech, the difference between dignity and offense is between an objective assessment of someone's social status versus subjective feelings of hurt or anger ([93], pp. 106–7). This links with defamatory principles concerning status and reputation.

When examining the bullying of teenager Rehtaeh Parsons, the abusive comments and photos, would objectively lower her in the eyes of society, but it is more than that. Right-thinking members

---

[39] See Whitman for a discussion of the arguments of Robert Post ([81], p. 1167).
[40] See analysis of the virtues of moderation see Grimmelmann [91].
[41] Whitman used this language, stating that "[w]hen the state turns an offender over to the public, it robs him of that transactional dignity" ([11], p. 1090).
[42] See also discussion by Waldron ([93], pp. 84–85) about the significance of Dickson CJ's reasoning in *Keegstra*.
[43] See discussion by Waldron of the similarities between degrading treatment and hate speech ([93], p. 109).

of society might see through the horrors of what was shared and in that way her reputation spared. What was not spared was the humiliation. Therefore, a further distinction can be made between humiliation and hurt feelings. Lindsey Stone might be initially hurt that she has been called-out by the Twitterverse for her unthinking photo and then as the groundswell of disapproval grew, her reputation and status were harmed. In her case it was the sheer size of the mob attack that arguably shifted the event to a humiliation. In the case of Parsons or the women in *gamergate*, the relentless and degrading treatment by the mob is more about the right to "decent treatment in society" ([93], p. 107), to notions of "one's right to live privately, away from unwanted attention, to pursue freely the development and fulfillment of one's personality," ([14], p. 316)[44] rather than people saying mean things, which is individualized, and reparable feelings of discomfort and hurt, or, to borrow from *Handyside v United Kingdom* [95], invokes free speech questions concerning the right to "offend, shock or disturb" ([95], para. 49). Stemming from this analysis of dignity, part of the way that public humiliation can be accounted for in the right to privacy is the analysis of the publicness of the shaming, and thus the right to privacy in public places.

4.2. Privacy in Public

One of the issues with the privacy engaged here is that it involves the concept of public privacy. Indeed many of the individuals who have been shamed had put themselves out there by participating in the discursive spaces online ([69], p. 193). The question is whether that should be the end of it analytically—the act of participating online closes down the privacy claim. I suggest this would be a truncated approach to privacy; it is the very publicness of the spectacle that feeds the feelings of humiliation by sharing it with a wider audience.[45] Monica Lewinsky explained her experience this way as being "humiliated to death" [40]. A common argument advanced is that if people do not like what is being said online or in certain communities online, they should just go somewhere else. To the shamed, the question might be "why do I have to leave" or "how am I supposed to not go online". Traditionally, the law does little to account for privacy in public places, particularly in America. Europe, and to a lesser extent Canada, have been more open to the right to privacy in public.

American tort law sets out four different privacy torts: intrusion on seclusion, publication of private facts, false light invasion of privacy and appropriation of personality ([97], §652).[46] In a public context, this has left little wiggle room for a claim to privacy in a public place, unless there is harassment or stalking ([99], pp. 9–10). This is exemplified in the case of *Moreno v Hanford Sentinel, Inc.* [100][47] where Cynthia Moreno, a university student, posted an "Ode to Coalinga" on her MySpace account under her first name. The Ode was a negative commentary about her hometown. The Coalinga High School principal saw the Ode and passed it to the local newspaper where it was published and cited to Moreno using her full name. Her family received death threats, a shot was fired at their house and they were forced to move from the town. The Court of Appeal rejected a tort claim of public disclosure of private facts, because by choosing to post information on MySpace the information was already public:

> [A] crucial ingredient of the applicable invasion of privacy cause of action is a public disclosure of private facts. A matter that is already public or that has previously become part of the public domain is not private...Here, Cynthia publicized her opinions about Coalinga by posting the Ode on myspace.com, a hugely popular internet site. Cynthia's

---

[44] Here Cheung was discussing the European Court of Human Right's interpretation of the meaning of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 in *Sidabras and Dziatuas v Lithuania* [94].

[45] Moreham discusses the risks to privacy related to wider dissemination of a photography ([96], p. 621–23).

[46] These torts were identified by William Prosser, and not without criticism, one of which is the failure to include breach of confidentiality in the mix. See discussion of Waldman ([82], pp. 617–18) and Solove and Richards [98].

[47] See discussion in Cheung ([69], pp. 197–98, 204) and Richardson et al. [101].

> affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material [100].

The message of such a case is that once information is posted publicly online, there can be no privacy claim.[48]

In Canada we are in the nascent stage of developing a tort of invasion of privacy, with most of the focus thus far on intrusion on seclusion rather than privacy in public places. The Ontario Court of Appeal in *Jones v Tsige* [102] introduced the four torts in the U.S. Restatement (Second) of Torts [97] into Canadian law. The Court held the defendant liable for the first tort, intrusion on seclusion, because she used her position as a bank employee to look up bank records of her partner's ex-spouse. Since *Jones*, other Canadian courts have applied the tort of intrusion on seclusion ([103], chap. 8), and more recently in *Doe 464533 v ND* [104], the Ontario Superior Court applied the second tort, revelation of private facts, to a case of revenge pornography. In *Doe*, the defendant was found liable for posting photographs of his ex-girlfriend on a pornography site.

The public shame surrounding revenge pornography has been a particularly effective mobilizing force in spurring legislative action in Canada.[49] The *Criminal Code* was amended in 2014 to add an offense of sharing intimate images ([65], s. 162.1).[50] Nova Scotia introduced a *Cyber-safety Act* [106],[51] although the Act was struck down for infringing the *Canada Charter of Rights and Freedoms* [64] for its overly broad definition of cyber-bullying [108].[52] More recently, Manitoba introduced the *Intimate Image Protection Act* [109], which created a tort of non-consensual distribution of intimate images.

More generally for privacy concerns, Canadian courts have tended to simply extend traditional torts of nuisance, trespass and defamation to account for privacy concerns ([103], pp. 30–34). It is unclear whether Canadian courts, in the future, might be more open to some form of a right to privacy in public places, perhaps encouraged by the developing case law stemming from *Jones*. Historically, however, the courts have tended to provide minimal protections in public places ([67], p. 2). In a constitutional context, the Supreme Court of Canada recognized that in certain circumstances one can have a right to privacy in public places [110],[53] although the case was rooted in the context of the Québec *Charter*, which provides for a right to one's image.

