



Selected Papers of Internet Research 16:
The 16th Annual Meeting of the
Association of Internet Researchers
Phoenix, AZ, USA / 21-24 October 2015

ON THE INTERNET NOBODY CAN SEE YOUR CAPE: THE ETHICS OF ONLINE VIGILANTISM

Mathias Klang
Umass Boston

Introduction

The discussion of vigilantism has been most active in the legal discourse, in which the term has been classified historically and divided into classical vigilantism, neovigilantism, pseudo-vigilantism and faux-(Hine 1998). However, a major problem with this discourse is that, for the most part, online activity would not fit easily into the existing terminology. This paper will open up the discussion and merge the theoretical, social and technical discussion on vigilantism by drawing on its modern forms.

As they are the easiest forms, the largest part of Internet vigilantism consists of publishing personal public information (doxxing) or spreading public information (shaming). However, there are more technically demanding forms of vigilantism, such as, hacking into servers in order to reveal private information and denial of service attacks. Finally, there are the harassment attacks such as sending merchandise to the persons home and the creative campaign to change create a neologism out of a politicians name.

Among the infamous early examples of online vigilantism is the 2005 dog poop girl where a South Korean girl was targeted for not cleaning up her dogs poop in a Seoul subway car. An image of the girl was uploaded and she was quickly identified, doxxed and humiliated.

Discussing the act at the time Daniel Solove (2005) focused on the power of technology to enhance the anger at the rule breaker and to punish: “The dog-shit-girl case involves a norm that most people would seemingly agree to - clean up after your dog. Who could argue with that one? But what about when norm enforcement becomes too extreme? Most norm enforcement involves angry scowls or just telling a person off. But having a permanent record of one’s norm violations is upping the sanction to a whole new level. The blogosphere can be a very powerful norm-enforcing tool, allowing bloggers to act as a cyber-posse, tracking down norm violators and branding them with

Suggested Citation (APA): Klang, M. (2015, October 21-24) *On The Internet Nobody Can See Your Cape: The Ethics Of Online Vigilantism*. Paper presented at Internet Research 16: The 16th Annual Meeting of the Association of Internet Researchers. Phoenix, AZ, USA: AoIR. Retrieved from <http://spir.aoir.org>.

digital scarlet letters.” Solove wrote from the perspective of the technology at the time and while the discussion on vigilantism has barely moved forward in the last decade the technology available to the vigilante has rapidly increased.

Empirical Material

As the purpose of this paper is to better understand the concept of digital vigilantism and to break the concept down into ethical components, the focus of this work will be on the more widespread aspects of the act, i.e. the process of spreading and shaming aspects. The goal is to observe this powerful tool in order to better understand and contextualize it in an ethical and social perspective.

This will analyze a series of cases where the general public involved in acting as a vigilante group, shaming the perpetrator and calling for retribution. The communication of the masses was done to punish norm violators for their transgression of social norms. In order to better understand the concept this paper will describe some recent examples of wide spread digital vigilantism such as:

The Tumblr site “Racists Getting Fired (and Getting Racists Fired!)” whose goal it is to collect racist social media posts along with contact information from the poster and information about their employment. Their purpose is explicit in the title, it is to encourage complaints to the employer and to have the person fired.

The Sacco tweet. In 2014, before getting on an 11 hour flight to South Africa Justine Sacco tweeted a comment that could be understood to be racist. The tweet spread far beyond her small group of followers and gained a huge amount of traction. The criticism about her tweet was harsh and large. Before the plane landed, her company had decided to fire her for her tweet.

The Tumblr site Public Shaming, which focuses on reproducing tweets that violate social norms. The goal is to publically shame individuals who publically behave badly. They publish tweets that are misogynistic, anti-workers rights and racist.

This work will also look at the more public aspects of Anonymous (Coleman 2014, Serracino-Inglott 2013). Their digital vigilantism that involves the spreading of private information obtained through hacking. The goal is not to study their denial of service or hacking but rather to focus on the ways in which the organization acts as a legitimization for acts of digital vigilantism.

A final interesting case was that of the game journalist Alanah Pearce who when she discovered that her abusive trolls were young teenage boys contacted their mothers and told her about what they had done (Brooker 2014). While the perpetrators personal information was not put online and they were not shamed to a wider social public, this case is interesting in that the media stories and social media reactions were positive towards Pearce’s actions.

The Armchair Vigilante

When Johnston (1996) attempted to define the concept of vigilantism in a legal context he outlined six necessary criteria in order for an act to be true vigilantism (planning, citizens, social movement, use of force, norm transgression, and control). These will be the starting point for this paper in the exploration of the online vigilante.

The goal of this work is to look at the ways in which technology is used in the process of vigilantism. The central question is to look at the ways in which liking, sharing and retweeting previously published information is carried out and to evaluate the behavior. The question is whether, and in what cases, the act of sharing makes it into an act of armchair vigilantism or digilantism (Coldewey 2013) and looks to understanding moral liability (Dumsday 2009, Leitch & Warren 2012). The paper will look at the use of social media in the process of sharing information with the intent of pointing to a breach of social or legal norms and assess where the lines may be drawn between retributive justice and simple sharing. In other words this paper will define the digital vigilante and provide a framework within which online acts can be understood.

Bibliography

Brooker, C. (2014) The gaming journalist who tells on her internet trolls – to their mothers. *The Guardian* <http://www.theguardian.com/culture/australia-culture-blog/2014/nov/28/alanah-pearce-tells-on-her-internet-trolls-to-their-mothers>

Coldewey, D. (2013). “Dawn Of The Digilante” *TechCrunch* <http://techcrunch.com/2013/04/21/dawn-of-the-digilante/>

Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* Verso Books.

Dumsday, T. (2009). On Cheering Charles Bronson: The Ethics of Vigilantism, *The Southern Journal of Philosophy*, Volume 47, Issue 1, pages 49–67, Spring 2009

Hine K. D. (1998). “Vigilantism Revisited: An Economic Analysis of the Law of Extra-Judicial Self-Help or Why Can't Dick Shoot Henry for Stealing Jane's Truck” *47 Am. U. L. Rev.* 1221 (1997-1998).

Johnston, L. (1996) “What is Vigilantism?” *British Journal of Criminology* (1996) 36 (2): 220-236.

Leitch, S. and Warren, M. (2012). “Cyber-bullying and vigilantism: should social media services be held to account?”, in S. Leitch and M. Warren (ed.) *Proceedings of 6th Australian Institute of Computer Ethics Conference, AiCE 2012*, Burwood, Australia, 13 February 2012, pp. 32-37.

Serracino-Inglott, P. (2013). Is it OK to be an Anonymous? *Ethics & Global Politics*, Vol. 6, No. 4, 2013, pp. 217–244. <http://dx.doi.org/10.3402/egp.v6i4.22527>

Solove, D. (2005). “Of Privacy and Poop: Norm Enforcement Via the Blogosphere”, *Balkinization* Thursday, June 30, 2005. <http://balkin.blogspot.com/2005/06/of-privacy-and-poop-norm-enforcement.html>