Philos. Technol. (2017) 30:55–72
DOI 10.1007/s13347-016-0216-4

RESEARCH ARTICLE

Digital Vigilantism as Weaponisation of Visibility

Daniel Trottier[1]

Received: 6 November 2015 / Accepted: 16 March 2016 / Published online: 1 April 2016

Abstract This paper considers an emerging practice whereby citizen's use of ubiquitous and domesticated technologies enable a parallel form of criminal justice. Here, weaponised visibility supersedes police intervention as an appropriate response. Digital vigilantism is a user-led violation of privacy that not only transcends online/offline distinctions but also complicates relations of visibility and control between police and the public. This paper develops a theoretically nuanced and empirically grounded understanding of digital vigilantism in order to advance a research agenda in this area of study. In addition to literature on vigilantism and citizen-led violence, this paper draws from key works in surveillance (Haggerty and Ericsson, *British Journal of Sociology, 51*, 605–622, 2000) as well as visibility studies (Brighenti 2007; Goldsmith, *British Journal of Criminology, 50*(5), 914–934, 2010) in order to situate how digital media affordances and cultures inform both the moral and organisational dimensions of digital vigilantism. Digital vigilantism is a process where citizens are collectively offended by other citizen activity, and coordinate retaliation on mobile devices and social platforms. The offending acts range from mild breaches of social protocol to terrorist acts and participation in riots. The vigilantism includes, but is not limited to a 'naming and shaming' type of visibility, where the target's home address, work details and other highly sensitive details are published on a public site ('doxing'), followed by online as well as embodied harassment. The visibility produced through digital vigilantism is unwanted (the target is typically not soliciting publicity), intense (content like text, photos and videos can circulate to millions of users within a few days) and enduring (the vigilantism campaign may be top search item linked to the target, and even become a cultural reference). Such campaigns also further a merging of digital and physical spaces through the reproduction of localised and nationalist identities (through 'us/them' distinctions) on global digital platforms as an impetus for privacy violations and breaches of fundamental rights.

✉ Daniel Trottier
trottier@eshcc.eur.nl

[1] Department of Media and Communication, Erasmus University Rotterdam, PO Box 1738, 3000 DR Rotterdam, The Netherlands

Keywords Vigilantism · Digital media · Internet · Surveillance · User led surveillance

1 Introduction

In 2013, Gary Cleary hanged himself in Leicestershire, UK after being pursued by *Letzgo Hunting*, an online group that exposes suspected paedophiles. Likewise, in 2015, Walter James Palmer faced global outrage including numerous death threats after being identified as the killer of a beloved lion in Zimbabwe. Both individuals were targeted by a clandestine form of criminal justice: digital vigilantism (DV). DV is a process where citizens are collectively offended by other citizen activity, and respond through coordinated retaliation on digital media, including mobile devices and social media platforms. The offending acts range from mild breaches of social protocol (bad parking; not removing dog faeces) to terrorist acts and participation in riots. These offensive acts are typically not meant to generate large-scale recognition. Therefore, the targets of DV are initially unaware of the conflict in which they have been enrolled.

This vigilantism includes, but is not limited to, a 'naming and shaming' type of visibility. This typically involves sharing the targeted individual's personal details by publishing them on a public site ('doxing'), including sensitive details such as the target's home address, work details as well as financial and medical information. The nature and source of this information may vary greatly, and may also implicate family members and associates. Such weaponised visibility is an example of citizens leveraging digital media for particular socio-political ends (Castells 2012). These ends include conventional justice through police or other legal channels, as well as unconventional justice such as online harassment and petitioning the target's workplace in order to terminate their employment. The visibility produced through DV is unwanted (the target is typically not soliciting publicity), intense (content like blog posts, photos and video evidence can circulate to hundreds of thousands or even millions of users within a few days) and enduring (the vigilantism campaign may be the first item to appear when searching the individual's name, and may become a cultural reference in its own right). DV can be fuelled by the circulation of misinformation (Starbird et al. 2014), such as when a target is misidentified as a suspect or offender. Moreover, there is evidence that such falsehoods circulate with greater volatility than truthful details (Lotan 2012). Yet it is also the accuracy and ease of collection and circulation of personal details that stands as a troubling factor when assessing DV's societal consequences.

While DV does not supplant conventional vigilantism, it is informed by such practices alongside a broader digital media culture that privileges user-generated content and communities as forms of 'engagement' and 'empowerment'. Likewise, it is informed by how digital media users engage with civic practices, notably in their policing of online spaces, as well as broader engagements with police and state actors. To this end, any distinction made between 'users' and 'citizens' when appraising DV campaigns warrants scrutiny. These factors mark a conceptual departure from conventional vigilantism, and as such must be considered as a matter of definitional concern. For example, lowered barriers to publishing and online coalescence imply that we can expect to find a broader range of political views expressed through DV campaigns. Yet there is also evidence to suggest that the digitalisation of vigilantism will facilitate a

reproduction of law and order politics and conservative social views found in conventional vigilantism (Schneider and Trottier 2012).

This paper reconsiders contemporary surveillance and visibility on digital media in light of the emergence of digital vigilantism. While surveillance is conceptually linked to top-down impositions ranging from Bentham's guard tower to Snowden's revelations about the Five Eyes intelligence regime, user-led surveillance practices may supplement or even contest such regimes. Following scholarly accounts of sousveillance (Mann et al. 2003) and surveillant assemblages (Haggerty and Ericson 2000), the relationship between 'big brother' and 'little sisters' warrants further scrutiny. Through DV, a more distributed network can be enrolled to identify targets, sidestepping privacy settings and legal safeguards through the efforts of willing social actors. One of the core challenges in approaching DV is to arrive at a cogent understanding of this phenomenon while resisting 'the easy reification and reductions of vigilante activity' (Burr and Jensen 2004, p. 143). This paper returns to literature on vigilantism as well as related sub-fields to consider how its features are either reproduced or transformed through digital media. The following section considers these definitional concerns, and is followed by conceptual overviews of three interrelated perspectives towards understanding how emerging forms of vigilantism force a reconsideration of surveillance practices. DV is a product of digital media platforms and user-generated cultural practices. It is also an enactment of citizenship that both contests and reinforces forms of state power and policing. Finally, DV is a matter of rendering a targeted individual visible, with implications for surveillance studies.