The United Kingdom has been more open to a right to privacy in public with seminal cases such as *Campbell v MGN Ltd.* [111], although the legal hook in this case was the particularly invasive nature of photographs in revealing personal information. The Daily Mirror published numerous articles revealing that Naomi Campbell was receiving treatment for drug abuse. The articles included a photograph of her leaving a Narcotics Anonymous meeting as well as details of her treatment. She had previously publicly denied that she was a recovering drug addict. The majority of the House of Lords considered there to be a public interest in revealing the fact that she was in recovery, but concluded that the fact that she was receiving treatment from Narcotics Anonymous, including details of that treatment and a photograph, amounted to an invasion of privacy. The focus, therefore, became the particularly intrusive nature of photographs.

---

[48] As Paton-Simpson explains, "[t]he message of these cases is, once reasonable people venture outside the safety of their own homes, they must expect that they may be followed, filmed, investigated and spied upon, by any person for any purpose" ([99], p. 4).

[49] The United Kingdom has also enacted legislation, which addresses revenge pornography. Section 33 of the *Criminal Justice and Courts Act* [105] makes it an offence, in certain circumstances, to disclose private sexual photographs or film.

[50] This puts aside, for the moment, an assessment of the flaws in the Bill C-13 [66], in particular the surveillance provisions. The provision criminalizing sharing of intimate images is sound, although it is of more use to adults than minors.

[51] Nova Scotia's Justice Department is currently drafting a new cyberbullying act: see [107].

[52] The Act included, for example, damage to self-esteem and emotional well-being in the definition of cyber-bullying ([106], s. 3(1)(b)). The judge criticized the definition as a "colossal failure" ([108], para. 165), and since the law centred around this definition, the Act in its entirety was struck down.

[53] See also discussion by Moreham ([96], p. 632).

Campbell extended the traditional tort of breach of confidence to what is now known in the United Kingdom as misuse of private information ([111], para. 14).[54] While the analysis in the case concerns the more traditional issue of revelation of private information, evident in the Lords reasoning is protection of one's dignity as a theoretical underpinning of the right to privacy. Baroness Hale, for example, noted the private nature of one's health information and the risk in publishing Campbell's attendance at the Narcotics Anonymous, not only in potentially dissuading her and others like her from seeking treatment, but for the distress it caused ([111], paras. 157–58). In this way, although unsaid, there is a greater social value in protecting this privacy. On public privacy, Lord Hoffmann stated,

> [T]he widespread publication of a photograph of someone which reveals him to be in a situation of humiliation or severe embarrassment, even if taken in a public place, may be an infringement of the privacy of his personal information. Likewise, the publication of a photograph taken by intrusion into a private place (for example, by a long distance lens) may in itself be such an infringement, even if there is nothing embarrassing about the picture itself ([111], para. 75).

Lord Hoffmann was still unconvinced Campbell had a privacy claim concerning the photographs, because in his view, the photograph added nothing to the text of the story, however on this the majority of Lords disagreed. The question for the majority was ultimately as to the content of the photograph and nature of the activity involved. Lord Hope of Craighead stated the question is whether publishing the photo will be offensive ([111], para. 122). Baroness Hale framed it as a question of whether the activity photographed was private ([111], para. 154). The focus on the essentially private nature of the activity in question makes it difficult to claim a right to public privacy concerning some aspects of online shaming, although it is useful to address some cases of cyber-bullying.

In contrast, Justice Eady in *The Author of a Blog v Times Newspapers Ltd.* [113] held that blogging was "essentially a public rather than a private activity" ([113], para. 11), even when done pseudonymously, and therefore there was no right to anonymity. In this case the Times Newspaper identified a police officer as the pseudonymous writer NightJack of a popular blog about police life in Lancashire. It was later revealed that hacking was involved in ascertaining the blogger's identity, but at the time of this application it was presented as typical investigative work through internet sources ([113], para. 3).[55] The Court noted that *Campbell* involved the revelation of personal information, unlike the situation here where the only information sought to keep private was the blogger's identity. Eady concluded:

> Those who wish to hold forth to the public by this means often take steps to disguise their authorship but it is in my judgment a significantly further step to argue, if others are able to deduce their identity, that they should be restrained by law from revealing it ([113], para. 9).

Ultimately, the Court held the author was more akin to an undercover journalist, who has no reasonable expectation of privacy concerning his or her identity ([113], paras. 10–11). This indicates a narrow reading of *Campbell*—that the privacy interest is more about the revelation of personal information than a broader right to privacy in public places. Megan Richardson *et al*, identify a similar privacy loss for the litigants in *Moreno* and *Author of a Blog*, a loss of an ability to carve out a space for private communications online:

> [M]any of those who engage with the internet may hope and imagine that their private communications with their chosen audience will somehow 'take place' beyond the observation of others; yet they find it difficult to delimit a place that will permit them the privacy they desire in the boundlessness of cyberspace ([101], p. 9).

---

[54] In *Judith Vidal-Hall & ors v Google Inc.* [112], the Court concluded that misuse of private information is a distinct tort from breach of confidence.

[55] For discussion of the revelation at the Leveson Inquiry of the hacking see Richardson et al. ([101], p. 1).

In these cases the focus was on the right of the user to control the boundary between public and private online, while the European Court of Human Rights (ECtHR) has been more open to protecting a broader right of public privacy.

Dignity and identity are arguably the analytical foundation that has allowed a public privacy right to develop under ECtHR jurisprudence. In *von Hannover v Germany* No. 1 [114] and No. 2 [115], for example, the ECtHR examined the right to privacy of princess Caroline of Monaco concerning photographs published of her, sometimes with her children, in various German magazines. The cases are distinguishable from many of the acts of online shaming analyzed here, because Princess Caroline is a public figure, therefore there is more of a general public interest in information about her and her family. Her wish to stop the revelation of particular information, in this case photographs detailing her daily life, is a different beast than online shaming. It is not inherently degrading and humiliating the way a public pile-on is, and does not engage as closely the social interaction involved, which is examined in the following section.

