Daniel Trottier

22 Digilantism

Abstract: This chapter considers the practice of digilantism, in which unaffiliated individuals seek online retaliation against seemingly illegal and immoral actions. Local communities and content creators adopt mobile devices and social platforms to make wrongdoers visible to an ever-expanding audience. These practices are inherently ambivalent. Not only do they implicate a range of progressive and regressive causes, they also complicate relations between states and vigilantes.

Keywords: digilantism, vigilante, justice seeking, scrutiny, denunciation

Introduction

Daniel Solove's 2007 book *Future of Reputation* opens with a now infamous 'dog poop' incident from South Korea, where a woman refused to pick up her dog's waste in a subway (see also Dennis, 2008 and Reichl, 2019). This triggered on-site and online outrage against her presumed sense of entitlement. Someone on the subway uploaded a photograph of her, at which point she was publicly identified. Popular culture dictates that the internet does not forgive, nor does it forget. This global media spectacle brought disproportionate punishment for the target, including online and offline harassment.

This case is one of the first major examples of digilantism, which refers to unaffiliated individuals taking offense at seemingly illegal and immoral actions and engaging in online retaliation. While digilantes may cooperate with police by sharing evidence, so too do they engage in their own forms of punishment, including getting the target fired, online harassment, and physical retaliation. Digilantism is justice seeking performed by individuals not deputized by local authorities. Participants use digital tools to identify and denounce alleged wrongdoers. These practices are criminologically relevant as a mediated expansion and mutation of embodied vigilantism (Johnston, 1996). Local communities and content creators adopt mobile devices and social platforms to make wrongdoers visible to an ever-expanding audience. In publishing allegations against a targeted individual, there is often a presumption of guilt that serves to bypass any deliberation or appeals to reason.

Funding: This research was funded by the Dutch Research Council (NWO), project number 276 – 45 – 004.

Digilantism is ambivalent in that it includes both regressive and progressive mobilizations. It may address long overlooked harms like sexual abuse (see Abuse by McAlinden), but often exceeds what we might consider a proportionate response. Its mandate extends seamlessly from crimes to moral offences that are not (yet) considered criminal. Despite the digital moniker, it not only includes responses to online offenses like revenge porn and nuisances like 'voluntourism' (posting problematic representations of humanitarian work, see Schwarz and Richey, 2019), but also offensive offline behavior like animal abuse (Chang and Poon, 2017) and 'manspreading' (taking up too much space in public, see Jane, 2017). Moreover, offenses and annoyances can be denounced online as well as offline, as when posters identifying people engaging in hate speech are plastered all over a city centre (Plesničar and Šarf, 2020). Other terms used include digital vigilantism, cyber vigilantism, internet vigilantism, virtual vigilantism, netilantism, and the 'human flesh search engine' in the Chinese context.

Digilantism in relation to vigilantism

We can build upon Johnston's six dimensions of embodied vigilantism that include (i) planning and premeditation by (ii) private voluntary citizens that (iii) constitutes a kind of social movement of 'autonomous citizenship' that (iv) uses and threatens the use of force (v) against a (perceived/potential) social transgression, and therefore (vi) conveys a sense of security to a local public, despite being illegal in many jurisdictions (Johnston, 1996: 220). These characteristics are to some degree challenged or disrupted by digital media (Trottier, 2017). The most striking dimension that digitization challenges is arguably the use of force (iv), which now relies heavily on cultural violence in terms of weaponization of visibility. This is a lasting and searchable stigma, that other media actors can yield at any point in time. Planning and premeditation (i) is also complicated, as digilantism campaigns are held together by a diversity of social actors. Some participants may trigger a vigilante reaction when they impulsively photograph and share asocial behavior they witness on a train. Other participants may comment on and share this content as part of their routine social media practice (see Social Media by Twigt), without a particular movement (iii) or reassurance of security (vi) in mind. But their actions may be coached, coordinated, and enhanced by those who intentionally cultivate a digilante movement, or online following. These professional digilantes may cultivate a sense of mediated vigilance among their audiences (Trottier, 2020). They create a type of audience participation that not only reacts to footage that entrepreneurs put out on their channels, but also is willing and able to source offensive content for these channels. It is important to view digilantism not just as series of cases, but as a generalized set of practices on social media that combines consuming content and enacting some sense of justice and punishment of targets.