2 Definitional Concerns

DV is represented in news media as a series of high-profile incidents that reflect an ideal type (Mann 2011; Madrigal 2013; Booth 2013), but it is also connected to a broader tendency that is informed by media logics and manifest as a set of practices that reflecting one or many features of an ideal type. As stated above, DV is a form of mediated and coordinated action. Its point of departure is moral outrage or a general sense of offence taking, typically towards an act that has been captured and transmitted via mobile devices and through social platforms. In response to this offence taking, users seek to render a targeted individual (or category of individual) visible through information sharing practices such as assembling and publishing their personal details ('doxing'). This response is typically led by individuals who may temporarily coalesce, for example, on a Facebook group, but are otherwise unaffiliated with a formal organisation. DV campaigns are driven by a range of criminological motivations, including responding to criminal events as well as the prevention and deterrence of potential transgressions. For example, the 2011 Vancouver Riot Facebook group justified its coordinated action as identifying suspected rioters, but also claimed 'this page is as strong a deterrent you will find to prevent this from happening again' (Vancouver 2011). Yet DV campaigns also pursue informational goals such as the identification of a targeted individual or category of individual, as well as articulating an understanding about shared norms and values, and consequently expressing a mediated collective identity that may be informed by national, religious or ethnic forms of solidarity.

At this exploratory stage, it is possible to distinguish between cases (a) that are wholly excluded from police work, and those that may (indirectly) inform police and state actions, (b) that are restricted to a regional context, and those that are not tethered to offences in a particular region, (c) that involve exclusively digitally mediated responses, and those that also include embodied actions such as visiting a target's residence, (d) that are largely presented as socially beneficial in public discourse, and those that are framed as harmful, (e) that are one-off responses not linked to an enduring socio-political movement, and those that emanate from established movement, and (f) that allow the targeted individual to communicate with digital vigilantes on mediated platforms, and those that exclude targets from participation. It is also possible to distinguish between cases (g) that follow relatively high-profile offences such as terrorist acts or riots, and those that in response to more mundane infractions such as bad parking or poor transit etiquette. We may expect that by virtue of the nature of the offending acts and the motivation of DV participants as well as other social actors such as the news media, the former would generate a greater amount of content and visibility in a comparatively limited period of time, but that this content may quickly be removed from social platforms due to legal, ethical and moral reasons (Reddit 2015). While evidence of such campaigns may be removed, news media coverage will likely remain, and will include information about individual targets and their alleged offending acts. In contrast, campaigns that target comparatively mundane offences may exhibit all or many of the same characteristics of vigilantism, but with participants and critics expressing less concern for privacy and proportionality.

In order to speculate in which ways DV departs from conventional embodied vigilantism, we may return to Les Johnston's (1996) six elements of vigilantism and consider how each of these features is reinforced, augmented or contested through digital media. First, there must be some degree of planning and premeditation on the part of instigators, such that an act of spontaneous self-defence would not be considered as vigilantism. While this remains the case with DV, digital media affordances greatly facilitate comparatively spontaneous coordination, such that material, spatial and temporal barriers are obviated. Second, Johnston identifies private voluntary agency as a core requirement. In other words, vigilant agents must be distinguished from police and state actors, as well as private entities which nevertheless 'function within the legal ambit of the state' (ibid., 225). With DV, the relationship with police is complicated, as the latter may make appeals to the public for information that may trigger vigilante responses (as in the *Kopschopper* case in the Netherlands, where a group attack on a youth was captured by CCTV and circulated to the public), or may otherwise make use of data collected by DV efforts. These developments are far from the first instance of police-public cooperation, yet digital media facilitate a repurposing of police appeals or content for extrajudicial goals. In addition, private entities such as social platforms are arguably complicit actors in DV campaigns insofar as they facilitate such coordination. Third, conventional vigilantism is understood as a form of 'autonomous citizenship' (ibid., 226) whereby citizens engage in self-protection within a given territory. As DV in practice connects embodied incidents (e.g. offences within a given jurisdiction) with a communicative realm that exceeds that territory, we may consider that the notion of citizenship is complicated, though not necessarily ruptured. Fourth, vigilantism involves the (threatened) use of force. While DV initiatives may contribute to embodied violence, its key tactic is a form of cultural violence (Galtung 1990) that simultaneously

renders targets visible and legitimates accompanying forms of violence, including the structural foreclosure of life chances (Gandy 2009). Fifth, Johnston notes that vigilantism 'arises when some established order is perceived to be under threat from the transgression (or potential transgression) of institutionalized norms' (1996, p. 229). Once again, with DV, the ability to oversee other geographic and cultural contexts greatly complicates the practice of asserting a singular established order. In other words, DV is less a matter of policing a local public space with local norms, but rather a fusion of localised publics with cross-contextual information sharing practices and norms that are manifest on digital platforms. Sixth, vigilantism serves to assert personal and collective security by providing 'the assurance that an established system of order will prevail' (ibid., 231). While this may remain the case with DV, we may question how the boundaries of the collective are asserted.

Following this brief overview that is summarised in the following table, Johnston's six features appear to be generally upheld. Yet the way these features are manifest through digital media amounts to a re-articulation of the boundaries of the collective (Table 1).

In considering the emergence of DV from conventional vigilantism, it appears that the further mediatisation of such campaigns imposes a number of consequences, notably in terms of how citizenship and policing are re-articulated in context that merge localised environments with deterritorialized platforms (Harvey 1989). What follows is a review of recent relevant literature in areas of vigilantism, crime media culture and online policing, in order to advance an understanding of DV as the practice of citizenship through user-led surveillance. These overviews will in turn inform an understanding of DV's weaponisation of visibility as an area of concern for surveillance studies.

3 Digital Media Affordances and Cultural Practices

DV is situated with a broader media culture of users being able to organise online (smart mobs, crowdsourcing), amongst an expansive and ever-asserting informational infrastructure (big data, smart cities), and may facilitate social harms (cyber-bullying, revenge porn, cyber-stalking, online harassment). The range and characteristics of DV is partly informed by these conditions, while often also being articulated as a response

Table 1 Key features of conventional and digital vigilantism

	Conventional vigilantism (Johnston 1996)	Digital vigilantism
Planning	Premeditation	Facilitated spontaneity
Private agency	Distinguished from state and corporate actors	Possible connections with state and corporate actors
Autonomous citizenship	Self-protection	Asserting new boundaries
Use of force	Embodied	Visibility as weapon
Reaction to crime/deviance	Threat of established order	Fusion of local and mediated norms
Personal and collective security	Policing localised territory	Mediated policing

to the above harms. DV is facilitated by a lowered threshold for coordinated action on digital platforms that is often manifested through crowdsourcing initiatives (Slavkovik et al. 2015). The convergence of formerly distinct social spheres on platforms such as Facebook and Twitter offer new organisational possibilities, but also lack of control over the scope and severity of a campaign by any single social actors. Lowered threshold for mediated intervention means that attempts to reproduce offline community often falter, either failing to elicit support or vastly exceeding boundaries and a proportionate response to a perceived offence. These possibilities are governed by media logics associated with social platforms (van Dijck and Poell 2013; Altheide and Snow 1979), alongside discursive formations of smart cities and big data, as well as broadcast media representations of crime and citizen participation (Huey et al. 2012; Rose and Fox 2014). These contribute to what Lanier (2006 in Dennis (2008, p. 354)) identifies as the 'strange allure of anonymous collectivism'.