The cases are notable, however, because the Court considered going about one's daily life to be something of an essentially private nature: "the photos of the applicant in the various German magazines show her in scenes from her daily life, thus engaged in activities of a purely private nature such as practising sport, out walking, leaving a restaurant or on holiday" ([114], para. 61).[56] In this way, one does not forfeit the right to privacy just because you exist out in the world. In *von Hannover* no. 2, the ECtHR reiterated this point more broadly, stating, "[t]here is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life" ([115], para. 95).[57]

The tendency in the cases is to look at whether there is a reasonable expectation of privacy in the circumstances. Scholars have questioned the application of this concept to public privacy [14,99]. Elizabeth Paton-Simpson interrogates it on normative and descriptive grounds. Normatively, she states it assumes that people venture into public without any expectation of privacy at all, and that they carefully keep private from this public world what they do not want revealed. The assumption is that people have a choice in this scenario and waive their right to privacy when they leave their home and fail to take privacy-protecting precautions. Descriptively, it assumes that people expect more privacy in their home than in public. Perhaps this is true, but she asserts this is a matter of degree, noting people do not tend to expect they will be observed any more than in a casual manner [99].

Waldman similarly explores the example of staring, arguing that staring feels like an invasion of privacy and yet involves no disclosure of information. He asserts that a violation of social trust is at the root of the privacy infringement, "our trust that no one will turn us into objects of gawking expression and leering eyes" ([82], p. 599). The social nature of this trust will be discussed in the following section on social privacy. This line between casual glances and gawking was articulated by ECtHR in *Peck v United Kingdom* [116], a case where CCTV footage was aired on TV showing the claimant walking down an alleyway moments after having attempted suicide. The Court commented, "the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation...and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995" ([116], para. 62).

Despite the publicness of Twitter, Sacco only had 170 followers, yet one re-tweet and her public expanded to 15,000 users and snowballed from there. In cases such as Rehtaeah Parsons, deeply personal information or images were shared with the public, reflecting a more traditional conception of privacy as unwanted revelation of personal information. However, once it was out there a frenzied mob discussion of their private lives ensued, deepening the harm suffered. Here arguments of scholars such as Citron are particularly compelling, that cybermobs can be addressed

---

[56] See also discussion in Moreham ([96], pp. 607–8).
[57] This was also stated in *Peck v United Kingdom* ([116], para. 57).

by supplementing traditional law with civil rights laws that better account for the psychic damage inflicted ([35], chap. 5; [36], pp. 39–49).

If one participates on Twitter it is arguable you assume you have no privacy in the space. There is no "zone of interaction" ([115], para. 95) that can be characterized as private, except for private messaging. However, the public humiliation possible on Twitter invites a different analysis of this public space. Rather, the concern is with notions of dignity and identity. One approach is to see the publicness of the space as not an impediment when dignity issues are engaged, rather as a factor to consider on a continuum from public to private. This thinking can be seen in *von Hannover*, discussed as the idea of integrity. The Court held that the princess had a right to privacy, despite the fact that the nature of the activities in public was not sensitive or embarrassing, in order to protect "one's physical and psychological integrity" ([114], para. 50).[58] The reasoning of the Court was that the primary purpose of the right to private life in Article 8 of the European Convention on Human Rights [117] was "to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings" ([114], para. 50).

Two trends in analysis are evident. First, in most cases, the focus of the analysis was on the private or public nature of the activity or space, the efforts at seclusion or anonymity, and the social norms that govern the space.[59] A Twitter account is normally public, but depending on one's privacy settings a Facebook account or group might be closed. In 2014, a group of male Dalhousie Dentistry students who were members of a closed Facebook group called "Class of DDS 2015 Gentlemen" were publicly shamed for a series of misogynistic comments.[60] This raises the question of whether these students had a reasonable expectation of privacy in a closed group or is the assumption that everything we post online is public (legally rather than shrewdly).[61] If the assumption is that it is public regardless of the privacy settings employed, then the intellectual distinction between public and private, at least in an online context, crumbles further.

In addition, if privacy is seen as an enabler of living the good life, then the importance of access to the internet becomes a consideration. Most accounts of online shaming involve the shamed retreating from the online world to avoid further humiliation and this can impact their ability to flourish in modern society. Indeed, the United Nations Human Rights Council passed a resolution in 2012 affirming access to the internet as a basic human right, because of its critical role in "promot[ing] the progress of society as a whole" [121]. The work of former and current special rapporteurs on the promotion and protection of the right to freedom of opinion and expression and on the right to privacy have been key in promoting international recognition of the importance of free speech and privacy concerning use of the internet [122–124]. In his 2011 report, former special rapporteur Frank La Rue recognized, among other things, access to the internet as a fundamental right and noted the risks of social networking to the right to privacy ([122], para. 11).

Second, where a right to public privacy has existed it tends to be framed as a right to retreat—a quiet space in public away from the public's attention—and on the related idea that we should not be vulnerable to have the minutiae of our lives scrutinized or aggregated just by being out and about in the world ([99], pp. 17–19).[62] Thus, it is still a Alan Westin inspired analysis that focuses on control, on the ability to stop the scrutiny in its tracks and control the data gathering and aggregation.

---

58 See discussion also in Cheung ([69], pp. 207–9).

59 See discussion in Richardson et al. [101] that case law tends to default to the view of the internet as a public space. Paton-Simpson states the factors that impact the degrees of privacy in public are i.e., "varying degrees of exposure or seclusion in different places and at different times, anonymity and the limitation of attention paid, various social rules, dispersion of information over space and time, and the ephemeral nature of our use of public space" ([99], p. 8).

60 Some of the offensive posts were detailed by the National Post [118]. See the Globe and Mail [119] for how the information was revealed.

61 In Canada, courts and employment tribunals have looked at the privacy settings of employees in assessing justification for workplace dismissals concerning social media use: see here Mangan [120].

62 Westin discusses this idea stating, "[k]knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas" ([125], p. 31).

Westin defines public privacy in its relation to anonymity, stating it is "when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance" ([125], p. 31). The harm with shaming seems to be more about how the event spiralled out of control, and about re-claiming one's identity, rather than identification or surveillance. The privacy right engaged concerning online shaming therefore can be seen to push the public privacy argument further. It is arguably triggered later on, after the mob attack. Your right is engaged once the persecution begins or once the private information was gathered for the reveal. In this way, some cases of online shaming have more in common with privacy claims of celebrities against paparazzi intrusions than it does about surveillance or information control.