Employing a vigilantism framing allows scholars to make sense of new practices emerging out of digital media usage. This lens also helps underline that digilantism is often representative of hegemonic values within a society (Rosenbaum and Sederberg, 1974), but a means for marginal communities to cope with their own vulnerabilities (Madsen, 2004). Abrahams also recognizes that researchers and practitioners “have some choice in how narrowly or broadly we define” vigilantism (1998: 6). Criminologists should keep this ambivalence in mind when assessing digital versions. The fact that incidents are crowdsourced among social actors on a global scale means that what seems like a ‘pure’ case of digilantism on first pass will include other actors (e. g., tabloid media online) engaging in other practices (e. g., harassment, counter-denunciations).

Several typologies highlight the moral ambivalence of just and harmful cases of vigilantism. Loveluck (2020) proposes a classification based on four ideal types that include more peripheral practices like flagging, organized leaking, and core practices like investigating and hounding. He acknowledges that any single case may include several of these types, for instance when an attempt to identify an assailant may scale up to “a more sustained mobilisation against” the individual that includes harassment (Loveluck, 2020: 227). In response Galleguillos proposes “a conceptual distinction between attacks and investigations” (2022: 358). Even if these fold into each other easily in practice, it is useful to consider that these may be distinct phases that mobilize separate actors. Here, practices like citizen journalism or citizen science may overlap with digilantism when they generate content that is knowingly or unknowingly used to denounce a targeted person (Mano, 2010). Likewise, digilantes may frame their actions as citizen journalism as a means of legitimation. Gainford (2022) proposes four broader sets of practices, namely informative, investigative, punitive, and disruptive. These distinctions are useful for mapping diverse motivations. Once again, these are ideal types that are complicated, as even local events can bring in global actors to denounce and punish targets. Punitive digilantism in particular is “reliant on the audience’s willingness to accept and consume the content” (Gainford, 2022: 203). This speaks to how digilantism depends on the good will of an audience to sustain legitimacy, as well as mediators and platforms that frame and share this content.

Relations with the state

Relations between vigilantes and the state are also important, especially when police may mobilize others to investigate. Relations between states, civilians, and private organizations are nodal (Shearing and Wood, 2003), as collaborations in policing are renegotiated. Researchers address relations between digilantes and police, noting that the former can assist in sharing information. Some collectives are “a potentially useful, if under-valued, component of cyber-security networks” (Huey et al., 2013: 81). High profile cases shape public perception, bringing demand for local authorities to be proactive when handling digilantism.

In the European context collaboration between police and public “are here to stay, but the rules of this ‘game’ have yet to be established,” and the police “discursively set boundaries” between acceptable and unacceptable public engagement online (Dekker and Meijer, 2020: 298). On the role of the state in Morocco, Chalfaouat (2020) notes digilantism is enacted through co-production of security in public participation. He recommends "the promotion of civic virtue to the public interest and the avoidance of retaliation" (Chalfaouat, 2020: 182). Digilantism is a continuum that includes collaborative relations with public authorities alongside practices deemed illegal. Researchers may consider how citizen (digital) vigilance is promoted by police and governments. Governments may mobilize civil society groups like StopXam, a digilante group against bad parking and other traffic nuisances (Gabdulhakov, 2020). Yet these partnerships may be abandoned and denounced by state media when no longer advantageous.

Digilantes are also motivated by the perception that police cannot handle digital crimes, such that they seek to restore order themselves. Likewise, research on a crowdsourced investigative Reddit community reveals "an ambivalent rapport between [community] members and the police whose limitations are frequently invoked to justify the development of investigative activities in the first place" (Myles et al., 2020: 333, *brackets added*). We can consider the diverse skills often required to perform digilantism, including hacking (see Hacking by Wall), open-source intelligence (OSINT) investigations, and the ability to command a supportive audience. Digilantes also rely on social engineering, including those who target so-called 'email scammers' (Byrne, 2013). These skills are centered around making the target visible while either remaining anonymous, or making oneself visible in a strategic way to maintain control over the media narrative. In these contexts, digilantes engage in image work when interacting with the public to "negotiate who they are (not) and what they (do not) do" (Myles et al., 2020: 319). Criminologists should follow how these practices are negotiated by digilantes, whether these are cohesive groups like neighborhood watch communities, or temporary partnerships on Reddit.