Digital media such as social platforms and mobile devices allow for an amplification of peer-to-peer communication, providing greater access to personal information as well as allowing the circulation of such information. This has shaped practices such as file-sharing, fundraising and political mobilisation. Indeed, online mobilisation is an emergent phenomenon that crosscuts digital media platforms and collective behaviour (Shirky 2008; della Porta 2013). Recent examples include members of social news platform Reddit sending dozens of pizzas to a 2-year-old cancer patient in 2013, as well as two spontaneous campaigns to reverse the dramatic price rise of Daraprim and cycloserine, two drugs respectively prescribed for treating HIV and tuberculosis. The former campaign notably prominently featured the identification and shaming of Martin Shkreli a hedge fund manager who initiated the price jump. In these cases, individual social actors effect social change, and bypass typical state and media channels in the process, while relying instead on privately run social media platforms.

Contemporary interpersonal culture is shaped by the ability to monitor and intervene in the lives of others (Andrejevic 2007; Niedzviecki 2009). Social platforms like Facebook, Twitter and Reddit allow citizens to discuss a targeted individual, publish their personal details and issue calls for action. In addition, mobile devices such as smart phones enable real-time recording and transmission of an offending act to other citizens. Previous research considers the crowdsourcing of surveillance practices on digital media (Trottier 2013a), as well as the changing nature of policing and visibility online (Trottier 2012a). These research streams suggest that bottom-up forms of organisation are facilitated by social platforms and that policing is changing as a result of digital media, which in turn shapes how these technologies are used. What remains to be investigated is how user-led surveillance practices intersect with police and institutional monitoring of digital media. DV occurs in a cultural context where users are coming to terms with the relation between online activity and offline consequences. While the 'early web' was characterised by a perceived distinction between online and offline in terms of the exercise of power (Jordan 1999), the emergence of social, geo-located and ubiquitous media has led to a dissolution of this distinction, to the extent that digital media activity can have lasting consequences in both local and global contexts. Thus, DV participants may not be aware of the actual impact of their actions (Ronson 2015). It is also important to note that DV is as much a communicative and mediated act as it is a collective enactment of social order. In other words, vigilantism on digital media can be framed in the context of online communication: the sharing of

personal details, photos and videos, adding commentary, discussion and calls for action. However, all of these actions culminate in a coordinated mass persecution of a targeted citizen.

Emerging affordances with digital media inform changing cultural expectations and practices by users, and in particular a renegotiation of the perceived appropriateness of the disclosure and circulation of other citizen's personal information. Concepts such as sharing (Meikle and Young 2012), but also privacy and proportionality, are necessarily reconsidered. Sites that rely on user-generated content are now amongst the most popular on the web. The fact that users embrace these services suggests that they are drawn to information their peers give and give off (Goffman 1959), and are occasionally compelled to provide their own content. Users clearly value the interpersonal benefits of new media technologies (Ellison et al. 2007), even if these benefits are part of a persistent campaign from software, hardware and telecommunication companies to generate demand for their platforms and services (Mosco 2004). Yet an increase in online sharing of personal information—as evidenced from the growth of services like Facebook, Twitter and Instagram—contributes to DV, as they provide both a platform and a set of practices that render DV meaningful and practical.

The meaning underlying 'social' in social media is a conceptual quagmire, yet the social connectivity they offer is a germane point of departure. Social media is shorthand for 'social convergence media', in that these services can bring together formerly discrete fragments of users' everyday life, leading a collapse of sociocultural contexts (Marwick and boyd 2011). Media boundaries determine behavioural patterns, and converging media will 'foster integrated behavioural patterns' (Meyrowitz 1990, p. 94). The act of converging formerly distinct behavioural patterns can amplify DV if behaviour in one context is deemed objectionable and actionable in another. This connectivity is framed in a broader cultural context of network sociality, where professional and personal spheres increasingly overlap (Wittel 2001). Social media sites are a means to consolidate users' social lives and identities, both of which have typically remained fragmented. The Internet used to be treated as a space that was distinct from the offline world. Now, the distinction between online and offline is largely obviated (Jurgenson 2012). The contemporary web connects formerly distinct sections of users' lives. This connection is even more pervasive with the prominence of mobile devices allowing users to submit and access content virtually anywhere. This convenience means that sharing may supersede reflecting. While users may exert a temporal buffer between reflection and presentation on social media (Davis 2010), this reflection is likely contextualised with a particular audience in mind. The fact that this imagined audience might not be the entire audience indicates how social media communication can facilitate DV.

Whereas the early web was understood in terms of anonymity and freedom from discrimination, the rise of social media has several features that suggest a closer and more complicated relation between individual users as well as institutions. These in particular result in a preponderance for online stigma (Trottier 2013b), as well as a compromised personal reputation (Solove 2007). Yet even if comparatively removed from an embodied setting, the early web was also characterised by practices of self-policing (Huey et al. 2012), whereby users asserted the boundaries of acceptable conduct. Though traditionally contained to the monitoring and policing of online conduct, social platforms and mobile media in particular render embodied acts and

infractions visible as well, and subject to collective editorialising and intervention through DV. For example, a Facebook group entitled *Dublin Bad Parking* (https://www.facebook.com/dublinparking/) directs attention not only to individual violators but also a localised spatial setting through the designation of problematic streets. Contextual convergence through social and mobile media also brings a transition from users policing the Internet, to users policing through the Internet. Not only do digital media platforms enact information flows amongst users, many also serve in practice and often in as news platforms that report and offer commentary on DV events. Platforms like Reddit may serve an acute role in, following earlier literature on media and vigilantism, lowering public confidence in states' abilities to manage crime and deviance (Davis 2006, p. 65; in Kucera and Mares 2015), emboldening users to become actively engaged with such offences (Huey et al. 2012, p. 87), and may follow a crime news media legacy of 'orchestrating a kind of virtual vigilantism, in which a proxy audience is constructed to celebrate vengeance against the perpetrators of unmitigated evil' (Reiner 2008, p. 5).

DV seeks to identify and shame unmitigated evil in embodied contexts, yet it also maintains an earlier digital media culture focus on online infractions. Thus, it reflects an often-negative assessment of digital media practices, including related phenomena such as cyber-bullying. Cyber-bullying refers to when users (typically youngsters) harass and intimidate other users through digital media. This poses a challenge for researchers and all stakeholders: DV and cyber-bullying are conceptually similar, as both are forms of online persecution. Yet DV can come as a response to cyber-bullying. For example, following the 2012 suicide of Canadian teenager Amanda Todd, an online community sought and published the personal details of the alleged bully (CBC 2012). While DV may be similar to cyber-bullying, it is often framed in terms of a moral compass (which may betray nationalist, racist, sexist or xenophobic tendencies). Both phenomena are related to media education, in that awareness of risks and guidelines are key to managing these problems. Subsequent research should further a theoretically and empirically grounded understanding of DV that situates it in relation to cyber-bullying, in order to address both issues as a matter of public policy and media education.