4.3. Social Privacy

Building on the discussion so far, an episode of online shaming is social, illuminating the weakness in approaching privacy as predominantly about the ability to control information flows. As Waldman explains, "privacy involves our relationship to society, not our departure from it" ([82], p. 591). Social interactions are the engine that make social networking tick, and are what make online shaming possible. After the Vancouver riots, it was the interactive nature of social media that identified rioters [126]. This interactivity was used by a couple who posted CCTV footage to YouTube to track down the woman who dumped their cat in a bin [127].[63] The video received worldwide attention, and the offender, in addition to being identified and fined, received death threats [128]. Some abuse is more coordinated, such as the organization through 4chan, 8chan and reddit of the campaign of abuse against the female games developers and critics, discussed above [47].

What happens then to the shamed? If we accept that there is a privacy dimension to their experience, that their dignity has been assaulted, their sense of self-worth and identity diminished by the humiliation, and let us assume in this instance we are focused on online shaming versus a humbling as explored above, the question is the social dimension of this experience. Many conceptions of privacy position the person seeking privacy protection as having a right to be left alone or a right to control the information flow. The privacy-claiming-person is removed from the social context and positioned as being him or her against the world.[64]

Rather, the social nature of a public shaming brings to light to the social dimension of privacy. Not only is the shaming a social occasion, but the person being shamed might not be seeking isolation. Rather, the harm in a shaming is that it can force a withdrawal from society, or at minimum from participation in the social spaces online. Certainly they would like the sharing, bullying and mocking to stop, but they also want to be able to go about their lives in this social world we live in without being vulnerable to a virtual lynching. The privacy interest here, therefore, is better framed as a right to carve out a private space within the public realm, a safe zone, where you can be free from attack.

This desire to participate in the social spaces rather than retreat is reflected in *R v Elliott* [130], an Ontario case concerning criminal harassment via tweets.[65] Unlike most of the cases of shaming explored in this paper, *Elliott* involved harassment by one person, Gregory Elliott, over a period of months against two women, Stephanie Guthrie and Heather Reilly. The women used their twitter accounts on a personal level, but also for advocacy for a feminist organization. The alleged harassment was more about the volume of tweets rather than any one single tweet standing out as threatening. The one exception was a tweet by Elliott along the lines of "a whole lot of ugly at the Cadillac Lounge" ([130], p. 52). Reilly had been tweeting with her friends concerning plans to meet at the Cadillac lounge, and she testified that, in reading his tweet, she was fearful he was going to come to the restaurant, moving the harassment from online to the real world.

---

[63] See link to the video of the incident [127]. It has been viewed over 1.5 million times.
[64] See Steeves ([129], p. 199) discussing this idea in the context of Westin's work.
[65] It specifically concerned s 264 of the *Criminal Code* [65].

There are five elements to a claim of criminal harassment under s 264 of the Canadian *Criminal Code*: repeated communication, harassment of the complainant, knowledge by the perpetrator that it was harassment, fear for personal safety and reasonableness of that fear [65]. The Court concluded that both women had been harassed but that their fear for their personal safety was not reasonable in the circumstances. In the case of Guthrie there was an additional hurdle as the Court held that Elliott did not know that he was harassing her, although he was reckless as to that knowledge. Putting aside analysis of the case concerning criminal harassment, two aspects of the case are particularly illuminative of the struggle between the right to freedom of expression and privacy.

First, the Court analyzed whether Elliott's use of hashtags the women used could qualify as harassment. For example, Guthrie used #AOTID, which was a hashtag for an event which she was connected to, and the question was whether repeated communications by Elliott using this hashtag was harassment. This necessitated analysis of the public or private nature of hashtags. Is a hashtag a billboard to spread ideas, to target someone walking by, or is it more analogous to a call for a public meeting ([130], p. 60). The Court was understandably reluctant to find there was harassment using hashtags. Twitter is, for the most part, a public forum, and hashtags are a way of linking disparate conversations under one theme. However, the Court accepted that Elliott was referring to Guthrie and aware of her connection with #AOTID when using the hashtag. Unfortunately, Justice Knazan did not select the analogy he preferred, rather setting up the broad issues at play and then drawing a conclusion on a narrower point, in this case that the use of the hashtag was not a communication as required for criminal harassment ([130], p. 60). He left open the door for future cases, however, if it is established that "a person used a hashtag with the intention that someone who followed or had to follow it would read it" ([130], p. 60). The threshold is quite rightly high for a criminal charge, but it is hard to imagine a scenario where the burden would be met.

This question of whether there can be something private in a public social interaction remains to be developed. One can imagine a situation where a court might, in the future, order an injunction preventing continued communication with a Twitter user, which might, in narrow circumstances include hashtags. The key point is that the responsibility, if social privacy is taken seriously, should not wholly rest with the victim to avoid being subject to the abuse. Such an order would not be easy to execute, as it would be difficult to pinpoint hashtags that the victim might use in the future, and it would be too heavy of a free speech curb to have the harasser monitor, in a sense, all the victim's tweets to avoid using hashtags they have used, not to mention the behaviour it would encourage that it was purportedly thwarting. However, it re-focuses the mind so that the burden is not entirely borne by the victim, and the responsibility, rather, rests with the aggressor.

The second social privacy point concerning *Elliott* was the Court's treatment of the tweets concerning Cadillac Lounge. The Court concluded that Reilly did not fear for her safety, or if she did, the fear was not reasonable. However, the Court then comments on the privacy roots of her alleged fear. It is worth replicating the entirety of the Court's analysis here:

> Her fear that he might have been at the Cadillac Lounge and that he could escalate to offline and real-life harassment (though she had no idea what he would do) is based on her view that there is privacy in Twitter and that one account holder can dictate what another account holder tweets. But on the whole of this evidence, relating to both her and Ms. Guthrie, Twitter is not private, by definition and in its essence.
>
> On this evidentiary record, asking a person to stop reading one's feed from a freely chosen open account is not reasonable. Nor is it reasonable to ask someone to stop alluding to one's tweets. To subscribe to Twitter and keep your account open is to waive your right to privacy in your tweets. Arranging a meeting or social event using tweets other than direct messages is like inviting strangers into your home or onto your phone line while you talk to your friends. Blocking only goes so far, as long as you choose to remain open.