Digital media platforms also promote global tendencies in media practice, including in justice seeking. Most prominently, they become common venues for denouncing child sexual abuse in countries including the United States, Germany, the Netherlands, Cambodia, and Russia (Hadjimatheou, 2021). These global initiatives have local adaptations that reflect systemic harms. In the Russian context, so-called pedophile hunting 'safaris' willfully conflate pedophilia "with homosexuality under the category of 'non-traditional sexual relations'", enabling "moral entrepreneurs to use the almost unchallenged condemnation of child abuse to strengthen their broader moral and political goals" (Favarel-Garrigues, 2020: 306).

Progressive and regressive digilantism

Progressive forms of digilantism against, for example, sexual abuse emerge due to a perceived lack of legitimate and effective institutional alternatives, including being able to rely on the police. Disproportionate punishment by digilantes may be explained by public perception that these crimes are poorly handled by law enforcement. Public discourse that celebrates feminist digilantism risks framing these practices as the only viable recourse for anyone wishing to avoid sexual abuse (Jane, 2016: 292). As digilantes are embedded in temporary partnerships with police, criminological research should address the division of responsibility between feminist digilantes and local authorities who may not want to appear unresponsive to gendered forms of abuse. Feminist digilantism is situated in post-#MeToo context: these initiatives raise awareness of longlasting acceptance of sexual harms across countries and contexts. Yet, feminist digilantes frequently encounter regressive denunciations and abuse online. At the same time, digilantism that targets women more generally also prevails, including among migrant communities from Central Asia (Gabdulhakov, 2019). Women in China may also be denounced by being placed into established sexist tropes, including "the ungrateful traitor, the corrupt elite, and the ugly slut" (Huang, 2023: 1). Here, no tangible crime may be committed, but moral policing may blend into criminal policing. Users may take offense on nationalist and gendered grounds, at which point they search for additional reasons to denounce and punish targets.

Progressive reckonings also happen in response to police violence against minorities, which has historically failed to receive appropriate justice. This is more openly acknowledged in the wake of the Black Lives Matters movement. In addition to denouncing police, digilantes target individuals who engage in illegal or immoral actions against minorities (Williams, 2020). Yet anti-Black digilantism also pervades. Consider the anti-scamming digilantism of 419eater.com in which members reply to suspected Nigerian scammers by "invok[ing] more traditional antiblack vigilante aesthetics" (Byrne, 2013: 78). The same tools and practices are used to target both racist and antiracist initiatives.

Digilantism often reflects political polarization in civilian mobilizations. Regressive and progressive movements invoke digilantism when making appeals to law and order, which can serve to promote broader social and political movements. It is important to note that for some digilante groups, "the core of their existence involves a physical presence in public space" (Vicenová, 2020: 249), such as those in Slovakia engaging in anti-Roma and anti-migrant vigilantism. The term 'societal vigilantism' suggests that for far-right participants, the "target is not deviant behaviours but collective attributes perceived as deviant" (Tanner and Campana, 2020: 263). Beyond selective 'crime fighting', far-right vigilantes position themselves as "soft leaders" within "information bubbles" (Tanner and Campana, 2020: 276). Selective 'crime fighting,' then, extends into social movements and collective identity construction (Johnston, 1996) to perpetrate violence against marginalized communities. Digilantism covers a range of contexts involving progressive and regressive extrajudicial attacks on wrongdoers. It can be used as tool to either minimize or scale up categorical harms. This leads to concerns about ethics over the appropriateness of digilantes doxing avowed fascists (Douglas, 2020; Milbrandt, 2020).

Another concern with the term digilantism is the relation and potential overlap with other digital practices. Digilantism coexists with digital activism: activists can easily shame and denounce targets as part of a broader repertoire. Targets may be individuals, but are likely to also include corporations and states. Conversely, digilantes may label themselves as activists depending on their socio-political ambitions (Gabdulhakov, 2020). They may engage in activist practices, especially mediated and communicative ones. At the same time, they may continue to bring attention to perceived wrongdoers. This may be both for the sake of restoring order, and to legitimate their cause. Digilantism may also resemble cyber-bullying: denunciation of a target may be invoked as moral justification for bullying (cf. Loveluck, 2020). But cyber-bullies and other malicious actors may simply fabricate legal and moral charges against a target, for instance when engaged in 'swatting' (sending police to a target's house on false pretences). We can also consider that some participants in digilante campaigns may seek to abuse others under morally justifiable conditions.