4 User/Citizen-Led Vigilantism as Critical Reinforcement of Law and Order

Vigilantism is framed as a kind of 'private violence' (Culberson 1990) or everyday policing (Burr and Jensen 2004) whereby citizens seek to assert their own form of criminal justice. Whereas the state is said to hold a monopoly on violent activity, through vigilantism citizens deny this state monopoly in an attempt to legitimate their own violent acts. In the case of digital media, this legitimation is explicitly posted as text, image and video content. Vigilantism more generally is typically fuelled by lowered public confidence in police and criminal justice (Haas et al. 2014), and in particular tends to follow a rhetoric that openly exhibits a 'disdain for due process' (Martin 2009, p. 147) notably in the wake of high-profile crimes. For example, the emergence of the Guardian Angels in the USA was a response to outrage following the murder of Catherine 'Kitty' Genovese in 1964. Police may stand as target of criticism, but more generally the role of the state, and the boundaries of acceptable state

intervention are scrutinized and contested by individual non-state actors. However, parallel developments such as neighbourhood watch programmes shared the Guardian Angels' desire for citizen-led safety, albeit with mutually endorsing relations with police and the state (Johnston 1996).

In terms of the role of emerging media, we may consider how independent outlets offer a perceivably more accurate extent of crime (Davis 2006). Lowered confidence in state actors is bound to a diminished control over information exchange amongst these actors. This is especially noticeable in comparatively public and visible facets of criminal justice, such as police work. Thompson (2005, p. 31) reports on how emerging technologies coupled with shifts in both political and journalistic cultures contributes to a 'new world of mediated visibility' that complicates conventional attempts to restrict or control information flows. Heightened visibility of scandal is now a general condition for governance, and policing in particular (Goldsmith 2010). In addition to publicizing and circulating critiques of police procedure, so too may DV campaigns target other institutional actors that are perceived to be complicit in the neglect of criminal justice. In the case of cyber-bullying and revenge porn, social platforms as well as telecommunications companies may come under criticism for failing to react to such crimes occurring through their infrastructure (Wilkinson 2009). DV campaigns are partly an expression of frustration towards visible evidence of police neglect and misconduct, but also in response to the functional opacity of platforms in which many crimes are either mediated or manifest. Such a desire to intervene in both the policing and securitisation of digital media stands as a pushback against the 'cherished goal of many engineers to *get the humans out of the loop*' of securitization and monitoring practices (Marx 2013, p. 57).

While both DV and conventional vigilantism are typically framed as a critical response against the state, DV's relation to a given state's socio-political climate is more complex, and often is ultimately supportive of the state and the enactment of law and order. Vigilantism is typically understood as extra-state, popular and extra-legal, yet it takes on 'state-like performances such as security enforcement' along with 'a perpetual renegotiation of the boundaries between state and society' (Burr and Jensen 2004, p. 144). Vigilantism does not mark a rupture from state and policing, but rather a renegotiation of acceptable boundaries, citizens acting in a way they believe the state should, to an extent blurs the boundaries between state and populist action (Lund 2001). Vigilantism in this context involves a criticism of state performance, alongside an alignment with state objectives. While lacking state authorization, vigilante groups 'do not perceive their actions as over-riding or transgressing the legal order but construct themselves as self-anointed guardians rescuing national sovereignty, citizenship and the law's moral sanctity, from cultural elites, moneyed interests, inept bureaucrats and a sclerotic state'. (Walsh 2014, p. 13). DV thus raises a curious dynamic in public perception of—and intervention in—policing, as participants may enact national sovereignty and citizenship on digital media that by definition exceed the scope and jurisdiction of any nation. While this complicates attempts by police to investigate crimes through social media (Trottier 2015), users and DV participants in particular may nevertheless expect some kind of (self-)policing of and through these platforms. As many users are immersed in a digital media culture that implicitly or explicitly prescribes self-policing online, the gradual dissolution of online/offline distinctions may lead to users employing a kind of self-reliant approach when embodied crimes and

transgressions are mediated (Huey et al. 2012). This dynamic is most notable in cases where the perceived crime retains an online dimension, as in cases of cyber-bullying or revenge porn. As a transgression that many users perceive as criminal, it holds relatively little legal meaning, and police are sceptical or simply understaffed and unable to respond to such cases (Broll and Huey 2015). If cyber-bullying and revenge porn stand as prominent harms in contemporary digital media culture, they may contribute to a perceived vacuum of many institutions failing to address crime in which digital vigilantism emerges (Oomen 2004, p. 156).

DV is situated in a broader media culture of other types of civilian linkages with policing and 'non-rule-based contributions to governance' (Powell 2011, p. 1), and in practice may rely on the same hardware, practices and cultural expectations. These activities include the outsourcing of vigilante activities to 'informal security agencies' that are analogous to private security agencies for those who cannot afford these services (Kucera and Mares 2015, p. 179). These groups typically maintain cooperative relations with the state, for example, by handing over detained culprits to the police. More broadly, DV may be linked to 'a growing neoliberal trend in citizen responsibilisation' (Warren 2009, p. 275). While states may not willingly support vigilantism, recent trends in policing are indicative of nodal governance between government, law enforcement, private industry and the general public, whereby the latter are engaged in 'voluntary ad hoc partnerships with law enforcement' (Huey et al. 2012, p. 83). In the context of border control, the enlistment of private individuals in official gatekeeping efforts (Walsh 2014, p. 1) generates three modalities (deputisation, responsibilisation and autonomisation), each with distinct state-citizen relations as well as a distinction between users being 'invited en masse' and cases where gathering and distributing information about targets is 'self-appointed and unauthorised, even if tacitly accepted' (ibid., 6). States play a role in designation and sanctioning of vigilantism, either condoning or condemning citizen-led policing. It is also worth noting that the term vigilante may be invoked as label by state against those without at least tacit approval, such that prominent members of specific communities can avoid being labelled as such (Martin 2009, p. 143). By designating those who may be regarded as a liability as vigilantes may be a way for state to police the boundaries of policing. Sanctioned and unsanctioned user-led contributions to policing suggest 'a potential collision' (Marx 2013, p. 56) between the exercise of public civic virtue and 'the ambiguated citizen-officer-suspect' that can bypass 'legal restraints and other judicial obstacles that somewhat hinder official state surveillance efforts' (Reeves 2012, p. 245).