> I am not satisfied beyond a reasonable doubt that Mr. Elliott's repeated communications caused Ms. Reilly to fear for her safety. But had I been so satisfied in relation to the Cadillac Lounge incident, *I would not be satisfied beyond a reasonable doubt that such fear, based as it was on an expectation that non-direct tweets are private, was reasonable in all of the circumstances* [emphasis added] ([130], p. 83).

The Court evidences a convoluted analysis whereby since Reilly viewed tweets as private, which the Court concluded were public, then her fears for her personal safety are unfounded. This is based on a narrow reading of privacy as being predominantly about seclusion or revelation of unwanted information. Rather, if the series of events in this case, namely harassing tweets, is viewed through the lens of social privacy, then the privacy nugget expressed by Reilly becomes clearer. This does not necessarily change the outcome of the case, but it is an important analytical point for future cases concerning online interactions. It was about being free from targeted attacks, about preserving and protecting her self-worth and identity.

As Waldman argues, we must protect interactions with strangers as they are important for making connections, learning tolerance, finding jobs and relationships, and so on. He asserts, "[a]ny theory of privacy that disincentivizes some measure of sharing and interaction with strangers, then, cripples the very core of a democratic society" ([82], p. 612). The implications of Justice Knazan's analysis is that the appropriate response of someone harassed is a forced retreat from the public place—if you do not like being harassed, you should just go elsewhere. This ties with the criticism above that the burden is placed on the harassed to manage the invasion of privacy, rather than on the harasser.

Two key features to social privacy are teased out here: that privacy is dynamic and that it does not necessarily involve isolation. Austin captures the social dynamic of privacy, stating, "[p]rivacy is not best understood as a state of social withdrawal but as a set of norms that enable social interaction" ([75], p. 55). This outward-looking conception of privacy sees privacy as an enabler in forming connections. Margalit argues that privacy is about intimacy, stating that privacy is "an enabling condition for forming meaningful relations, the paradigms of which are family relations and friendship. Not loneliness but the possibility for intimacy is at the core of the idea of privacy" ([83], p. 262). This links the social with the analysis of identity above, that individuals need to be able to build and re-write the narrative of their lives ([89], chap. 9). In this way, identity can be seen to be rooted in a social context and public humiliation through shaming can be seen to disrupt this process.

One compelling account of privacy is by Waldman arguing that infringements of privacy are in essence breaches of trust. He asserts that "privacy, particularly in the information-sharing context, is really a social construct based on trust between social sharers, between individuals and Internet intermediaries, between groups of people interacting online and offline—broadly understood" ([82], p. 590). The answer to animate this right is more compelling in an American context, as he suggests rooting the right in the traditional breach of confidence action, something that has remained undeveloped in American law ([82], Section IV). This basis for a right to privacy is familiar to countries such as the United Kingdom.[66] Nevertheless, the broader claim of the trust-basis of privacy is persuasive. One interesting point for future research is the link between trust and civility, namely in what context the expectation that flows from trust takes the shape of civility.

In this social context, one way to frame privacy is as an interpersonal boundary control mechanism, as suggested by Irwin Altman, allowing the individual to define and re-define what their sense of self-identity finds acceptable as being in-bounds.[67] A focus on the concept of control, however, risks the privacy conundrum being seen to be resolved through simple control mechanisms. As long as the shamed can control what is acceptable and unacceptable there is no wrong. However, this does not account for the enabling function of privacy explored here. Valerie Steeves makes this

---

[66] This was the basis for the development of the tort of misuse of private information articulated in *Campbell* [111].
[67] See Steeves ([129], pp. 201–3) discussing the work of Irwin Altman [131].

point, arguing that the responsibility to negotiate the right should not be the sole burden of the individual ([129], pp. 206–7). This was the criticism in the analysis in *Elliott* detailed above.

Looking at the social interactions online, one can see the regulatory process between laws, markets and norms is dialogical and dynamic [18,132]. Within this, privacy can be viewed as "a dynamic process that is exhibited by the individual in social interaction with others, as the individual withdraws from others in solitude or moves from solitude to intimacy and general social interaction" ([129], p. 206). Privacy can be as much about intimacy and companionship rather than isolation. The public humiliation harm caused by online shaming disrupts the ability to form these connections online and off. Steeves suggests that the focus should be about the "quality of interaction between social actors" ([129], pp. 206–7) and this enables a right to privacy to exist in public places. This means that every situation is different, and while we can focus on boundary control it is driven from an analysis of what the shamer has done rather than what the shamed can control. In this way privacy is "an internal dimension of society" ([133], p. 15) and protecting it becomes as much about the social values at stake as the individual ([133], p. 15). This invites reflection on the kind of culture change we need to promote to protect privacy in online social spaces.

5. Conclusions

There is something fantastical about the idea of regulating online shaming, because it immediately raises concerns about regulating meanness, a social issue that the law is ill-equipped nor advised to weigh-in on. However, there is a crucial difference between a desire to wrap everyone in a bubble and create a right to be treated nicely as opposed to recognizing a right to be free from assaults on one's dignity and identity. Such nuance is critical to free speech questions of hate speech versus offense, public curiosity versus public interest and gossip versus substance.

This paper seeks to show how online shaming illuminates weaknesses in dominant privacy debates concerning dignity, the public right to privacy and the social dimension of privacy. A common link between these theories and points of debate is the public humiliation and attacks on identity experienced by victims of online shaming, the idea of "this isn't who I am" that pervades the stories of the shamed. Indeed, dignity was a central point of resonance. Any analysis of the social right to privacy or a right to privacy in public stemmed from concern about the assault on a shamed's dignity caused by a public humiliation. Drawing from Luban [76], I differentiate between humbling, where an individual is rightly knocked down a peg for a social transgression, and humiliation, which is an attack on one's dignity. Waldron makes a similar differentiation in the context of hate speech, differentiating between attacks on dignity, which objectively lower someone's social status, and offensiveness, which are subjective feelings of hurt or anger [91].