Finally, we can ask what counts as participation in digilantism? This varies from initiating campaigns against targets and making physical interventions, to adding views, likes, and comments to a viral video, and thus joining a collective audience. Leading and contributing to digilante activities typically amounts to content generation practices (Favarel-Garrigues, 2020). We can extend the notion of participation to consider the role of media platforms and the press in directing mediated attention to cases of digilantism. Content creators, tabloids, and other media actors report and editorialize on the offense, the vigilante retaliation, and any social or legal fallout (Trottier, 2020). These incidents propel a digital media economy based on engagement. In turn, public understandings of crime and punishment are shaped not only by media entities, but in a way that narrows the focus to the alleged moral failings of individuals, and other often unnamed masses of individuals who are said to punish them.

Conclusion

The term digilantism evokes several forms of ambivalence that warrant further attention:

- Digilantism transcends an online/offline distinction, as incidents can be fully mediated on digital platforms, all while bearing material impact on local communities.
- While digilantism is often a response to criminal events, digital media users can also mobilize against moral offences with the same repertoires.
- These pursuits may reflect progressive as well as regressive notions of justice, notably in polarized contexts.
- Police and other state actors may choose to support or to sanction these endeavors.
- Taken together, digilantism remains a troubling mix of justice seeking and entertainment.

Crime and entertainment media have a long history of being intertwined, through various initiatives that include crime-based reality television. Scrutiny and denunciation of others spills across contexts, including fandoms. Not only does denunciation become a form of entertainment, but entertainment itself becomes denunciation entertainment when anti-fans pursue justice via cancellation of celebrities (Ng, 2022).

Suggested reading

Loveluck, B. (2020). The many shades of digital vigilantism. A typology of online self-justice. *Global Crime*, 21(3 – 4), 213 – 241.

Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston marathon bombings. *British Journal of Criminology*, 57(2), 341 – 361.

Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology*, 30, 55 – 72.

Trottier, D., Gabdulhakov, R., & Huang, Q. (eds.) (2020). *Introducing Vigilant Audiences.* Cambridge: Open Book Publishers.

References

Abrahams, R. (1998). *Vigilant Citizens: Vigilantism and the State.* Cambridge: Polity.

Byrne, D. N. (2013). 419 digilantes and the frontier of radical justice online. *Radical History Review*, 2013(117), 70 – 82.

Chalfaouat, A. (2020). Empowerment, social distrust or co-production of security: A case study of digital vigilantism in Morocco. In D. Trottier, R. Gabdulhakov, & Q. Huang (eds.), *Introducing Vigilant Audiences* (pp. 161 – 186). Cambridge: Open Book Publishers.

Chang, L. Y., & Poon, R. (2017). Internet vigilantism: Attitudes and experiences of university students toward cyber crowdsourcing in Hong Kong. *International Journal of Offender Therapy and Comparative Criminology*, 61(16), 1912 – 1932.

Dekker, R., & Meijer, A. (2020). Citizens as aides or adversaries? Police responses to digital vigilantism. In D. Trottier, R. Gabdulhakov, & Q. Huang (eds.), *Introducing Vigilant Audiences* (pp. 281 – 305). Cambridge: Open Book Publishers.

Dennis, K. (2008). Viewpoint: Keeping a close watch – The rise of self-surveillance and the threat of digital exposure. *The Sociological Review*, 56(3), 347 – 357.

Douglas, D. M. (2020). Doxing as audience vigilantism against hate speech. In D. Trottier, R. Gabdulhakov, & Q. Huang (eds.), *Introducing Vigilant Audiences* (pp. 259 – 279). Cambridge: Open Book Publishers.

Favarel-Garrigues, G. (2020). Digital vigilantism and anti-paedophile activism in Russia. Between civic involvement in law enforcement, moral policing and business venture. *Global Crime*, 21(3 – 4), 306 – 326.

Gabdulhakov, R. (2019). In the bullseye of vigilantes: Mediated vulnerabilities of Kyrgyz labour migrants in Russia. *Media and Communication*, 7(2), 230 – 241.

Gabdulhakov, R. (2020). Heroes or hooligans? Media portrayal of StopXam (Stop a Douchebag) vigilantes in Russia. *Laboratorium*, 11(3), 16 – 45.