DV complicates citizenship through the blurring of boundaries between police and public, as well as through the enactment of national identities and hegemonic cultural values through digital media. Through mediated and 'glocalised' (Wellman 2002) outrage and the sustained visibility of perpetrators, DV campaigns exercise a kind of us/them identity reflecting a 'hegemonic bloc, rallying conservative factions' within society (Oomen 2004, p. 155). Conventional vigilantism is typically bound to a single nation, and often reflects nationalist identity building (Kucera and Mares 2015). This can be seen through the use of nationalist and xenophobic rhetoric, for example, white nationalism amongst Ku Klux Klan members in the USA. Yet due to the coupling of digital media and vigilantism, distance is no longer a barrier in vigilantism or nationalist manifestations (Dennis 2008, p. 356). The backlash to the 2011 Vancouver riot made a

clear distinction between a local 'us' based in downtown Vancouver and an outsider 'them' relegated to the outer suburbs (Schneider and Trottier 2012), even though participants in the campaign themselves were not geographically restricted. Furthermore, DV campaigns may indeed challenge conventional identity-based movements, such as when Anonymous sought to openly identify a thousand KKK members (CBC 2015).

This violence resembles a kind of citizen-led communication counter-power (Castells 2007). In particular, groups like Anonymous appear to pose a challenge to conventional state power (Coleman 2012; Fuchs 2013). Yet the connection between state power and DV is unclear, and forces a reconsideration of state-citizen relations. While there is empowering and emancipatory potential in terms of citizen use of digital media technology, vigilante engagement of digital media also occurs alongside police and other branches of the state asserting greater control over digital media. Vigilantism is commonly understood as a challenge to monopolisation of state power, but also as a reproduction of that power, as police and state power assert greater control over digital media. This is seen through the publishing of guidelines and strategies, as well as legal clarifications and technical enhancement of police practice on digital platforms. Thus, if citizens are empowered in their use of digital media users, states are 'power users' through their ability to aggregate data, target groups and individuals, and partner with private companies that manage these platforms (Trottier 2014).

5 Surveillance and User-Led Regimes of Visibility

Compared to conventional vigilantism, DV makes explicit use of targets' personal information by rendering them visible to public scrutiny. It is informed by (self-)surveillant tendencies located within the contemporary practice of citizenship and policing through digital media. Surveillance implies watching over others, and can be performed by individuals as well as organisations. David Lyon succinctly refers to surveillance as 'processes in which special note is taken of certain human behaviours that go well beyond idle curiosity' (2007, p. 13). Surveillance processes can be broken up into discrete steps: the collection of personal data, the interpretation of that data and social consequences stemming from that assessment. This distinction is important due to temporal as well as contextual gaps between these steps, notably as digital media allow surveillance practices to traverse these gaps. Contemporary surveillance is located in police practices (Marx 1988), emerging technologies such as CCTV cameras and national identity card regimes (Norris and Armstrong 1999; Lyon 2009), as well as micro-level interactions to manage one's identity (Goffman 1959). These contextually disparate practices share a tendency to collect and repurpose information about social actors. Gathering personal information is a prevalent organisational logic contemporary governments and institutions (Dandeker 1990). Surveillance is ubiquitous, not just because of seemingly ever-present digital technologies, but because watching and assessing pervade 'virtually every enduring social relationship' (Rule 2011: 64). While the prevalence of domesticated (Silverstone and Haddon 1996) digital media provides an infrastructure for DV, these depend primarily on interpersonal practices of self-scrutiny and lateral-scrutiny (Andrejevic 2005; Author 2012). Thus, even in maintaining a conceptual distinction between seemingly

neutral monitoring practices and surveillance, it is important to note that information yielded in the former can supplement the latter, given their coexistence on a pervasive digital media landscape.

The convergence of formerly distinct surveillance regimes amplifies the ability to both gather and in turn distribute personal information. This includes merging databases and individual profiles through technological innovation such as converging functionality in hardware or software platforms (Jenkins 2006) or as a result post 9–11 legislation (ex: the 2001 USA PATRIOT Act; Canada's Bill C-51). Such developments facilitate surveillant assemblages (Haggerty and Ericson 2000) that can produce wide-reaching profiles of targeted individuals through temporarily sustained partnerships between social actors. Social media platforms and mobile devices in particular amount to a 'mutual augmentation' of formerly distinct surveillance and information sharing practices (Trottier 2012b). Thus, the fact that DV takes place on these platforms and devices means that it is not only the product of a general informational convergence but that it can also further amplify other forms of surveillance, such as when a potential employer or border agent searches for personal information about a DV target, and finds evidence of the DV campaign and their offending act.

In assessing the societal impact of surveillance, privacy is typically invoked as an individual and collective right 'to determine for themselves when, how and to what extent information about them is communicated to others' (Westin 1967, p. 337), as well as to simply be 'let alone' (Warren and Brandeis 1890). Privacy is also as a cultural value that is redefined and performed through everyday social interactions, for example, by managing secrecy and evading unwanted exposure in everyday mediated and embodied contexts (Nippert-Eng 2010). A common feature to both legally and culturally bound definitions of privacy is the implication of control over personal information flows, a quality that has been greatly complicated with the advent of digital media. DV highlights the complex nature of privacy and public space. It is a private form of violence that at the outset marks a severe privacy violation for the targeted individual. Yet it takes place in platforms that constitute a potential public sphere (Fuchs 2014), even if these are privately owned, and tempered through privacy settings.

DV represents the intersection of digital media culture and contemporary citizenship and policing. In practice, it is informed by existing individually led surveillance that also draw from digital media affordances. In order to understand this culture of mediated policing, it bears reflecting on contemporary practices of managing visibility, including self-visibility. Following historical accounts of surveillance practices that complicate a typical top-down watcher/watched dichotomy (Le Roy Ladurie 1978), digital media affordances and practices inform several subject positions that in turn inform DV practices. Not only are these perspectives stemming from the possibility of data collection being folded into everyday activities through digital media (Marx 2013) but they also indicate a lack of agency when it comes to managing one's own visibility. DV campaigns are by definition unwanted forms of visibility. Yet in terms of information they build upon, they are not entirely distinct from the voluntary disclosure of information, or the celebration of transparent forms of social engagement (Brin 1998). Participatory surveillance refers to a process whereby social media users knowingly share information about themselves, and derive some form of empowerment from this sharing (Albrechtslund 2008; Cascio 2005). This perspective serves as a helpful intervention to scholarly accounts that assume that users unknowingly violate their

privacy when uploading content to social platforms. Indeed, users often yield specific pleasures and values from online sharing, for example, when sharing their exercise details with an online community, alongside other types of life-logging (O'Hara et al. 2008). However, a conceptual as well as practical concern is whether it is possible for a user to fully consent to sharing personal data, given the volatility of platforms, users and mediating devices. As unanticipated risks become embedded in public awareness, we can imagine that these are factored in as a kind of transaction cost associated with participatory surveillance. Thus, an individual may voluntarily disclose information about their workplace and family life, under the guise of empowering visibility. Upon being targeted by a DV campaign, disclosures that were originally a form of empowerment and self-actualization could contribute to further social harm.