In the case of public privacy and social privacy, this paper shows the need for the law to develop to better reflect the dynamic social space within which we now experience our private lives. Online shaming is a public occasion, yet the right to public privacy has tended to be framed in law, at least in Canada and the UK, as a right of seclusion, a right to retreat from public attention. Similarly, online shaming is a social occasion, yet social privacy features minimally, if at all, in the cases, with most analysis thus far in scholarly work. Victims of online shaming often want to continue to participate in the spaces online, they simply want to be free from attack. These privacy interests immediately rub against free speech rights, and we should be concerned with formulating a privacy right that drifts into the territory of regulating meanness and offence. However, the failure to address the gap in privacy law concerning the public and social dimension of privacy has left many victims without legal recourse in the face of brutal abuse.

Public humiliation disrupts the ability to make connections and build one's identity and it is this aspect of privacy that requires re-imagining. The next step will be to develop a framework for such a privacy model, something that is beyond the scope of this paper. The key will be to finely connect the dignity points raised—namely differentiating humbling versus humiliation—and privacy as such. One way to do this is to further develop the conceptual underpinnings of privacy as an enabling

rather than secluding right. As an enabling right, the focus is less on a right of seclusion, although this is certainly a key aspect to the right to privacy. Rather, in recognizing that privacy is as much about companionship and social interactions as isolation, the focus broadens to more fully capture the continuum from seclusion to interaction within which we live. The privacy interest becomes about enabling participation in social spaces, enabling connections and relationships to form, and about enabling identity-making. Privacy theory has always struggled with its public and social dimension (and whether such a dimension exists at all). Modern shaming and the new technologies through which it is deployed highlight that this public and social space is a critical arena where privacy should be more fully accounted for.

Acknowledgments: I want to thank the participants in the 2015 Privacy Discussion Forum, hosted by Université Paris, for their comments on a draft version of this article, as well as the participants of the 2016 Internet Works-in-Progress conference, hosted by New York Law School, and British and Irish Law Education and Technology Associate (BILETA) conference, hosted by the University of Hertfordshire, for their comments on my presentation on the topic.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Jennifer Jacquet. *Is Shame Necessary: New Uses for an Old Tool*. New York: Pantheon Books, 2015.
2. Nathaniel Hawthorne. *The Scarlet Letter*. Boston: Ticknor, Reed and Fields, 1850.
3. Daniel Solove. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven: Yale University Press, 2007.
4. Lauren Goldman. "Trending Now: The Use of Social Media Websites in Public Shaming Punishments." *American Criminal Law Review* 52 (2015): 415–51.
5. Jon Ronson. *So You've Been Publicly Shamed*. New York: Riverhead Books, 2015.
6. *United States v Gementera*, 379 F.3d 596 (9th Cir. 2004).
7. Eric Posner. "A Terrible Shame: Enforcing Moral Norms without Law Is No Way to a Virtuous Society." *Slate*, 9 April 2015.
8. Kate Klonick. "Re-Shaming the Debate: Social Norms, Shame, and Regulation in an Internet Age." *Maryland Law Review* 75 (2016): 1029–65. [CrossRef]
9. Dan M. Kahan. "What Do Alternative Sanctions Mean?" *University of Chicago Law Review* 63 (1996): 591–653. [CrossRef]
10. Toni M. Massaro. "The Meanings of Shame: Implications for Law Reform." *Psychology, Public Policy and Law* 3 (1997): 645–704. [CrossRef]
11. James Q. Whitman. "What is wrong with Inflicting Shame Sanctions." *Yale Law Journal* 107 (1998): 1055–92. [CrossRef]
12. Martha C. Nussbaum. "Objectification and Internet Misogyny." In *The Offensive Internet*. Edited by Saul Levmore and Martha C. Nussbaum. Cambridge: Harvard University Press, 2010.
13. Chad Flanders. "Shame and the Meanings of Punishment." *Cleveland State Law Review* 55 (2007): 609–35.
14. Anne Cheung. "Revisiting Privacy and Dignity: Online Shaming in the Global E-Village." *Laws* 3 (2014): 301–26. [CrossRef]
15. Joel Reidenberg. "Lex Informatica: The Formulation of Information Policy Rules through Technology." *Texas Law Review* 76 (1998): 553–93.
16. Lawrence Lessig. "Social Meaning and Social Norms." *University of Pennsylvania Law Review* 144 (1996): 2181–89. [CrossRef]
17. Lawrence Lessig. *Code and Other Law of Cyberspace Ver. 2.0*. New York: Basic Books, 2006.
18. Andrew Murray. *The Regulation of Cyberspace*. Abingdon: Routledge-Cavendish, 2006.
19. Jonathan Zittrain. *The Future of the Internet and How to Stop It*. New Haven: Yale University Press, 2007.
20. Mark A. Lemley. "The Law and Economics of Internet Norms." *Chicago-Kent Law Review* 73 (1998): 1257–94. [CrossRef]
21. Lizzy Davies. "Facebook Refuses to Take Down Rape Joke Pages." *The Guardian*, 30 September 2011.
22. Meredith Bennett-Smith. "Facebook Vows to Crack Down on Rape Joke Pages after Successful Protest, Boycott." *Huffington Post*, 29 May 2013.

