On Véliz's Argument

Josh Lind

4 December 2019

Background

In her article, "Online Masquerade: Redesigning the Internet for Free Speech Through the Use of Pseudonyms" (2018), Dr. Carissa Véliz argues for the implementation of regulated non-public pseudonymity (RNPP) online. Non-public pseudonymity (NPP), as I will use in this paper, refers to a system in which every citizen receives a finite number of usernames that they are allowed to use throughout their life. Users of sites such as Twitter or Reddit would be restricted to posting from these internet-wide pseudonyms, and the true identity behind each username would only be known to the account holder and an incorruptible organization that maintains everyone's pseudonyms. Regulated, in RNPP, refers to the existence of a team of employees that would reclaim pseudonyms in cases where the pseudonym was abused, such as repeated bullying or hate speech.

Véliz begins her article by analyzing the positive and negative implications of anonymity and its converse, identifiability. Véliz wraps up these first two sections by writing "we want to make sure both that valuable speech can be made to be low-cost (have no repercussions), and that abusive and inappropriate speech is either not allowed to take place or if it does take place, that it is costly for the perpetrators" (p. 7). This claim emphasizes the need for a middle ground, and for the majority of her article, Véliz works to defend how RNPP satisfies this need.

In what follows, I provide an explicit formulation of Véliz's argument, attempt to reconstruct Véliz's justification of the premises, and critically evaluate the argument. In my evaluation, I argue that Véliz overstates the benefits of mandating pseudonymity and underrepresents the negative implications; therefore, her second premise is false, and thus the argument is unsound.

Véliz's Argument

In explicit form, Véliz's argument is as follows:

(P1) We should implement rules that increase the overall well being of a society.
(P2) The careful implementation of RNPP would increase the overall well being of our society.
(C1) We should carefully implement RNPP.

The first premise of Véliz's argument is simply a restatement of act utilitarianism. Act utilitarianism is a fitting moral framework to employ when considering the implementation of RNPP because its implementation would result in numerous potential benefits and drawbacks for all internet users. Also, respect-based moral frameworks such as the humanity formulation of Kantianism often fail when considering the morality of laws, due to the fact that some percentage of the population will oppose the enactment of the law or policy.

The second premise is the primary claim that Véliz attempts to defend throughout her article. That is, that the careful implementation of RNPP would have a net benefit on society. Véliz defends this premise indirectly by justifying the sufficient claim that RNPP would retain most of the benefits of both anonymity and identifiability, without bringing along the disadvantages of either. After enumerating the implications of anonymity and identifiability, Véliz begins to justify the second premise by describing how such a policy could be implemented. Throughout her description, Véliz works to defuse obvious objections by providing constraints on how RNPP should be carried out. For instance, Véliz clarifies that Pseudo, a fictional organization that "would act as fiduciaries of the link between real names and pseudonyms," would never publicize an individual's pseudonym because it would "undermine the whole system of pseudonymity" (Véliz, 2018, p.10). Additionally, Véliz ends her section on methods of implementation by clarifying that the purpose of her article is to communicate the upshot of RNPP, not to provide a clear cut way in which pseudonymity should be implemented. After, she brings up three plausible objections to the claim that implementing RNPP would be optimific. The first objection that Véliz discusses is the notion that reliance on "supranational mechanisms of enforcement" such as Pseudo would be infeasible. Véliz refutes this claim by pointing out the existence of a similar organization, the Internet Corporation for Assigned Names and Numbers, that has successfully functioned for years (Véliz, 2018, p. 11). The second objection Véliz replies to is the claim that implementing RNPP would promote deception online. In response, Véliz writes that deception of the internet would decrease because netizens, citizens of the internet, would always know whether they were communicating with a real identity or a pseudonym. Additionally, deception could be circumvented by allowing netizens to publicize their credentials, such as degrees or awards. Lastly, Véliz defends her argument against the objection that RNPP would result in increased censorship. Véliz refutes this objection due to two reasons: prohibitions against egregious behavior such as hate speech doesn't amount to censorship, and backlash one might receive as a result of unpopular speech would be significantly contained as it would not affect the image of that netizen as a whole.

Argument Evaluation

In the following paragraphs, I will evaluate Véliz's argument. Her argument is logically valid, as the conclusion follows from the premises. Thus, for Véliz's argument to be sound, both of the premises must be true. However, I believe that Véliz's second premise is false, and thus her argument is unsound.

One claim Véliz makes in her article that overstates the benefits of RNPP is her claim that the implementation of RNPP would lead to an internet "relatively free from harassment" (p. 11). The validity of this claim relies on the false assumption that most trolls on the internet use anonymous accounts, when in reality, social media users are significantly less bashful than Véliz would hope. Consider the case of Facebook, where countless users regularly post abusive and inappropriate speech despite the identifiable nature of the site. Furthermore, trolls on anonymous sites such as Reddit or Twitter often use the same pseudonym across many sites. Therefore, it seems unlikely that the implementation of RNPP would drastically reduce the amount of unproductive speech on the internet.

While Véliz does include a section at the end of her paper detailing the importance of regulatory bodies such as Pseudo holding up their promises, Véliz underrepresents the privacy concerns that would be brought about by RNPP. Specifically, Véliz doesn't give ample consideration to the fact that RNPP would create a substantial target for hackers. To motivate this point, let us first consider what information Pseudo would need to store about netizens in order to effectively sustain RNPP across the internet. First, Pseudo would need to store some form of unique identification for all netizens that links one's pseudonyms with their real identity. This identification would likely take the form of social security numbers and similar programs in other countries. Secondly, in order for Pseudo to police the internet, they would need to collect all posts that one makes online, or at least keep a record of posts that are deemed unacceptable. Therefore, the information stored by Pseudo, if made public, would have devastating consequences on the ability for netizens to engage in low-cost speech. Additionally, we've seen in recent years that companies holding sensitive information can't realistically make the claim that their data is unhackable. In September of 2017, Equifax, one of the largest credit reporting companies in the US, reported "that its systems had been breached and the sensitive personal data of 148 million Americans had been compromised... The data breach included names, home addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers" (EPIC). This breach serves as a reminder that data is never fully secure, and that organizations like Pseudo would be vulnerable to attacks.

One might reject this justification for why RNPP brings about worse consequences than the current system by arguing that netizens today face the same issues brought up in the previous paragraph. Specifically, an objector might claim that Twitter, Reddit, and other companies face the same risk of being hacked, and thus the users experience the same risks that come with potential identifiability. Initially, this objection seems plausible as we could reasonably assume that Pseudo would have security measures at least as robust as all current online mediums; however, the disanalogy in this case is that with Twitter, Reddit, and other mediums for open discussion, the user decides how much sensitive information they want to divulge. Thus, if an anonymous Twitter account was hacked, the user wouldn't experience any of the negative repercussions of identifiability. In contrast, a compromised Pseudo profile would link the real user with every post they’ve ever made on the internet. This could result in social rejection, getting fired, and in some cases physical harm.

Conclusion

In this paper, I have argued that Véliz’s argument is unsound because regulated non-public pseudonymity wouldn’t have a net positive impact on our society. First, I drew out an explicit formulation of Véliz’s argument. Second, I attempted to justify the premises in her argument. Lastly, I provided my evaluation of her argument, and justified why the second premise is false.

References

Center, E. P. I. (n.d.). EPIC - Equifax Data Breach. Retrieved from https://epic.org/privacy/data-breach/equifax/.

Véliz, C. (2018). Online Masquerade: Redesigning the Internet for Free Speech Through the Use of Pseudonyms. *Journal of Applied Philosophy*. doi: 10.1111/japp.12342]