As a further departure from the typical watcher/watched framework, sousveillance (Mann et al. 2003) refers to a reversal of the surveillant gaze, whereupon relatively powerless social actors watch (typically recording and transmitting footage of) a more powerful actor. Such practices are linked to recent political movements including Edward Snowden and Chelsea Manning's revelations about government surveillance schemes, as well as cop-watching initiatives (the latter of which takes advantage of social media to render police misconduct visible). While mobile devices and social platforms are used in key political interventions, scholars may question how these uses contest or confirm power differentials. In the case of cop-watching initiatives, consider police adoption of body-worn cameras that provide a more authoritative account of the same incidents (Brucato 2015; Sandhu and Haggerty 2016). Such tendencies to seek out and transmit injustices may easily slip to instances where a power differential is less apparent. As an example, consider the difference between filming a case of police harassing a citizen, and filming a case of a citizen harassing a fellow citizen. Sousveillance is situated in a cultural context where individuals are vigilant firstly towards the self, and secondly towards others (Mann et al. 2003; Dennis 2008, pp. 348–9). Self-scrutiny and scrutiny of others are inextricably linked in contemporary digital media culture.

Under the rubric of empowerment and self-care, users may feel an obligation to watch over their peers. Lateral surveillance refers to a broader cultural condition of individuals monitoring the conduct of other individuals (Andrejevic 2005). As this concept is not limited to social media platforms, it underlines a broader media culture characterised by a lack of trust in the other, coupled with a media savvy that compels individuals to bypass self-presentation through a series of techniques and technologies, including nanny cams and home drug test kits. As so much social interaction now occurs online, it stands to reason that interpersonal interactions are also shaped by this kind of media savvy. A social dynamic that crosscuts the above three concepts is that individuals are watching over other individuals, along with watching over themselves. This implies a broader attempt at control over information flows, and an assertion of informational autonomy. It also speaks to a blurring of the boundary that would otherwise distinguish socializing and surveillance, as both now involve the asynchronous overview of aggregated personal data on social platforms. Thus, persecution of others through DV may be remotely or quite tangibly informed by a culture of 'survivalist individualism' (Andrejevic 2007), whereby self-preservation in any range of contexts depends on watch over others, and publically revealing inconsistent or discrediting behaviours. Consider cohabitation-based reality TV shows where both

contestants and viewers are encouraged to catch other contestants engaged in dishonest and immoral behaviour (Andrejevic 2005). Likewise, migrants seeking to escape scrutiny and persecution in a hostile environment may watch over fellow migrants, and intervene by excommunicating those deemed to be a liability (Madsen 2006).

These subject positions inform routine forms of interpersonal interaction, as well as exceptional coalescence in vigilante campaigns. They not only mark a domestication of technologies that render the self and others visible but also the possibility that the distribution of personal information can become an 'explicit strategy of individuals who know very well that mediated visibility can be a weapon in the struggles they wage in their day-to-day lives' (Thompson 2005, p. 31). DV is distinguished from conventional vigilantism through its primary reliance on weaponised visibility for social change as well as social harm. In the case of the *Kopschopper* incident in the Netherlands, two of the assailants received lesser sentences from the court, on the basis of the social visibility to which they had already been subjected (RTL Nieuws 2013). DV constitutes a severe violation of the targeted individual's privacy and data protection rights, as their personal details are publicly transmitted without their consent. Targets may be selected on the basis of gender and ethnicity. DV also amounts to a kind of criminal justice response that is performed by untrained non-professionals. It challenges police process, and it can undermine perceptions of authority and statehood, while reproducing the worst abuses of state-sanctioned violence. DV is typically manifest as a series of crimes, including harassment, stalking and uttering death threats. Citizens learn to minimise self-harm in terms of uploading their own personal information, but to what extent are they taught not to put others in harm's way? It is crucial that media literacy guidelines teach citizens to recognise the harms in these tendencies.

6 Conclusion

When vigilantism is expressed through digital media, it seeks and circulates targeted offenders' personal information. The purpose of these acts is both informational in the sharing of details about transgressions, but also punitive in the type of visibility wilfully enacted against the target. DV groups typically act in defiance of police, and police typically condemn and prosecute vigilante activity. Yet these relations may resemble a more nodal form of governance, for example when Toronto police reach out to DV hacking communities in order to identify those responsible for the Ashley Madison data breach (Smith Cross 2015). Such potential partnerships may comply with recommendations that police crowdsource the search for data, but not actual investigations (Ackerman 2013), while others believe that both are feasible with effective safeguards (Brabham 2013). In either case, the possibility that social actors appropriate police appeals as a means to harm others remains an area of concern for surveillance studies. These developments suggest that DV should not be regarded as an aberration from other digital media practices, but instead located on a continuum of forms of user-led policing and citizenship.

Social media platforms like Facebook and Twitter are default platforms for interpersonal, but also collective activities. These tendencies are not the sole remit of any single activist or militant organisation. Rather, they are a tendency that can potentially emerge through online communication. DV is also an unmistakably global

phenomenon. In North America, the online response to the 2011 Vancouver riot and the 2013 Boston bombing manhunt profoundly impacted the lives of those who were (wrongly) targeted, and received substantial media coverage. Within the EU, groups like *Letzgo Hunting* and Facebook's *Association of Citizens Saint Sava* mark a reliance on digital media for targeting child exploiters and drug dealers. Likewise, the 'human flesh search engine' in China has featured prominently in public discourse about the Internet (Cheung 2009). In the wake of civil unrest, the MENA region has seen the rise of groups that use digital media to monitor, report and co-ordinate against crimes, including sexual violence. Subsequent research will contribute to conceptual clarity about DV in relation to other user-led practices on digital media. This rests heavily on a theoretically informed understanding of DV, as well as its overlaps with existing phenomena. This will depend on empirical attention to groups, along with media representations of groups, including on hybrid social news platforms such as Reddit and *GeenStijl* that simultaneously serve as platforms where these campaigns are manifest. These developments also mark a categorical blurring between online and offline engagements, local and global participants and contexts, positive as well as between critical public perception, personal details and public interest.

References

Ackerman, S. (2013). Data for the Boston marathon investigation will be crowdsourced. *Wired* 16 April. http://www.wired.com/2013/04/boston-crowdsourced/.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday* 13 (3): http://firstmonday.org/article/view/2142/1949.

Altheide, D. L., & Snow, R. P. (1979). *Media logic*. Beverly Hills: Sage.

Andrejevic, M. (2005). The work of watching one another: lateral surveillance, risk, and governance. *Surveillance & Society, 2*(4), 479–497.

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence: University of Kansas Press.

Booth, R. (2013). Vigilante paedophile hunters ruining lives with internet stings. *The Guardian* 25 October. http://www.theguardian.com/uk-news/2013/oct/25/vigilante-paedophile-hunters-online-police.