23. Eric Kain. "Reddit Makes Headlines Boycotting GoDaddy over Online Censorship Bills." *Forbes*, 26 December 2011.
24. Coral Braun, and Yonah Jeremy Bob. "Shurat HaDin Exposed Facebook's Double Standard in Removing Inflammatory Material on Its Site." *The Jerusalem Post*, 5 January 2016.
25. Anne Cheung. "Revisiting Privacy and Dignity: Online Shaming in the Global E-Village." University of Hong Kong Faculty of Law Research Paper No. 2012/019. Hong Kong: Faculty of Law, The University of Hong Kong, 2012. Available online: https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2010438 (accessed on 25 October 2016).
26. "And Now, a Funny Holiday Joke from IAC's PR Boss." Tweeted by Sam Biddle. Available online: http://valleywag.gawker.com/and-now-a-funny-holiday-joke-from-iacs-pr-boss-1487284969 (accessed on 25 October 2016).
27. Alison Vingiano. "This Is How a Woman's Offensive Tweet Became the World's Top Story." *BuzzFeed*, 21 December 2013.
28. Adrien Chen. "The Troll Hunters." *MIT Technology Review*, 18 December 2014.
29. Mariel Gruszko. "Crowd-Sourcing Surveillance: When Does Little Brother Get Too Big?" *Witness*, 5 July 2011.
30. Ciaran Mc Mahon. "Why We Need a New Theory of Cyberbullying. Working Paper Series #14.3.cb." Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2531796 (accessed on 25 October 2016).
31. Steve Bruce. "Young Man Enters Guilty Plea in High-Profile Nova Scotia Child Porn Case." *Herald News*, 22 September 2014.
32. Michael Macdonald. "Year of Probation for Second Man Who Pleaded Guilty in Rehtaeh Parsons Case." *The Globe and Mail*, 15 January 2015.
33. "Amanda Todd's Story: Struggling, Bullying, Suicide, Self Harm." YouTube video, 8:54, posted by "ChiaVideos", 11 October 2011. Available online: https://www.youtube.com/watch?v=ej7afkypUsc (accessed on 25 October 2016).
34. NoBulying.com. "The Unforgettable Amanda Todd Story." Available online: http://nobullying.com/amanda-todd-story/ (accessed on 25 October 2016).
35. Danielle Citron. *Hate Crimes in Cyberspace*. Cambridge: Harvard University Press, 2014.
36. Danielle Keats Citron. "Civil Rights in Our Information Age." In *The Offensive Internet*. Edited by Saul Levmore and Martha C. Nussbaum. Cambridge: Harvard University Press, 2010.
37. *Jones v Dirty World Entertainment Recordings LLC*, No. 13-5946, 2014 WL 2694184 (6th Cir. 16 June 2014).
38. *Communications Decency Act*, 47 USC.
39. Jeffrey Rosen. "Privacy in Public Places." *Law & Literature* 12 (2000): 167–91. [CrossRef]
40. Monica Lewinsky. "The Price of Shame." *TED*, March 2015.
41. Danielle Keats Citron, and Mary Anne Franks. "Criminalizing Revenge Porn." *Wake Forest Law Review* 49 (2014): 345–91.
42. National Network to End Domestic Violence. "A Glimpse from the Field: How Abusers are Misusing Technology." *Technology Safety*, 7 February 2015.
43. Norton. "Online Harassment: the Australian Woman's Experience." Available online: https://phoenix.symantec.com/Norton/au/online-harassment-experience-women/ (accessed on 25 October 2016).
44. Becky Gardiner, Mahana Mansfield, Ian Anderson, Josh Holder, Daan Louter, and Monica Ulmanu. "The dark side of Guardian comments." *The Guardian*, 12 April 2016.
45. The Guardian. "The Web We Want." Available online: https://www.theguardian.com/technology/series/the-web-we-want (accessed on 25 October 2016).
46. Jenn Frank. "How to Attack a Woman Who Works in Video Gaming." *The Guardian*, 1 September 2014.
47. Caitlin Dewey. "The Online Guide to Gamergate You Will Ever Need to Read." *The Washington Post*, 14 October 2014.
48. Press Association. "Two Face Jail over Twitter Abuse of Banknote Campaigner." *The Guardian*, 24 January 2014.
49. Staff and Agencies. "Two Jailed for Twitter Abuse of Feminist Campaigner." *The Guardian*, 24 January 2014.
50. Brian Leiter. "Cleaning Cyber-Cesspools: Google and Free Speech." In *The Offensive Internet*. Edited by Saul Levmore and Martha C. Nussbaum. Cambridge: Harvard University Press, 2010.
51. Ellen Nakashima. "Harsh Words Die Hard on the Web." *The Washington Post*, 7 March 2007.

52. *Elonis v United States*, 575 US __ (2015).
53. *McAlpine v Bercow*, [2013] EWHC 1342 (QB).
54. Mark Sweney. "Lord McAlpine Settles Libel Action with Alan Davies over Twitter Comment." *The Guardian*, 24 October 2013.
55. Press Association. "Lord McAlpine Libel Row with Sally Bercow Formally Settled in High Court." *The Guardian*, 22 October 2013.
56. Ellen Branagh. "Lord McAlpine Drops Defamation Claims against Twitter Users with Fewer Than 500 Followers." *The Independent*, 21 February 2013.
57. *Pritchard v Van Nes*, 2016 BCSC 686.
58. Ursula Kennedy. "Q&A with Caroline Criado-Perez. 'What Happened to Me Was a Wake-Up Call for Society'." *The Guardian*, 3 May 2015.
59. *Communications Act*, 2003 c 21.
60. *Chambers v DPP*, [2012] EWHC 2157.
61. *Public Order Act*, 1986 c 64.
62. *Malicious Communications Act*, 1988 c 27.
63. *Protection from Harassment Act*, 1977 c 40.
64. *Canadian Charter of Rights and Freedoms.* Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.
65. Criminal Code, RSC 1985, c C-46.
66. Bill C-13. *An Act to Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Sess, 41st Parl, 2013 (assented to 9 December 2014).
67. Teresa Scassa. "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy." *Canadian Journal of Law and Technology* 7 (2010): 193–220.
68. Cass Sunstein. "Believing False Rumors." In *The Offensive Internet*. Edited by Saul Levmore and Martha C. Nussbaum. Cambridge: Harvard University Press, 2010.
69. Anne Cheung. "Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd." *Journal of Media Law* 2 (2009): 191–217.
70. Lawrence Lessig. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.
71. Andrew Couts. "Anonymous, Amanda Todd and the Dangers of Vigilante Justice Online." *Digital Trends*, 17 October 2012.
72. Twitter. "#congratsyouhaveanallmalepanel." Available online: https://twitter.com/hashtag/congratsyouhaveanallmalepanel (accessed on 26 January 2017).
73. *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Marios Costeja Gonzalez*. Case 12 (2014) C-131/12.
74. Viktor Mayer-Shonberger. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press, 2009.
75. Lisa Austin. "Privacy, Shame and the Anxieties of Identity." 2012. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2061748 (accessed on 25 October 2016).
76. Universal Declaration of Human Rights, 1948.
77. The Charter of Fundamental Rights of the European Union, 2000/C 254/01.
78. David Luban. *Legal Ethics and Human Dignity*. Cambridge: Cambridge University Press, 2007.
79. *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212.
80. *R v Fearon*, 2014 SCC 77, [2014] SCR 621.
81. James Q. Whitman. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale Law Journal* 113 (2004): 1151–221. [CrossRef]
82. Ari Ezra Waldman. "Privacy as Trust: Sharing Personal Information in a Networked World." *University of Miami Law Review* 69 (2015): 559–630.
83. Avishai Margalit. "Privacy in the Decent Society." *Social Research* 68 (2001): 255–68.
84. Jeffrey Rosen. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.
85. Jeffrey Rosen. "Out of Context: The Purposes of Privacy." *Social Research* 68 (2001): 209–20.
86. Lisa Austin. "Privacy and the Question of Technology." *Law and Philosophy* 22 (2003): 119–66.
87. Jon Ronson. "How One Stupid Tweet Ruined Justine Sacco's Life." *The New York Times*, 12 February 2015.