Gainford, A. L. (2022). *The Challenges of Digilantism for Law Enforcement and Public Order* (Doctoral dissertation, University of Leeds).

Galleguillos, S. (2022). Digilantism, discrimination, and punitive attitudes: A digital vigilantism model. *Crime, Media, Culture*, 18(3), 353 – 374.

Hadjimatheou, K. (2021). Citizen-led digital policing and democratic norms: The case of self-styled paedophile hunters. *Criminology & Criminal Justice*, 21(4), 547 – 565.

Huang, Q. (2023). The discursive construction of populist and misogynist nationalism: Digital vigilantism against unpatriotic intellectual women in China. *Social Media+ Society*, 9(2). https://doi.org/10.1177/20563051231170816

Huey, L., Nhan, J., & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice*, 13(1), 81 – 97.

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

Jane, E. A. (2017). “Dude … stop the spread”: Antagonism, agonism, and #manspreading on social media. *International Journal of Cultural Studies*, 20(5), 459 – 475.

Johnston, L. (1996). What is vigilantism? *The British Journal of Criminology*, 36(2), 220 – 236.

Loveluck, B. (2020). The many shades of digital vigilantism. A typology of online self-justice. *Global Crime*, 21(3 – 4), 213 – 241.

Madsen, M. L. (2004). Living for home: Policing immorality among undocumented migrants in Johannesburg. *African Studies*, 63(2), 173 – 192.

Mano, W. (2010). Between citizen and vigilante journalism: ZimDaily’s Fair Deal Campaign and the Zimbabwe crisis. *Communicare: Journal for Communication Sciences in Southern Africa*, 29(sed-1), 57 – 70.

Milbrandt, T. (2020). ‘Make them famous’: Digital vigilantism and virtuous denunciation after Charlottesville. In D. Trottier, R. Gabdulhakov, & Q. Huang (eds.), *Introducing Vigilant Audiences* (pp. 215 – 258). Cambridge: Open Book Publishers.

Myles, D., Benoit-Barné, C., & Millerand, F. (2020). ‘Not your personal army!’ Investigating the organizing property of retributive vigilantism in a Reddit collective of websleuths. *Information, Communication & Society*, 23(3), 317 – 336.

Ng, E. (2022). *Cancel Culture: A Critical Introduction.* Cham: Palgrave Macmillan.

Plesničar, M. M., & Šarf, P. (2020). ‘This web page should not exist’: A case study of online shaming in Slovenia. In D. Trottier, R. Gabdulhakov, & Q. Huang (eds.), *Introducing Vigilant Audiences* (pp. 187 – 213). Cambridge: Open Book Publishers,

Reichl, F. (2019). From vigilantism to digilantism? In B. Akhgar, P. S. Bayerl, & G. Leventakis (eds.), *Social Media Strategy in Policing: From Cultural Intelligence to Community Policing* (pp. 117 – 138). Cham: Springer International Publishing.

Rosenbaum, H. J., & Sederberg, P. C. (1974). Vigilantism: An analysis of establishment violence. *Comparative Politics*, 6(4), 541 – 570.

Schwarz, K. C., & Richey, L. A. (2019). Humanitarian humor, digilantism, and the dilemmas of representing volunteer tourism on social media. *New Media & Society*, 21(9), 1928 – 1946.

Shearing, C., & Wood, J. (2003). Nodal governance, democracy, and the new ‘denizens’. *Journal of Law and Society*, 30(3), 400 – 419.

Solove, D. J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet.* New Haven: Yale University Press.

Tanner, S., & Campana, A. (2020). “Watchful citizens” and digital vigilantism: A case study of the far right in Quebec. *Global Crime*, 21(3 – 4), 262 – 282.

Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology*, 30, 55 – 72.

Trottier, D. (2020). Denunciation and doxing: Towards a conceptual model of digital vigilantism. *Global Crime*, 21(3 – 4), 196 – 212.

Vicenová, R. (2020). The role of digital media in the strategies of far-right vigilante groups in Slovakia. *Global Crime*, 21(3 – 4), 242 – 261.

Williams, A. (2020). Black memes matter: #LivingWhileBlack with Becky and Karen. *Social Media + Society*, 6(4). https://doi.org/10.1177/2056305120981047.