Brabham, D. (2013). The Boston marathon bombings, 4Chan's think tank, and a modest proposal for an emergency crowdsourced investigation platform. *Culture Digitally* 17 April. http://culturedigitally.org/2013/04/boston-marathon-bombing-and-emergency-crowdsourced-investigation/.

Brighenti, A. (2007). Visibility: A Category for the Social Sciences. *Current Sociology*, 55(3), 323–342.

Brin, D. (1998). *The Transparent Society: Will technology force us to choose between privacy and freedom?* Reading: Addison-Wesley.

Broll, R., & Huey, L. (2015). "Just being mean to somebody isn't a police matter": police perspectives on policing and cyberbullying. *Journal of School Violence, 14*(2), 155–176.

Brucato, B. (2015). Policing made visible: mobile technologies and the importance of point of view. *Surveillance & Society, 13*(3/4), 455–473.

Burr, L., & Jensen, S. (2004). Introduction: vigilantism and the policing of everyday life in South Africa. *African Studies, 63*(2), 139–152.

Cascio, J. (2005). The rise of the participatory panopticon. *WorldChanging.com*. http://www.worldchanging.com/archives/002651.html.

Castells, M. (2007). Communication, power and counter-power in the network society. *International Journal of Communication, 1*, 238–266.

Castells, M. (2012). *Networks of outrage and hope: social movements in the internet age*. Cambridge: Polity.
CBC. (2012). Amanda Todd's alleged tormentor named by hacker group. *CBC.ca* 15 October. http://www.cbc.ca/news/canada/british-columbia/amanda-todd-s-alleged-tormentor-named-by-hacker-group-1.1134233.
CBC. (2015). Anonymous plans to 'unhood' 1,000 Ku Klux Klan members online. *CBC.ca* 29 October. http://www.cbc.ca/news/trending/anonymous-plans-to-reveal-the-identities-of-1-000-kkk-members-1.3295523.
Cheung, A. S. Y. (2009). China Internet going wild: cyber-hunting versus privacy protection. *Computer Law & Security Review, 25*(3), 275–279.
Coleman, G. (2012). Our weirdness is free, the logic of anonymous—online army, agent of chaos, and seeker of justice. *Triple Canopy*, January. http://gabriellacoleman.org/wp-content/uploads/2012/08/Coleman-Weirdness-Free-May-Magazine.pdf.
Culberson, W. (1990). *Vigilantism: Political history of private power in America*. Westport: Greenwood Press.
Dandeker, C. (1990). *Surveillance, power and modernity: bureaucracy and discipline from 1700 to the present day*. New York: St. Martin's Press.
Davis, D. E. (2006). Undermining the rule of law: democratization and the dark side of police reform in Mexico. *Latin American Politics & Society, 48*(1), 55–86.
Davis, J. (2010). Architecture of the personal interactive homepage: constructing the self through Myspace. *New Media & Society, 12*(7), 1103–1119.
della Porta, D. (2013). *Can democracy be saved: participation, deliberation and social movements*. Cambridge: Polity.
Dennis, K. (2008). Keeping a close watch—the rise of self-surveillance and the threat of digital exposure. *The Sociological Review, 56*(3), 348–357.
Ellison, N., Steinfield, C., Lampe, C. (2007). The benefits of Facebook 'friends': social capital and college students' use of online social network sites. *Journal of Computer Mediated Communication* 12(4). http://jcmc.indiana.edu/vol12/issue4/ellison.html.
Fuchs, C. (2013). The Anonymous movement in the context of liberalism and socialism. *Interface: A Journal for and About Social Movements, 5*(2), 345–376.
Fuchs, C. (2014). Social media and the public sphere. *tripleC, 12*(1), 57–101.
Galtung, J. (1990). Cultural violence. *Journal of Peace Research, 27*(3), 291–305.
Gandy, O. H. (2009). *Coming to terms with chance: engaging rational discrimination and cumulative disadvantage*. Farnham: Ashgate.
Goffman, E. (1959). *The presentation of self in everyday life*. New York: Anchor Books.
Goldsmith, A. J. (2010). Policing's new visbility. *British Journal of Criminology, 50*(5), 914–934.
Haas, N. E., de Keijser, J. W., & Bruinsma, G. J. N. (2014). Public support for vigilantism, confidence in police and police responsiveness. *Policing and Society, 24*(2), 224–241.
Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology, 51*, 605–622.
Harvey, D. (1989). *The condition of postmodernity*. Oxford: Blackwell.
Huey, L., Nhan, J., & Broll, R. (2012). 'Uppity civilians' and 'cyber-vigilantes': the role of the general public in policing cyber-crime. *Criminology & Criminal Justice, 13*(1), 81–97.
Jenkins, H. (2006). *Convergence culture: where old and new media collide*. New York: New York University Press.
Johnston, L. (1996). What is vigilantism? *British Journal of Criminology, 36*(2), 220–236.
Jordan, T. (1999). *Cyberpower: an introduction to the politics of cyberspace*. London: Routledge.
Jurgenson, N. (2012). The IRL fetish. *The New Inquiry*. 28 June. http://the-newinquiry.com/essays/the-irl-fetish.
Kucera, M., & Mares, M. (2015). Vigilantism during democratic transition. *Policing and Society, 25*(2), 170–187.
Lanier, J. (2006). Digital Maoism: the hazards of the new online collectivism. *Edge.org* 29 May. http://www.edge.org/3rd_culture/lanier06/lanier06_index.html.
Le Roy Ladurie, E. (1978). *Montaillou: the promised land of error*. New York: Vintage Books.
Lotan, G. (2012). A tale of three rumors. *Truthiness in Digital Media* 5 March. http://blogs.law.harvard.edu/truthiness/2012/03/05/541/.
Lund, C. (2001). Precarious democratization and local dynamics in Niger: micro-politics in Zinder. *Development and Change, 32*(5), 845–869.
Lyon, D. (2007). *Surveillance studies: an overview*. Cambridge: Polity Press.
Lyon, D. (2009). *Identifying citizens: ID cards as surveillance*. Cambridge: Polity Press.
Madrigal, A.C. (2013). Hey Reddit, enough Boston bombing vigilantism. *The Atlantic* 17 April. http://www.theatlantic.com/technology/archive/2013/04/hey-reddit-enough-boston-bombing-vigilantism/275062/.
Madsen, M. L. (2006). Living for home: policing immorality among undocumented migrants in Johannesburg. *African Studies, 63*(2), 173–192.
Mann, B. (2011). Social media "vigilantes" I.D. Vancouver rioters — and then some. *The Huffington Post Canada* 2 July. http://www.huffingtonpost.ca/bill-mann/vancouver-riot-social-media_b_889017.html.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3), 331–355.