88. Norberto Nuno Gomes de Andrade. "Human Genetic Manipulation and the Right to Identity: The Contradictions of Human Rights Law in Regulating the Human Genome." *SCRIPT-ed* 7 (2012): 429–52.
89. Paul Bernal. *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge: Cambridge University Press, 2014.
90. Helen Nissenbaum. "Privacy as Contextual Integrity." *Washington Law Review* 79 (2004): 119–57.
91. James Grimmelmann. "The Virtues of Moderation." *Yale Journal of Law and Technology* 17 (2015): 42–109.
92. *R v Keegstra*, [1990] 3 SCR 697.
93. Jeremy Waldron. *The Harm in Hate Speech*. Cambridge: Harvard University Press, 2012.
94. *Sidabras and Dziatuas v Lithuania*, Application nos. 55480/00 and 59330/00, 27 July 2004.
95. *Handyside v United Kingdom*, (1979–1980) 1 EHRR 737.
96. Nicole Moreham. "Privacy in Public Places." *Cambridge Law Journal* 65 (2006): 606–35. [CrossRef]
97. Restatement (2d) of Torts (2010).
98. Daniel J. Solove, and Neil M. Richards. "Privacy's Other Path: Recovering the Law of Confidentiality." *The Georgetown Law Journal* 96 (2007): 153–82.
99. Elizabeth Paton-Simpson. "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places." *The University of Toronto Law Journal* 50 (2000): 305–46. [CrossRef]
100. *Moreno v Hanford Sentinel Inc.*, 172 CalApp (4th) 1125 (2009).
101. Megan Richardson, Julian Thomas, and Marc Trabsky. "The Internet Imaginary and the Problem of Privacy." University of Melbourne Legal Studies Research Paper No. 633. Melbourne Law School, University of Melbourne, Melbourne, Australia, 2012. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2252274 (accessed on 26 October 2016).
102. *Jones v Tsige*, 2012 ONCA 31, 108 (3d) 241.
103. Barry Sookman. *Computer, Internet and Electronic Commerce Law*. Toronto: Carswell, 1988.
104. *Doe 464533 v ND*, 2016 ONSC 541.
105. *Criminal Justice and Courts Act*, 2015 c 2.
106. *Cyber-safety Act*, SNS 2013, c 2.
107. CBC. "Nova Scotia to Craft New Cyberbullying Law." *CBC*, 14 April 2016.
108. *Crouch v Snell*, 2015 NSSC 340.
109. *Intimate Image Protection Act*, SM 2015, c 42.
110. *Aubry v Éditions Vice-Versa inc*, [1998] 1 SCR 591.
111. *Campbell v MGN Ltd*, [2004] UKHL 22.
112. *Judith Vidal-Hall & ors v Google Inc*, [2014] EWHC 13.
113. *The Author of a Blog v Times Newspapers Ltd*, [2009] EWHC 1358 (QB).
114. *Von Hannover v Germany No. 1*, Application no. 59320/00, [2004] ECHR 294 (24 June 2004).
115. *Von Hannover v Germany No. 2*, Application 40660/08, [2012] ECHR 228 (7 February 2012).
116. *Peck v United Kingdom*, Application, 44647/98 [2003] ECHR 44 (28 January 2003).
117. *European Convention for the Protection of Human Rights and Fundamental Freedoms*, 1950.
118. The National Post. "Dalhousie Investigating 'Deeply Disturbing' Facebook Page about Female Dentistry Students." *The National Post*, 16 December 2014.
119. Jane Taber. "Dalhousie Dentistry Student Blew the Whistle on Facebook Group: Lawyer." *The Globe and Mail*, 18 January 2015.
120. David Mangan. "A Platform for Discipline: Social Media Speech and the Workplace." Available online: http://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1084&context=olsrps (accessed on 25 October 2016).
121. UN Human Rights Council A/HRC/20/L.13 (2012).
122. Report of the special rapporteur on the promotion and protection of the right to freedom of expression, Frank La Rue to the Human Rights Council, A/HRC/17/27 (2011).
123. Report of the special rapporteur on the promotion and protection of the right to freedom of expression, David Kaye to the Human Rights Council, A/HRC/32/38 (2016).
124. Report of the special rapporteur on the right to privacy, Joseph A. Cannataci to the Human Rights Council, A/HRC/31/64 (2016).
125. Alan F. Westin. *Privacy and Freedom*. New York: Atheneum, 1967.

126. Christopher Parsons. "Shame Justice on Social Media: How It Hurts and Ways to Limit It." 8 May 2012. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2151204 (accessed on 25 October 2016).
127. "Cat in bin in Coventry." YouTube video, 1:26, posted by "atalbot01", 22 August 2010. Available online: https://www.youtube.com/watch?v=MOuCjzVAO_w&feature=player_embedded (accessed on 25 October 2016).
128. Patrick Barkham. "Cat Bin Woman Mary Bale Fined £250." *The Guardian*, 19 October 2010.
129. Valerie Steeves. "Reclaiming the Social Value of Privacy." In *Privacy, Identity and Anonymity in a Networked World: Lessons from the Identity Trail*. Edited by Ian Kerr, Valerie Steeves and Carole Lucock. New York: Oxford University Press, 2009.
130. *R v Elliott*, 2016 ONCJ 35.
131. Irwin Altman. *The Environment and Social Behavior*. Monterey: Brooks/Cole Publishing, 1976.
132. Andrew Murray. "Nodes and Gravity in Virtual Space." *Legisprudence* 5 (2011): 195–221. [CrossRef]
133. Daniel J. Solove. "'I've Got Nothing To Hide' and Other Misunderstandings of Privacy." *San Diego Law Review* 44 (2007): 745–72.