Martin, J. (2009). Vigilantes unmasked: an exploration of informal criminal justice in contemporary South Africa. *Australian & New Zealand Critical Criminology Conference Proceedings*, 142–150. Monash University.

Marwick, A., & Boyd, D. (2011). I tweet honestly, i tweet passionately: twitter users, context collapse, and the imagined audience. *New Media & Society, 13*(1), 114–133.

Marx, G. T. (1988). *Undercover: police surveillance in America*. Berkeley: University of California Press.

Marx, G. T. (2013). The public as partner? Technology can make us auxiliaries as well as vigilantes. *Security & Privacy, 11*(5), 56–61.

Meikle, G., & Young, S. (2012). *Media convergence networked digital media in everyday life*. Basingstoke: Palgrave Macmillan.

Meyrowitz, J. (1990). Redefining the situation: extending dramaturgy into a theory of social change and media effects. In S. Riggins (Ed.), *Beyond Goffman: Studies on communication, institution, and social interaction* (pp. 65–97). New York: Mouton de Gruyter.

Mosco, V. (2004). *The digital sublime: myth, power and cyberspace*. Cambridge: MIT Press.

Niedzviecki, H. (2009). *The peep diaries: how we're learning to love watching ourselves and our neighbours*. San Francisco: City Lights.

Nippert-Eng, C. (2010). *Islands of privacy*. Chicago: University of Chicago Press.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: the rise of CCTV*. Oxford: Berg Publishers.

O'Hara, K., Tuffield, M. M., & Shadbolt, N. (2008). Lifelogging: privacy and empowerment with memories for life. *Identity in the Information Society, 1*(1), 155–172.

Oomen, B. (2004). Vigilantism or alternative citizenship? The rise of Mapogo a Mathamaga. *African Studies, 63*(2), 153–171.

Powell, A. (2011). Emerging issues in internet regulation: the unstable role of WikiLeaks and cyber-vigilantism. In *Research handbook on internet governance*. Cheltenham: Edward Elgar. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1932740.

Reddit. (2015). *Promote ideas, protect people*. 14 May. http://www.redditblog.com/2015/05/promote-ideas-protect-people.html.

Reeves, J. (2012). If you see something, say something: lateral surveillance and the uses of responsibility. *Surveillance & Society, 10*(3/4), 235–248.

Reiner, R. (2008). The rise of virtual vigilantism: crime reporting since World War II. *Criminal Justice Matters, 43*(1), 4–5.

Ronson, J. (2015). How one stupid tweet blew up justine sacco's life. *The New York Times Magazine* 12 February. http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html.

Rose, M., & Fox, R. R. (2014). Public engagement with the criminal justice system in the age of social media. *Oñati Socio-legal Series, 4*(4), 771–798 [online].

RTL Nieuws. (2013). Welke straf krijgen de kopschoppers van Eindhoven? *RTL Nieuws* 11 December. http://www.rtlnieuws.nl/nieuws/binnenland/welke-straf-krijgen-de-kopschoppers-van-eindhoven.

Rule, J. (2011). 'Needs' for Surveillance and the Movement to Protect Privacy. *Routledge Handbook of Surveillance Studies*, edited by Lyon D., Ball, K. and Haggerty, K. D. , 64–71. New York: Routledge.

Sandhu, A. & Haggerty, K. D. (2016). Policing on camera. *Theoretical Criminology* (forthcoming).

Schneider, C., & Trottier, D. (2012). The 2011 Vancouver Riot and the Role of Facebook in Crowd- Sourced Policing. BC Studies: The British Columbian Quarterly 175(Autumn): 57–72.

Shirky, C. (2008). *Here comes everybody: the power of organizing without organizations*. New York: Penguin.

Silverstone, R., & Haddon, L. (1996). Design and the domestication of information and communication technologies: technical change and everyday life. In R. Mansell & R. Silverstone (Eds.), *Communication by design: The politics of information and communication technologies* (pp. 44–74). Oxford: Oxford University Press.

Slavkovik, M., Dennis, L. A., & Fisher, M. (2015). An abstract formal basis for digital crowds. *Distributed Parallel Databases, 33*, 3–31.

Smith Cross, J. (2015). Police request for anonymous help with Ashley Madison called 'historic' *Metro News*, 24 August. http://www.metronews.ca/news/toronto/2015/08/24/toronto-police-call-for-ashley-madison-help-historic.html.

Solove, D. (2007). *The future of reputation: gossip, rumor, and privacy on the Internet*. New Haven: Yale University Press.

Starbird, K., Maddock, J., Orand, M., Achterman, P., Mason, R. M. (2014). Rumors, false flags, and digital vigilantes: misinformation on twitter after the 2013 Boston Marathon Bombing. *iConference 2014 Proceedings*, 654–662. doi:10.9776/14308.

Thompson, J. B. (2005). The new visibility. *Theory, Culture & Society, 22*(6), 31–51.

Trottier, D. (2012a). Policing Social Media. *Canadian Review of Sociology* 49(4), 411–425.

Trottier, D. (2012b). *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Farnham: Ashgate.

Trottier, D. (2013a). Crowdsourcing CCTV Surveillance on the Internet. *Information, Communication & Society* 17(5), 609–626.

Trottier, D. (2013b). *Identity problems in the Facebook Era*. New York: Routledge.

Trottier, D. (2014). Big Data Ambivalence: Visions and Risks in Practice. *Big Data? Qualitative Approaches to Digital Research*, edited by Hand, M. and Hillyard, S. 51–72. Emerald Publishers.

Trottier, D. (2015) Coming to terms with social media monitoring: Uptake and early assessment. *Crime Media Culture* 11(3), 317–333.

van Dijck, J., & Poell, T. (2013). Understanding social media logic. *Media and Communication, 1*(1), 2–14.

Vancouver. (2011). *Vancouver riot pics: post your photos*. http://www.facebook.com/vancouverriotphotos.

Walsh, J. P. (2014). Watchful citizens: immigration control, surveillance and societal participation. *Social & Legal Studies, 23*(2), 237–259.

Warren, I. (2009). Vigilantism, the Press and Signa Crimes 2006–2007. *Australian & New Zealand Critical Criminology Conference Proceedings*, 275–284. Monash University.

Warren, S. & Brandeis, L. D. (1890) "The right to privacy" *Harvard Law Review* 15(5).

Wellman, B. (2002). Little boxes, glocalization, and networked individualism. In M. Tanabe, P. van den Besselaar, & T. Ishida (Eds.), *Digital cities II* (pp. 11–25). Berlin: Springer.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Wilkinson, P. (2009). Social network sites criticized on bullying. *CNN.com* 18 November. http://edition.cnn.com/2009/TECH/11/18/cyber.bullying/index.html?iref=allsearch.

Wittel, A. (2001). Toward a network sociality. *Theory, Culture and Society, 18*(6), 51–76.